



HAIVISION

Haivision Media Gateway 1.6
Administrator's Guide

HVS-ID-AG-MGW-1.6, Issue 01

Edition Notice

© 2015-2023 Haivision. All rights reserved.

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

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

Edition Notice	2
About Haivision	2
Trademarks	2
Disclaimer	2
Contents	3
About This Document	6
Conventions	6
Typographic Conventions and Elements	6
Action Alerts.....	6
Obtaining Documentation.....	7
Getting Service Support	7
Touring the Interface	8
Overview	8
Features.....	8
Basic Layout and Elements	10
Persistent Screen Elements	10
Variable Screen Elements	11
Interface Screens	12
Sign In Screen	12
Browse Routes Screen.....	13
Administration Screen	15
About Media Gateway Dialog.....	15
Getting Started	17
Accessing Media Gateway	17
Signing into the Media Gateway Interface	17
Signing Out of the Media Gateway Interface	19
Changing Passwords.....	19
Setting Up a Test Route.....	20
Setting Up a Source Stream.....	20
Setting Up a Destination.....	22
Creating a Route	23
Working with Media Gateway	26
Multi-site Live Workflow	26
Pairing the Gateways with Media Platform	27
Defining the Locations (Media Platform).....	27
Source Forwarder.....	28
Source Receivers	29
Multicast Workflow	30
Run-Through Example.....	30
Run-Through Example Recap.....	38
Working with Routes	40
Creating a Route	40
Editing a Route.....	44
Starting, Stopping, and Deleting a Route	45
Viewing a Route’s Statistics	45
Working with Destinations.....	48
Adding a Route’s Destination	49
Editing the Destination.....	49

Starting, Stopping, and Deleting a Destination Node.....	50
Performing Admin Tasks	51
System Activity	51
Viewing the System Activity Dashboard	51
Clearing the Video Cache.....	55
Reports (Logs).....	55
Enabling Diagnostic Logging.....	55
Viewing Reports (Logs).....	56
Media Platform.....	57
Pairing Media Gateway with a Media Platform Server.....	57
Creating your Ecosystem Workspace.....	57
Acquiring a Pairing Passcode.....	58
Pairing the Devices	58
Viewing the Status of Media Gateway Connections	60
Blocking New Media Gateway Connections	60
Updating the Media Platform Server	60
Clearing the Media Platform Server	61
Disconnecting from a Media Platform Server	61
Licensing	61
Licensing Media Gateway.....	61
Adding a Media Gateway License.....	62
Viewing the Status of a License.....	62
Viewing the Media Gateway Version Number	63
Network.....	64
Configuring the Network.....	64
Network Settings	65
Creating a Bonded Interface.....	67
Removing a Bonded Interface.....	67
Presets.....	68
Exporting and Importing Presets	68
Network Storage.....	68
Enabling Network Storage.....	69
Disabling Network Storage.....	69
Certificates	69
Generating a Certificate Signing Request	70
Importing and Activating a Certificate	71
Generating and Importing a Private Key.....	71
Certificate Settings	73
Security	74
Update	74
Downloading System Updates.....	74
Installing/Updating a Package (HaiBundle).....	75
Accounts	75
Viewing the Available User Accounts	75
Changing an Account's Password	76
Using the Console UI	78
Accessing the Console UI.....	78
Showing General Information	79
Editing Network Settings	80
Testing the Network Settings.....	81
Viewing System Logs Available through the Console UI	82
Changing the Current User's Password.....	83
Changing the haiadmin Password	84
Opening a Console UI Terminal Window	84
Setting the Clock	85
Setting the Timezone.....	86
Rebooting or Shutting Down.....	87
Logging Out of the Console UI	88
Troubleshooting	89
Known Issues and Solutions.....	89
Erratic Behavior after a Recent Update	89

Cannot start the Web-Based Interface.....	89
The Web-Based Interface Sign-in isn't Working.....	89
Identifying your Software Version from the Interface.....	89
Status Indicator is not Green	89
Error Message states Failed to receive segment_ cross domain request denied	90
Warranties	91
1-Year Limited Hardware Warranty	91
EXCLUSIONS AND LIMITATIONS	91
OBTAINING WARRANTY SERVICE.....	92
APPLICABLE LAW	92
EULA - End User License Agreement.....	93
READ BEFORE USING	93
SLA - Service Level Agreement.....	93
1. Introduction.....	93
2. Definitions	93
3. Service Levels for the Video Content Management System	93
4. Exceptions to Availability for the VCMS	94
5. Credits for Downtime for the VCMS.....	95
6. Support Services for the VCMS	95
7. Service Levels for Haivision Streaming Media Service	96
8. Credits for Outages of Haivision Streaming Media Service	96
9. No Secondary End User Support	96
Getting Help	97

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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



Tip

Indicates highlights, suggestions, or helpful hints.



Note

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



Important

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

⚠ Caution

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

⚠ Warning

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

Obtaining Documentation

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

Getting Service Support

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

Touring the Interface

Note

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

Topics Discussed

- [Overview](#)
- [Features](#)
- [Basic Layout and Elements](#)
 - [Persistent Screen Elements](#)
 - [Variable Screen Elements](#)
- [Interface Screens](#)
 - [Sign In Screen](#)
 - [Browse Routes Screen](#)
 - [Administration Screen](#)
 - [About Media Gateway Dialog](#)

Overview

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

Features

What's New

Version 1.6 adds the following features:

- [Optional Network Storage](#) — Licensed option that enables you to store the Media Gateway video cache on a Network-Attached Storage (NAS) device through a Network File System (NFS) connection.
- [Support for 608/708 closed captions from DirectTV.](#)
- [Support for alternate language track for HLS outputs.](#)

HLS Output

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

Certificates

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

Multi-site Live Streaming Support

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

Stream Conversion

Note

Media Gateway does not support third-party devices.

Unicast/Multicast Streaming

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

3rd Party Devices

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

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

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

Firewall Friendliness

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

Encryption

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

Stream Management

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

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

Network Routing

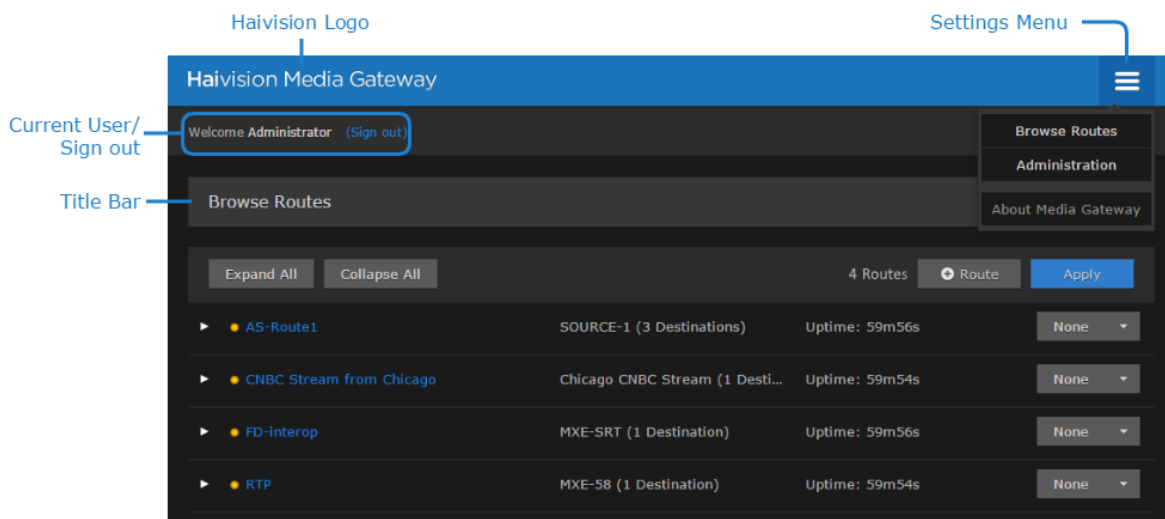
Provisioned with two or more NICs, the Media Gateway lets you route unicast or multicast traffic from one network segment (e.g., SRT over WAN) to another network segment (e.g., TS-UDP over LAN).

Appliance packaging

Media Gateway is available as a hardware appliance with pre-loaded operating system and software. The appliance can be easily upgraded, and has a console user interface to facilitate troubleshooting and low-level configuration. Media Gateway is also available as a software-only product or as a cloud service (available on AWS Marketplace, Microsoft Azure, and Alibaba Cloud).

Basic Layout and Elements

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




Persistent Screen Elements

The following elements are constant and available from any screen.

Haivision Logo (Home Screen/Quick Access)

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

Settings Menu

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

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



Tip

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

Current User/Sign out

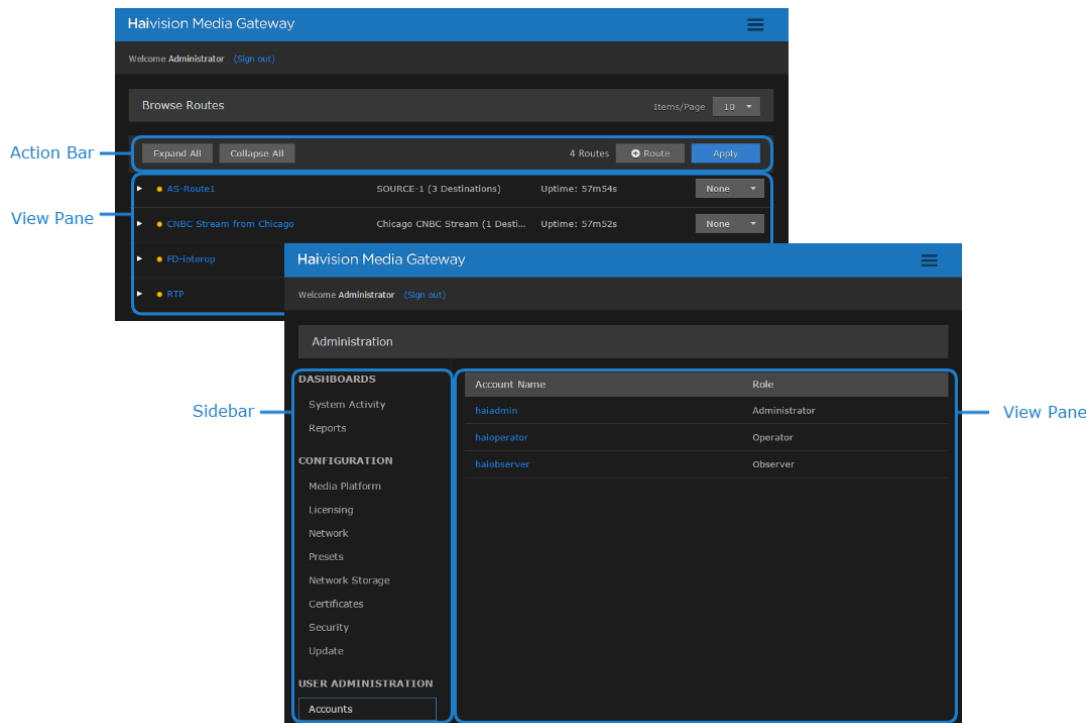
Identifies the user who is currently signed into the system. The Sign Out action link allows you to exit out of the system and return to the Sign In screen.

Title Bar

Identifies the name of the current screen.

Variable Screen Elements

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

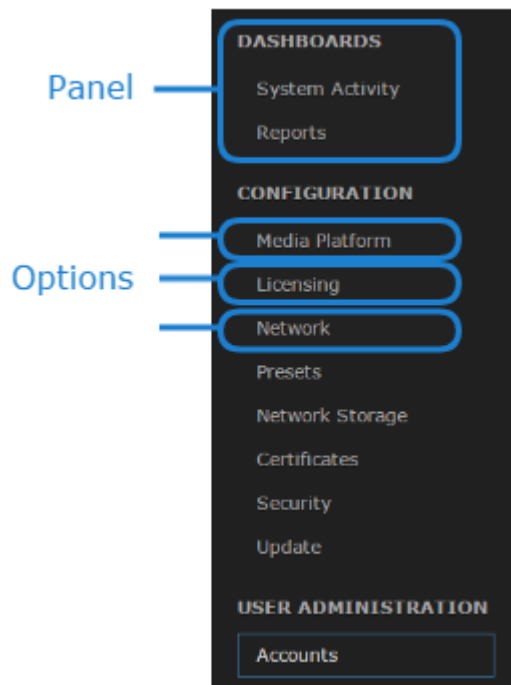


Action Bar

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

Sidebar

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



View Pane

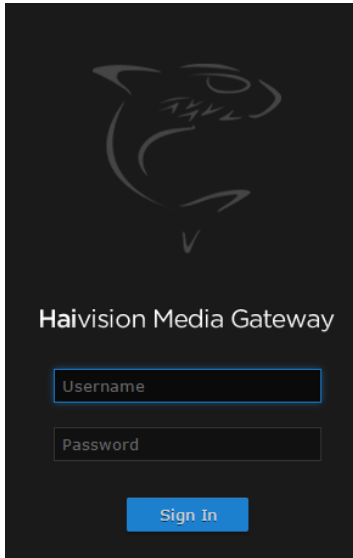
The view pane, depending on the current screen, displays the appropriate items, fields, or status information.

Interface Screens

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

Sign In Screen

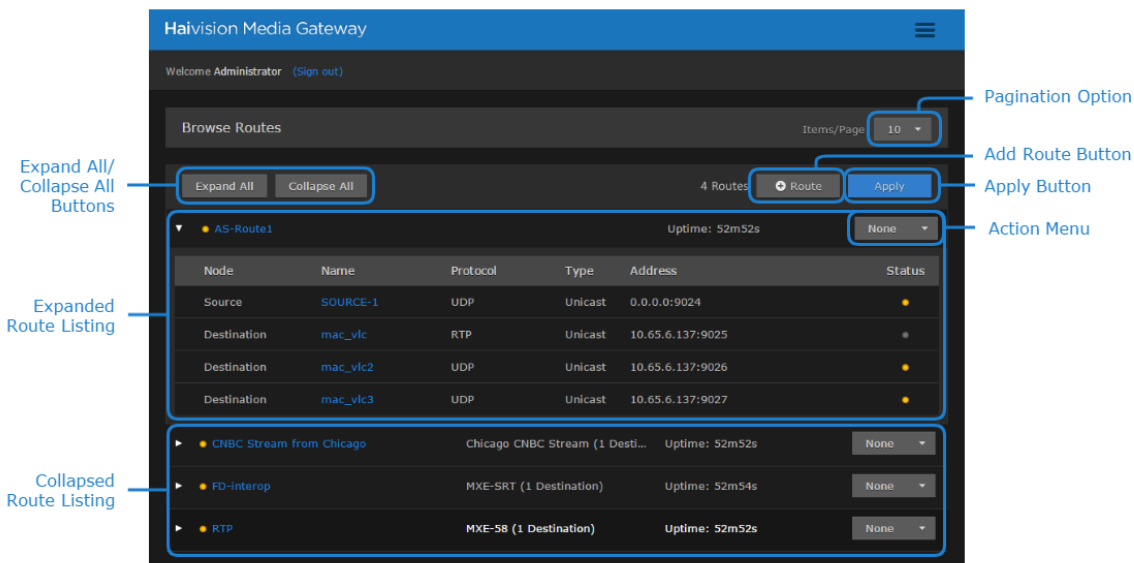
When you start the Media Gateway interface, a Sign In screen appears prompting you to sign into the system ([Signing into the Media Gateway Interface](#)).



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

Browse Routes Screen

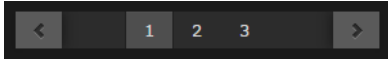
The Browse Routes screen gives you a quick overview of the devices currently managed by Media Gateway. The View Pane lists the available routes. You can expand/ collapse the routes to list more detailed information regarding their source and destinations.



Browse Routes Screen Elements

Title Bar

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



Action Bar

The Action Bar contains the following buttons:

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

View Pane

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

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

View Pane (Expanded)

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

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


i Note

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

Administration Screen

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

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

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

Administration Screen Elements

Sidebar

The sidebar groups the options into various panels:

- **Dashboards Panel**
 - **System Activity** — Provides quick statistics on the system (CPU/memory usage and system uptime), the current version of the software, Video-on-Demand (VOD) bandwidth graph, and disk space statistics.
 - **Reports** — Offers access to a number of different logs providing system, application, and diagnostic messages.
- **Configuration Panel**
 - **Media Platform** — Provides the status and settings pane for pairing the Media Gateway with a Media Platform.
 - **Licensing** — Allows you to add Media Gateway licenses and view their bandwidth limits and status.
 - **Network** — Provides access to the network configuration settings as well as information on the interfaces.
 - **Presets** — Allows you to export the current configuration as a preset file and import a preset file and apply it to the device.
 - **Network Storage** — (Optional license feature) Enables you to move video cache from your Media Gateway to Network-Attached Storage (NAS) through a Network File System (NFS) connection.
 - **Certificates** — Allows you to install an SSL security certificate.
 - **Security** — Allows you to enable FIPS compliance and an advisory banner.
 - **Update** — Identifies the currently installed bundle and allows you to update to a new version of software.
- **User Administration Panel**
 - **Accounts** — Identifies the current roles (administrator, operator, and observer) on the system and the members for each. Allows you to change the user passwords.


View Pane

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

About Media Gateway Dialog

The About Media Gateway dialog provides you with information regarding the current version and build of the installed product and the copyright information.

To open the About Media Gateway dialog:

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

To dismiss the About Media Gateway dialog:

1. Click the **Close** button to dismiss the dialog.



Getting Started

Note

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

Topics Discussed

- [Accessing Media Gateway](#)
 - [Signing into the Media Gateway Interface](#)
 - [Media Gateway SSL Encryption](#)
 - [Signing Out of the Media Gateway Interface](#)
- [Changing Passwords](#)
- [Setting Up a Test Route](#)
 - [Setting Up a Source Stream](#)
 - [Setting Up a Destination](#)
 - [Creating a Route](#)

Accessing Media Gateway

Note

Reference the *Important Notice* document or contact your system administrator for sign-in credentials.

Signing into the Media Gateway Interface

Note

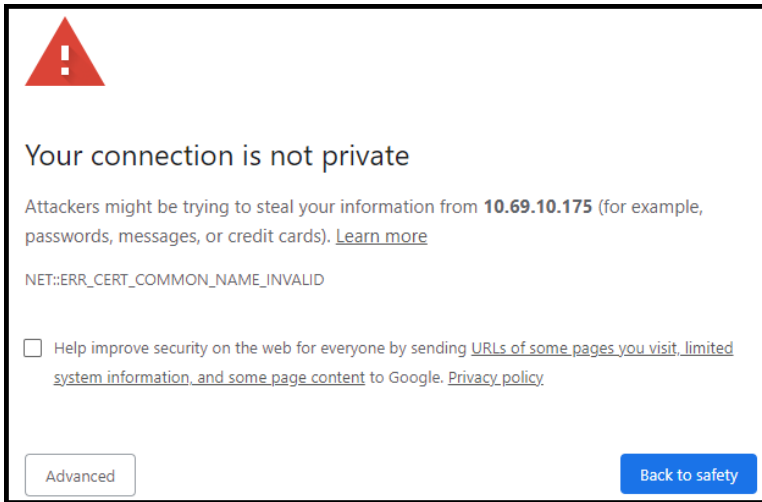
To sign into Media Gateway, ensure that your browser has cookies enabled.

To access the Media Gateway:

1. Open a Web browser and enter the URL or IP address of the Media Gateway server in the browser's address bar. For instance:
`http://<ipaddress>` or `http://<systemurl>` where
 - `<ipaddress>` is the IP address of the system where Media Gateway is installed. For example, `http://10.69.12.152` Connect a monitor to the appliance to display this address on the Console UI. For details, see the *Quick Start Guide*.
 - `<systemurl>` is the system's URL, such as `http://gateway.haivision.com`.
2. When the browser accesses the Media Gateway website, it requests the security certificate to confirm that the site is trusted. If a security certificate is not available or is self-signed, a message similar to the following appears. See [Media Gateway SSL Encryption](#) for more details.

Note

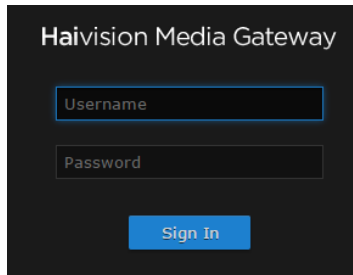
Responses may vary depending upon the browser used.



Important

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

- At the Sign In screen, enter your Media Gateway username and password. See the *Important Notice* document for these credentials and more information.



- Click the **Sign In** button. The Web interface opens to the Browse Routes screen.

Related Topics

- [Sign In Screen](#)
- [Signing Out of the Media Gateway Interface](#)
- [Media Gateway SSL Encryption](#)
- [Changing an Account’s Password](#)

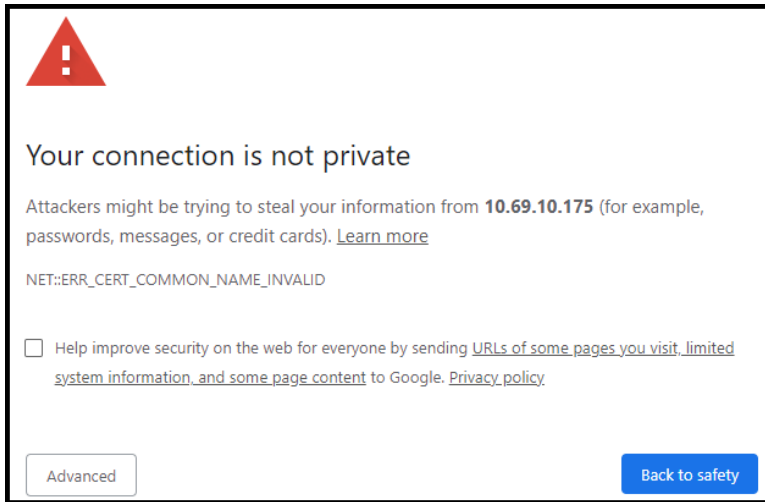
Media Gateway SSL Encryption

Note

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

Media Gateway ships with a self-signed SSL certificate key set which works with any configured server hostname. However, web browsers do not consider self-signed certificates to be trusted, because they

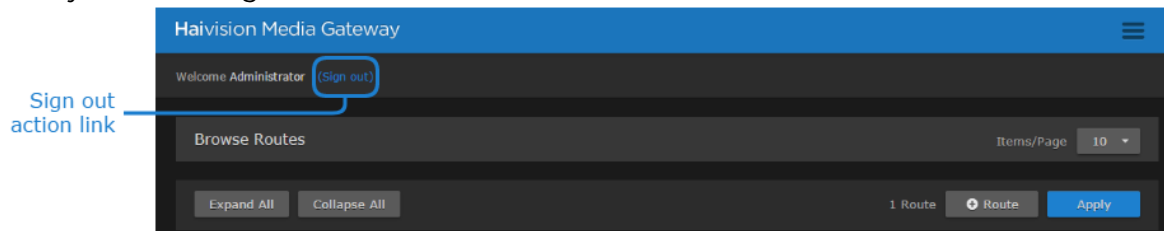
are not signed by a Certificate Authority. Consequently, when accessing the website with a self-signed certificate, users see a security warning and are prompted for authorization as shown below.



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

Signing Out of the Media Gateway Interface

1. When signed into the Media Gateway Interface, click the **Sign Out** action link at the top left corner 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 Media Gateway Interface](#)

Changing Passwords

Important

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

Setting Up a Test Route

Media 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 Media Gateway server is operating normally by setting up a test route. To do this, you need to:

- Set up a **source** (configure a video stream output on a Makito X encoder).
- Set up a **destination** (configure a Makito X Decoder to play back the source stream).
- Define a **route** on the Media 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. 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

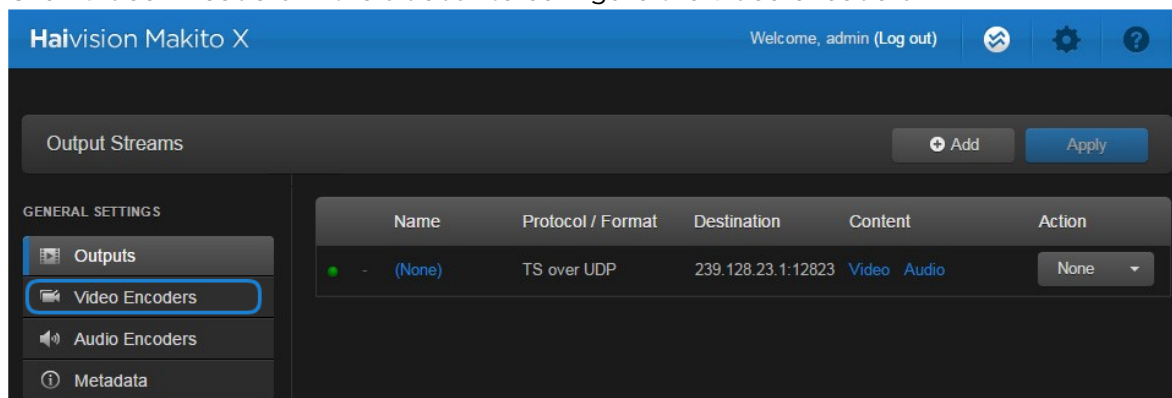
Tip

As you set up the test stream, you may wish to refer to the *Makito X User's Guide*, available from the [Haivision InfoCenter](#).

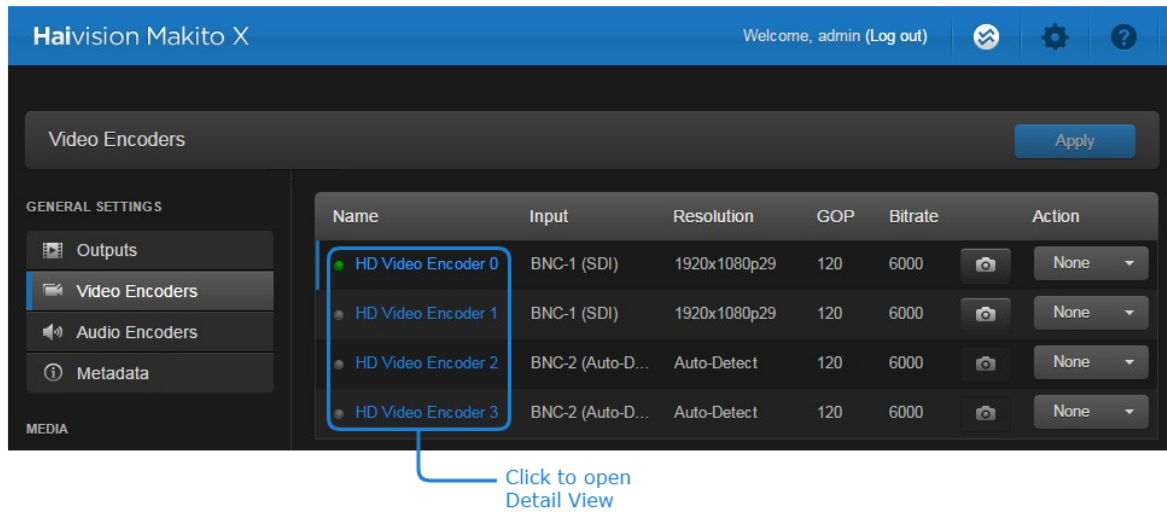
Important

The IP address of your computer must be in the same subnet.

1. If you have not already done so, power up the Makito X Encoder.
2. Open a Web browser to the IP Address for the Makito X and log in. The Web interface opens to the Outputs List View.
3. Click **Video Encoders** in the sidebar to configure the video encoders.

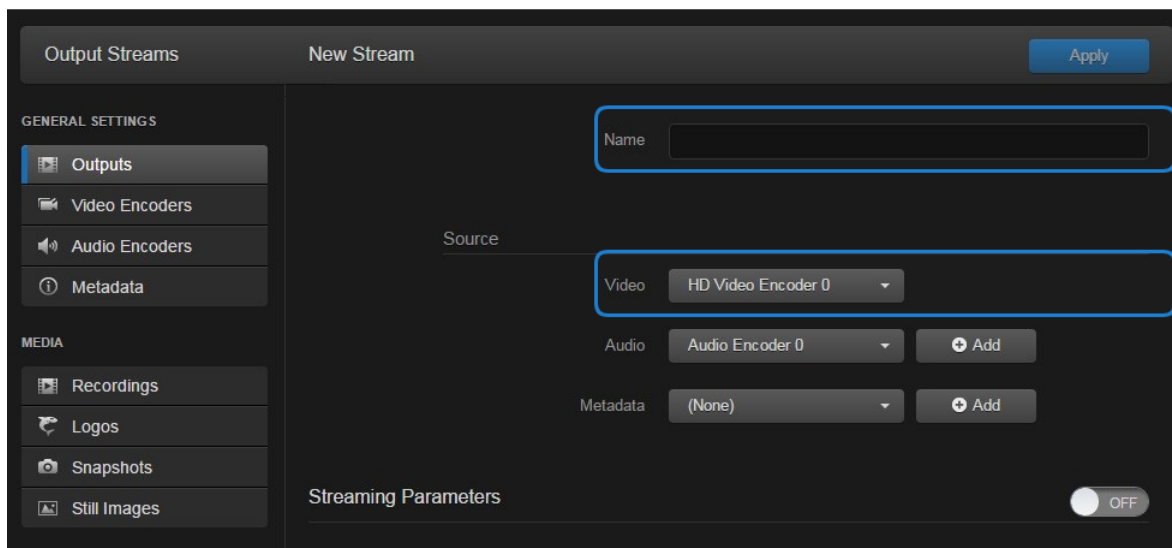


- On the Video Encoders List View, click a link in the table to select an encoder.

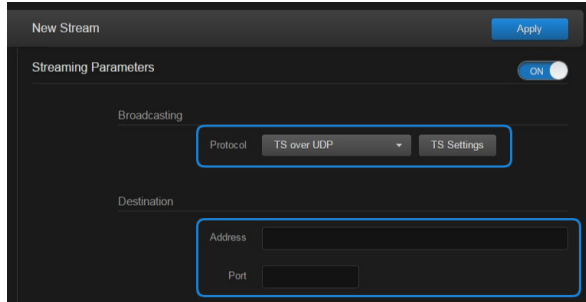


The Video Encoder Detail View opens, displaying the settings for the selected video encoder.

- Select or enter the new values in the appropriate fields.
- Click the **Start** button, and then click **Apply**.
- To set up streaming, click **Outputs** in the sidebar.
- To add an output stream, click the **+Add** button.
- On the New Stream page, type a Name for the stream and select the encoder you started in Step #6.



- To set up streaming:
 - Toggle the Streaming Parameters button to On.
 - In the Broadcasting section, select TS over UDP for the Protocol.
 - In the Destination section, type in the IP Address of the Media Gateway server, and specify a Port number. (You need to specify this number on the Media Gateway server.)



- To apply your changes and start streaming, click the **Apply** button. The new stream appears in the list of output streams.

Name	Protocol / Format	Destination	Content	Action
(None)	TS over UDP	239.128.23.1:12823	Video Audio	None
Media Gatew...	TS over UDP	10.65.146.131:7010	Video Audio	None

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

Setting Up a Destination

Tip

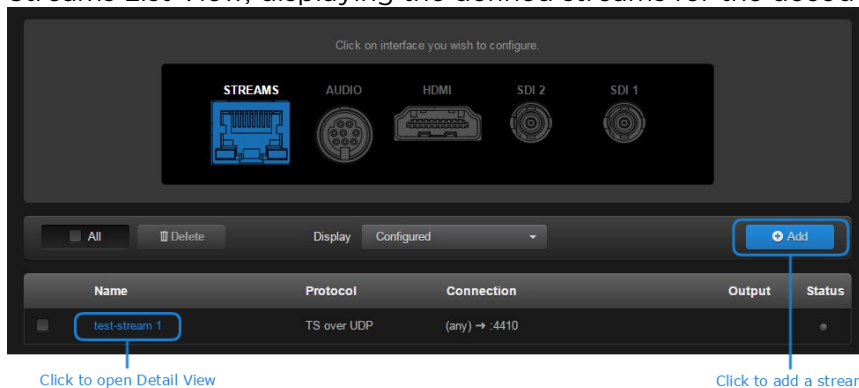
As you configure the stream input, you may wish to refer to the *Makito X Decoder User's Guide*, available from the [Haivision InfoCenter](#).

1.

Note

For the purpose of this test, you should have a monitor connected to the SD1 output.

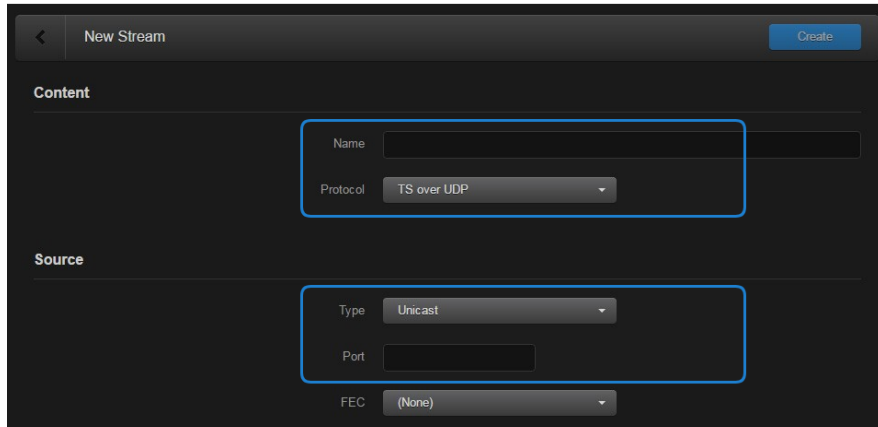
- Open a Web browser to the IP Address for the Makito X and log in. The Web interface opens to the Streams List View, displaying the defined streams for the decoder.



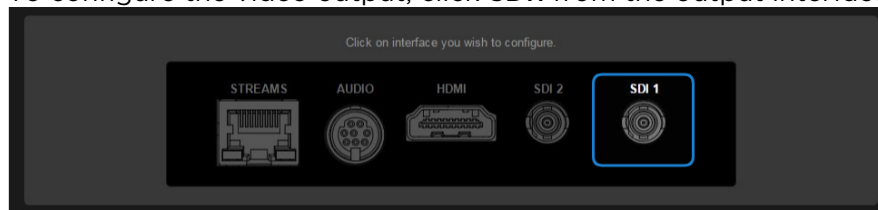
Click to open Detail View

Click to add a stream

- To add an incoming stream, click **+Add**.
- 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 (you will need to enter this port number on the Media Gateway server). Click **Create**.

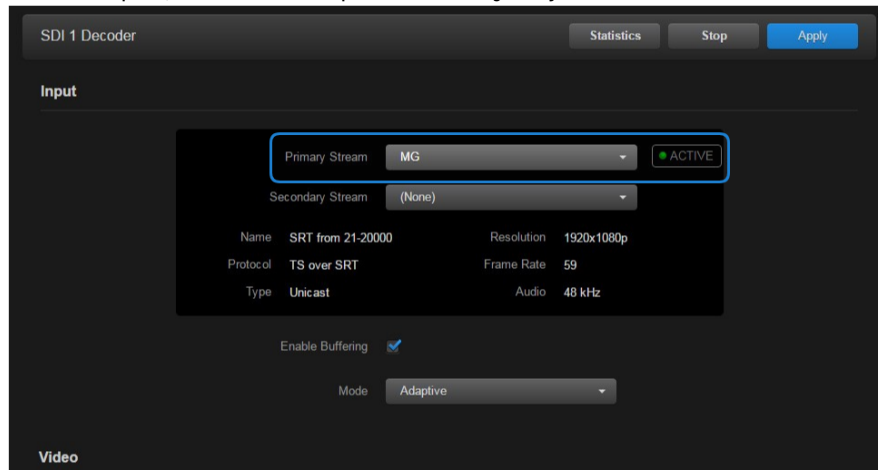


5. To configure the video output, click **SDI1** from the output interface bar.



The SDI1 Decoder page opens, displaying the current video decoding settings.

6. Under Input, select the input stream you just created from the Primary Stream drop-down list.

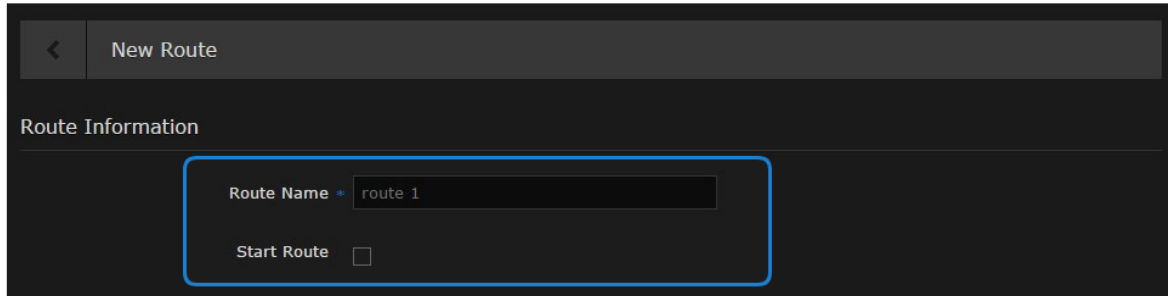


7. To apply your changes, click **Apply**.

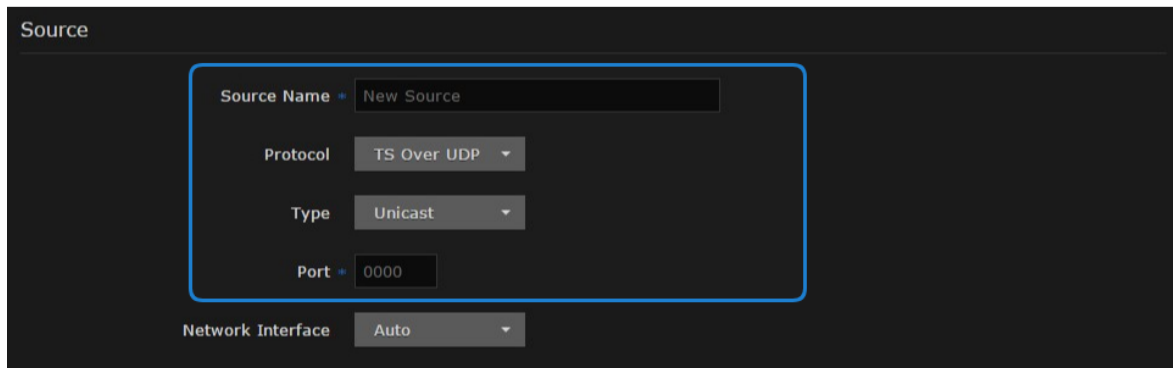
For more details, refer to the *Makito X Decoder User's Guide*.

Creating a Route

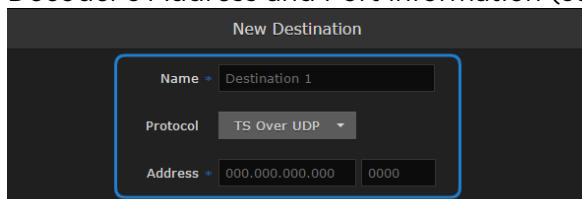
1. If you have not already done so, sign in to the Media Gateway Web interface.
2. On the Browse Routes screen, click the **+Route** button.
3. Supply a Route Name and check the **Start Route** checkbox so that the stream is started upon creation.



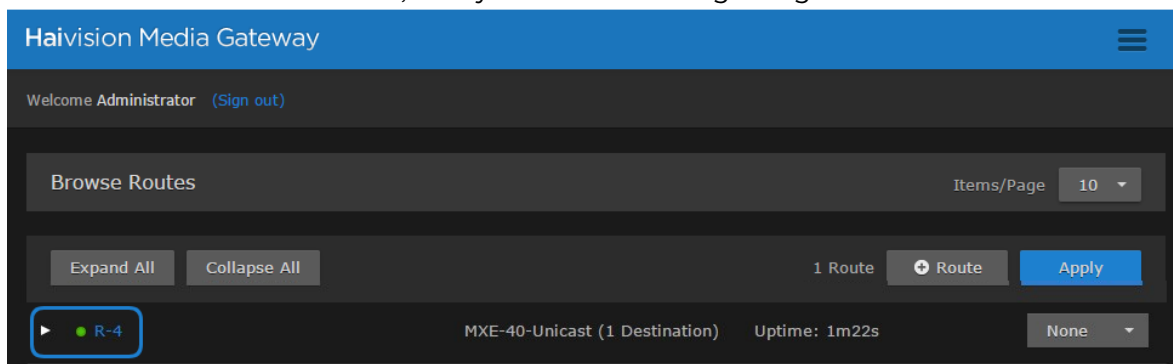
- In the Source section, provide a Source Name, select **TS over UDP** for the Protocol (for this example), and enter the Port number from the Makito X (source) encoder (see Step #10 in [Setting Up a Source Stream](#)).



- Click the **+Destination** button.
- Under New Destination, provide a destination Name, the Protocol (**TS over UDP**), and the Makito X Decoder's Address and Port information (see Step #4 in [Setting Up a Destination](#)).



- When finished, click **Add**. The new route appears in the Destination list.
- Click **Create**.
- On the Browse Routes screen, verify that the status light is green.



You should now see the video from the Makito X Encoder (source) relayed via Media Gateway to the monitor connected to the Makito X Decoder (destination).

For more details, refer to the *Media Gateway Administrator's Guide*.

Working with Media Gateway

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

Topics Discussed

- **Multi-site Live Workflow**
 - **Pairing the Gateways with Media Platform**
 - **Defining the Locations (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**
 - **Adding a Route's Destination**
 - **Editing the Destination**
 - **Starting, Stopping, and Deleting a Destination Node**

Overview

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

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

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

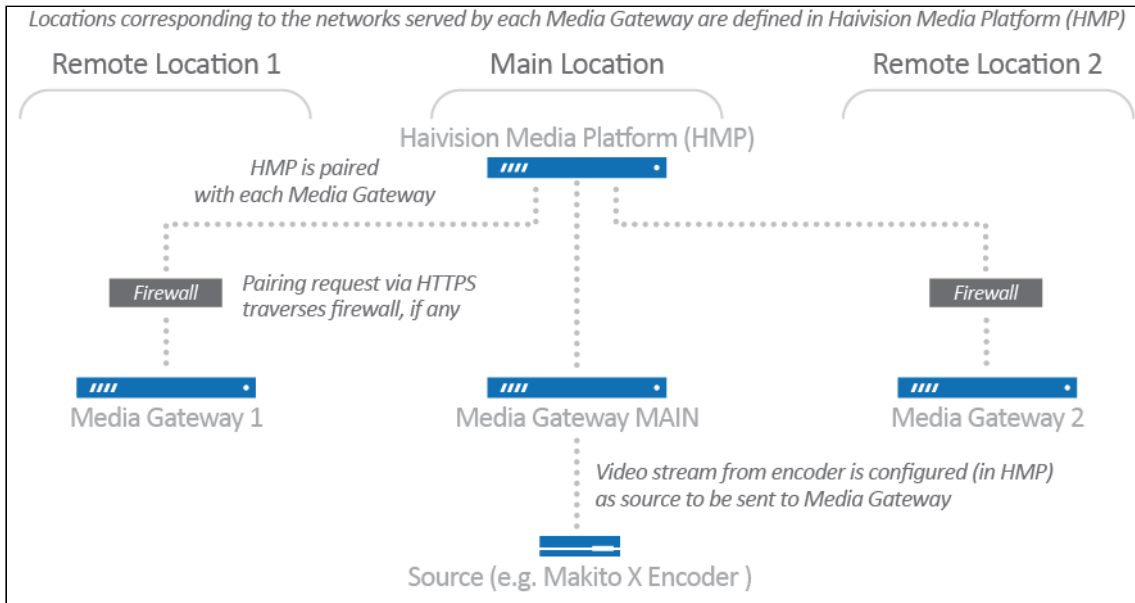
While MPEG-based streams typically do not fare well traveling across the internet, the latest Haivision SRT protocol easily optimizes streaming over unpredictable networks, ensures end-to-end security, and traverses firewalls. Plus, Media Gateway allows stream conversion to TS over UDP or TS over RTP,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

Multi-site Live Workflow

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

Pairing the Gateways with Media Platform

The first step in establishing a multi-site live configuration is to pair the Media Gateways with the Media Platform that is driving the session. In Media Platform, you also need to establish a connection between the video source (for example, a Makito X Encoder) and one of the paired Media Gateways:



Note

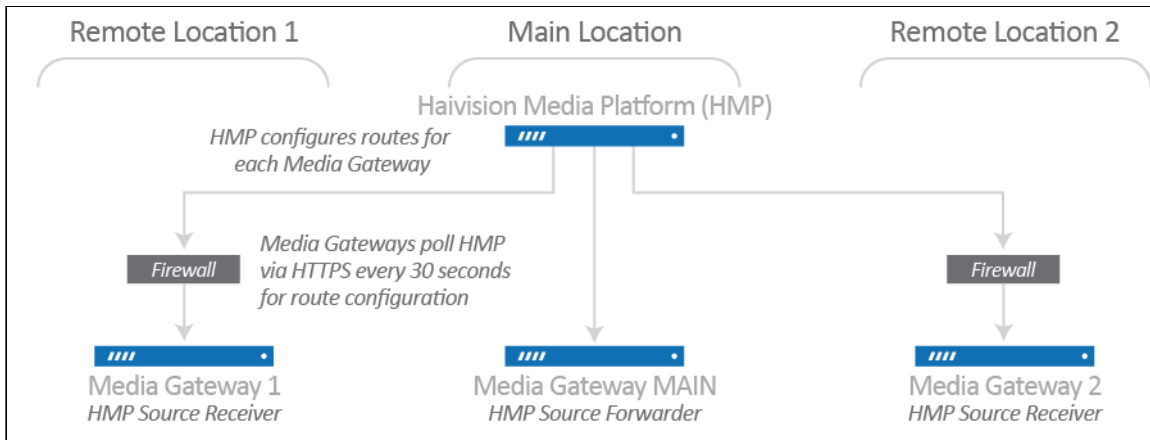
The video source can be connected to the Media Gateway at any of the locations. It does not have to be co-located with the Media Platform. The Media Gateway to which the source is connected must, however, be identified as such on the Media Platform.

Defining the Locations (Media Platform)

After the pairings are complete, you define "locations" in the Media Platform corresponding to the networks served by the various Media Gateways (i.e., the networks on which the users watch the live video). The Media Gateway serving as the ingest point for the live video is considered to be the **source forwarder** in this context. The other Media Gateways are identified as **source receivers**. Based on these locations and the forwarder/receiver designations, Media Platform generates routing configurations for each of the locations. The respective Media Gateways poll the Media Platform at intervals of approximately 30 seconds, and download the routing configuration files.

Note

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



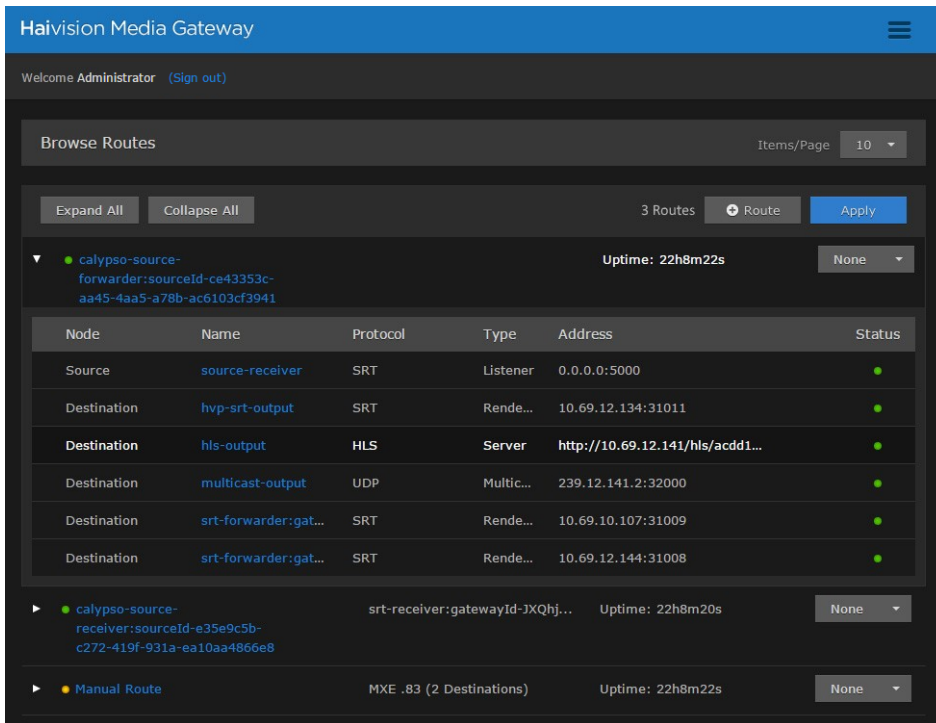
Source Forwarder

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

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

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

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



Note

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

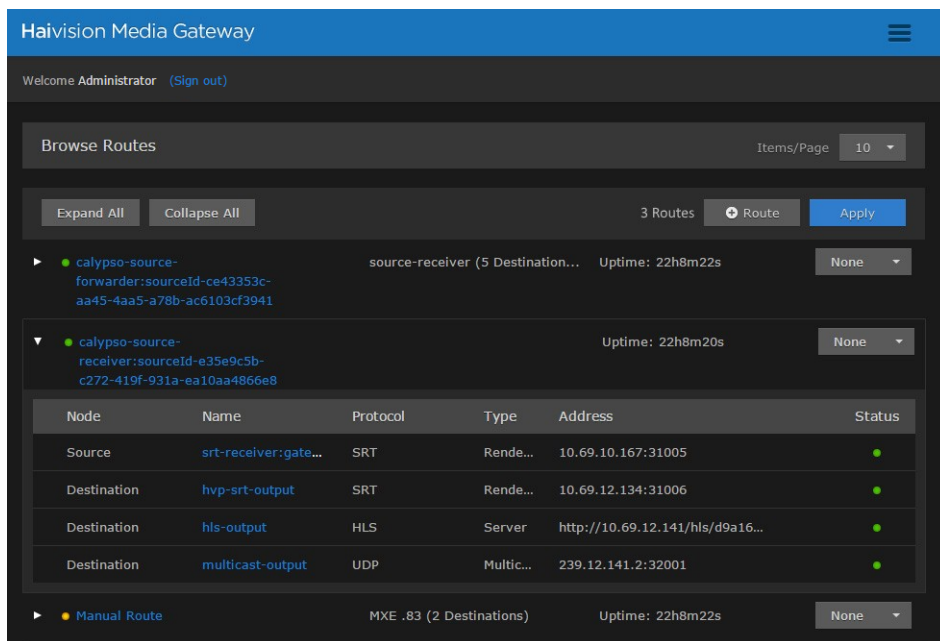
Source Receivers

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

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

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

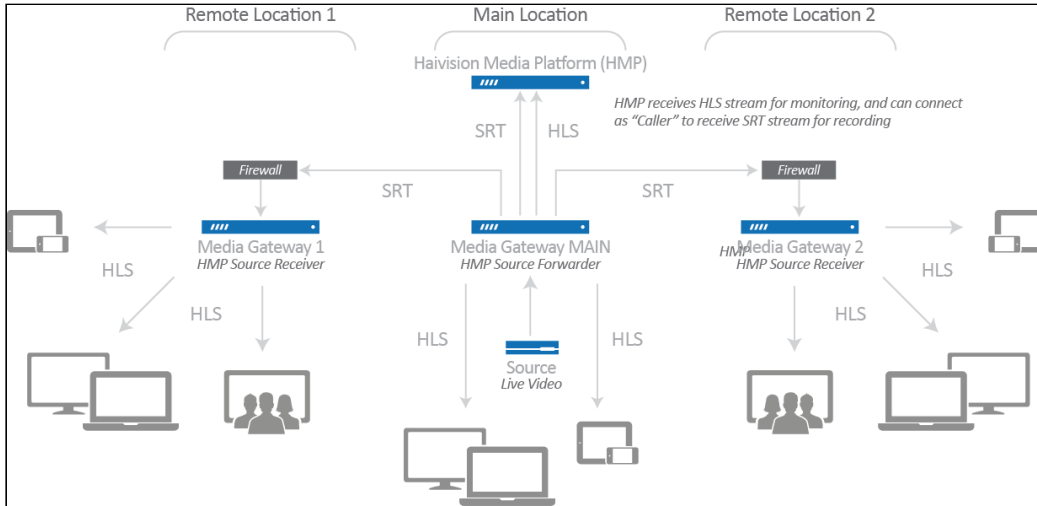
In the following sample screenshot, the route shows the Media Gateway (receiver) propagates the source to a single destination, corresponding to an HLS stream for the local audience:



Note

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

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

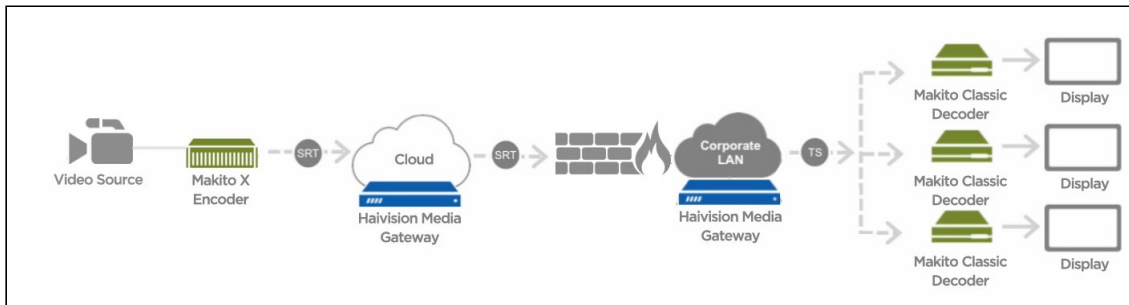


For more information, including complete instructions on how to configure a multi-site live session, please refer to the *Haivision Media Platform Administrator's Guide*.

Multicast Workflow

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

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



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

Note

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

Run-Through Example

Tip

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

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

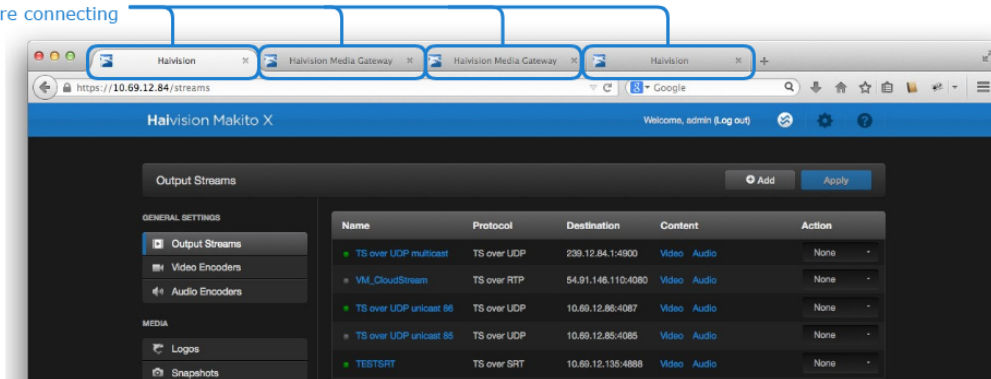
Tip

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

Creating your Workspace (Optional)

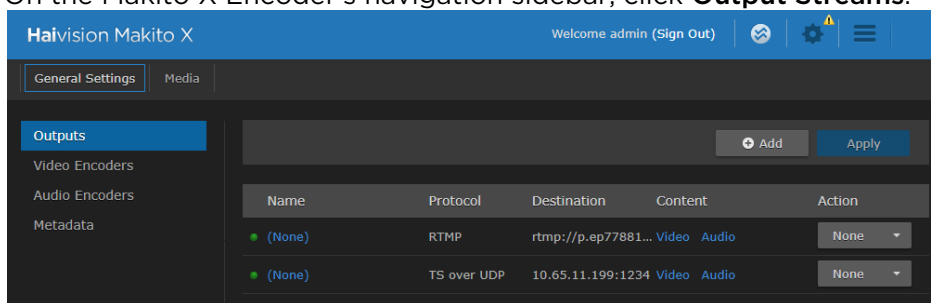
1. In your web browser, open a tab, enter the Makito X Encoder web interface URL, and log in when prompted.
2. Open another new tab, enter the cloud-based Media Gateway web interface URL, and sign in when prompted.
3. Open another new tab, enter the remote site's LAN-based Media Gateway web interface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

Open a tab for each device you are connecting



Establishing the Source

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

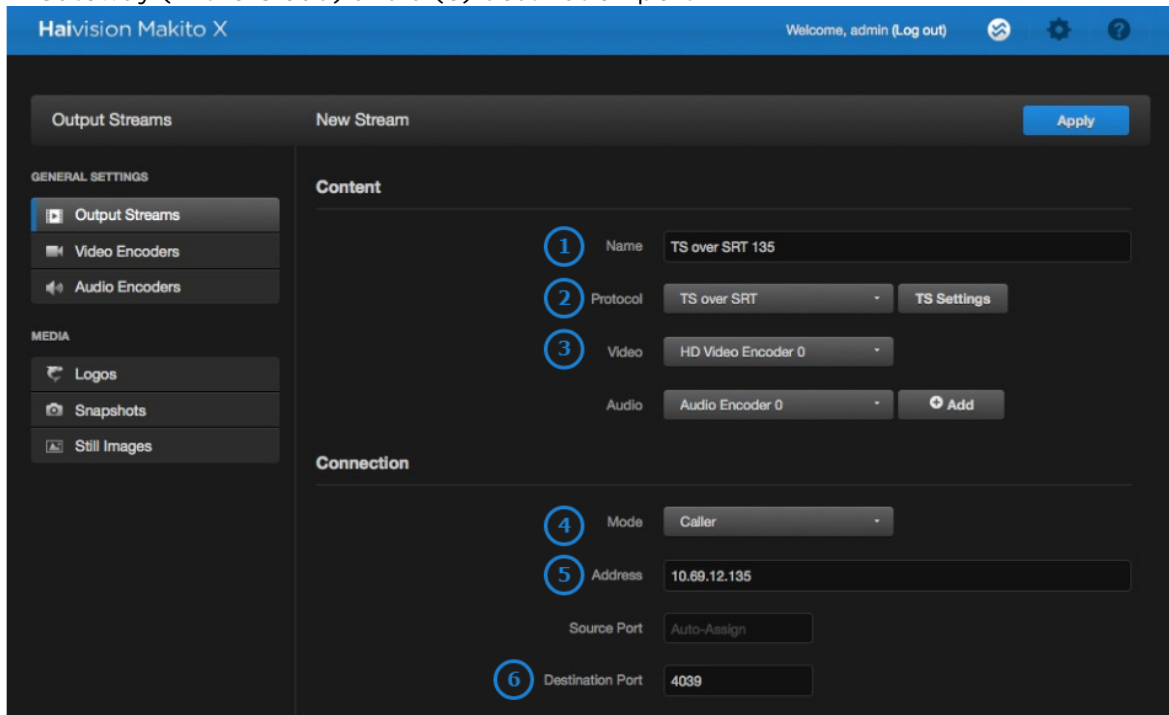


3. The view pane lists the available streams. For this example, we are going to add a stream that uses TS over SRT. Click the **+Add** button. If you have an existing SRT stream, you can modify it instead.

Note

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

4. When the New Stream screen opens:
 - In the Content section, provide a (1) stream name and specify the (2) TS Over SRT protocol. For (3) video, select an active video encoder.
 - In the Connection section, specify the (4) mode as "Caller," enter the (5) address for the Media Gateway (in the Cloud) and a (6) destination port.



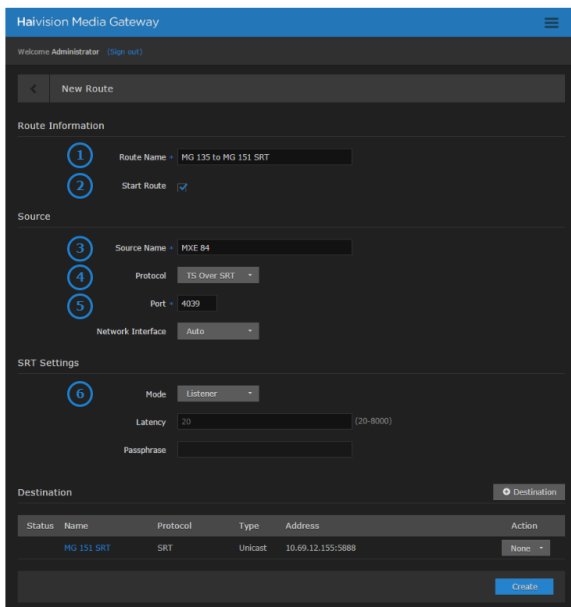
Tip

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

5. Click **Apply**.

Connecting the Source to the Cloud-Hosted Media Gateway

1. If you followed the steps in [Creating your Workspace \(Optional\)](#), switch to the Media Gateway's browser tab. Else, enter the URL for the Media Gateway encoder web interface and sign in when prompted.
2. On the Browse Routes screen, click the **+Route** button.
3. When the New Route screen opens:
 - In the Route Information section, supply a (1) route name and click the (2) Start Route checkbox so that the stream is started after creation.
 - In the Source section, provide a (3) source name, specify the (4) protocol as TS Over SRT (for this example), and enter the (5) port from the source encoder.
 - In the SRT Settings section set the (6) mode to Listener.



Tip

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

4. Click the **+Destination** button.
5. In the New Destination dialog:
 - Enter the information for the LAN-based Media Gateway. Provide a (1) name, the (3) address, and the (4) port information.
 - Change the (2) protocol to "TS over SRT."
 - Under the SRT Settings section, change the (5) type to "Caller."

Note

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

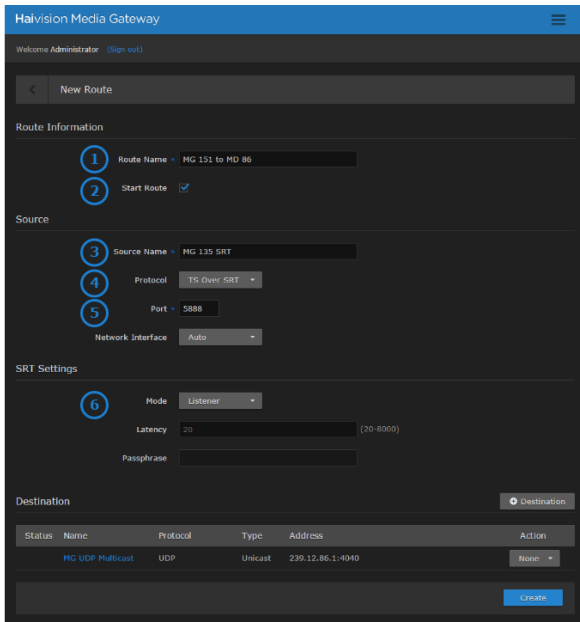
Tip

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

6. When finished, click **Add**.
7. On the New Route screen, when finished, click **Create**.
8. On the Browse Routes screen, expand the route to verify that the status lights change to green.

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

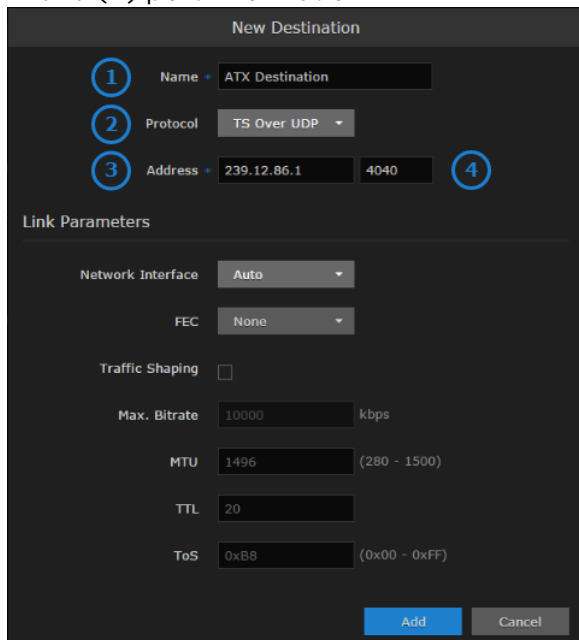
1. Switch to the LAN-based Media Gateway browser tab or enter the URL for the LAN-based Media Gateway web interface.
2. Click **+Route** button to add a new route.
3. In the New Route screen:
 - Supply a (1) route name and click the (2) Start Route checkbox so that the stream will be started upon creation.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



Tip

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

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

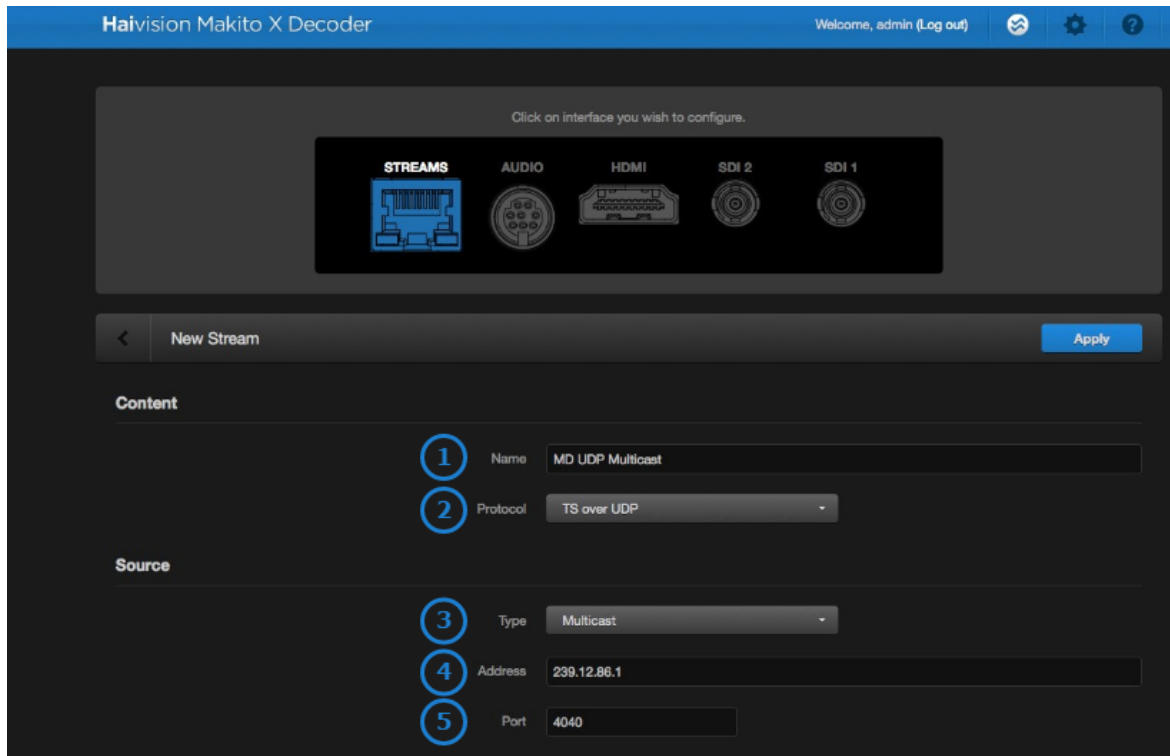


6. When finished, click **Add**.
7. In the New Route screen, click **Create**.

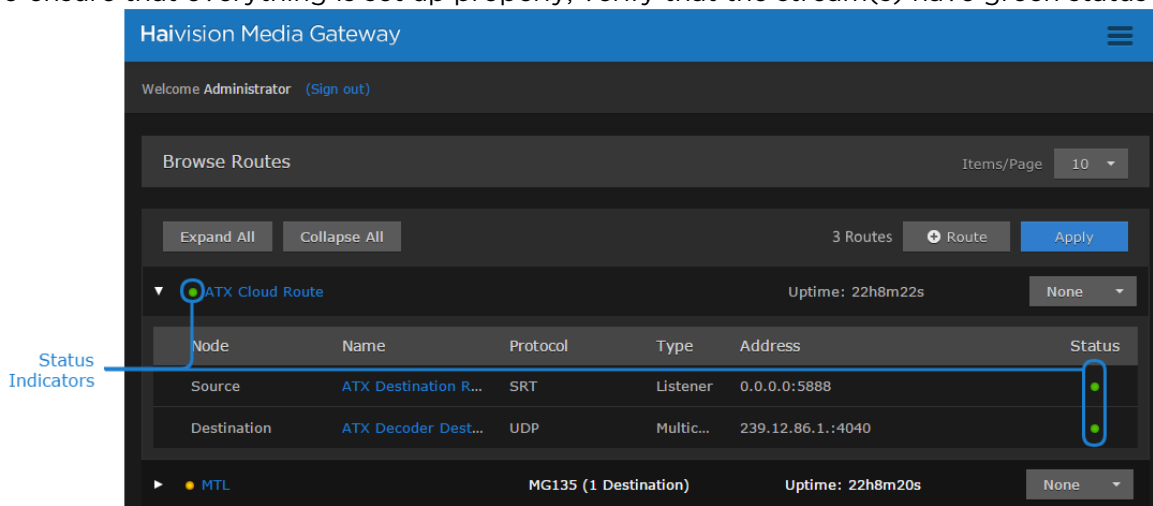
Connecting the Makito X Decoder

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

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



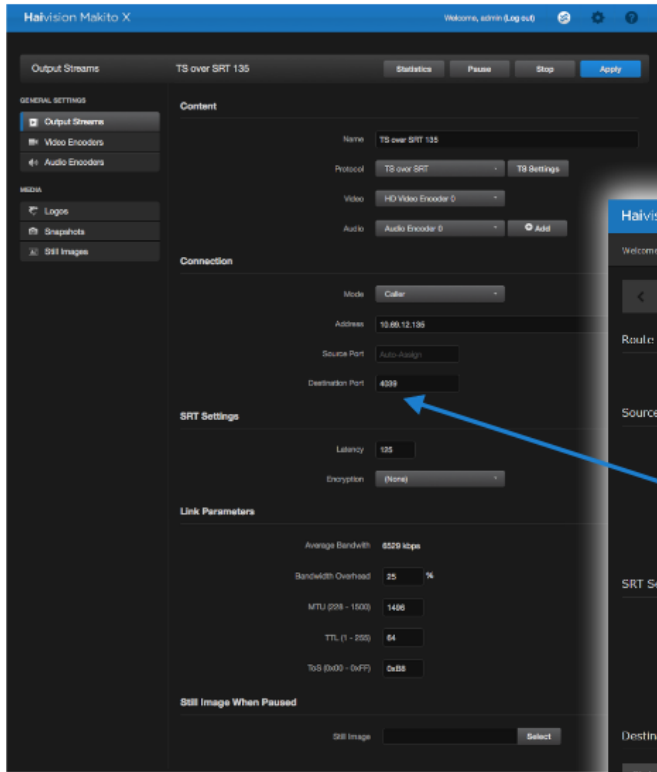
4. Click **Apply**.
5. Repeat steps #2 and #3 as needed to define additional streams.
6. To ensure that everything is set up properly, verify that the stream(s) have green status indicators.



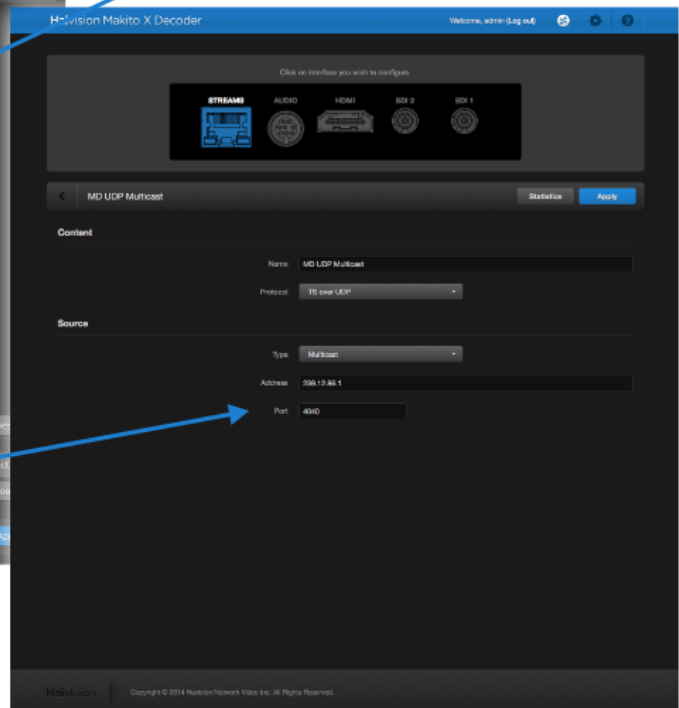
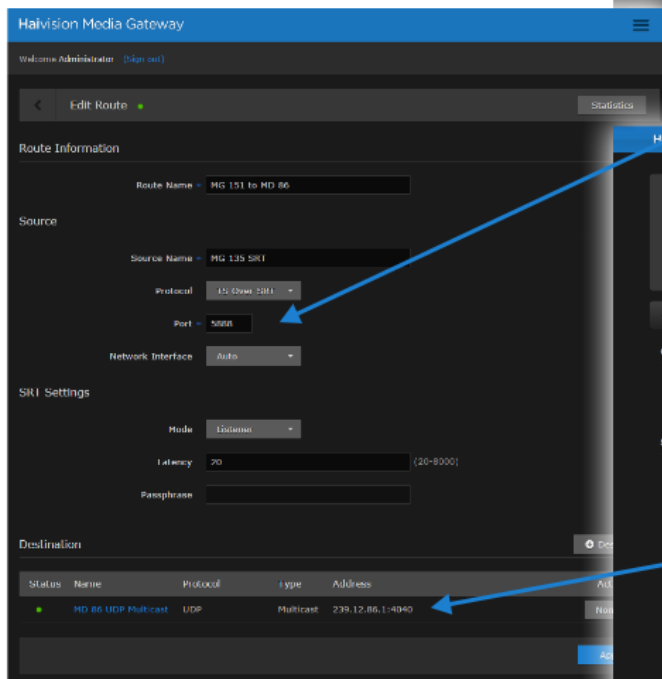
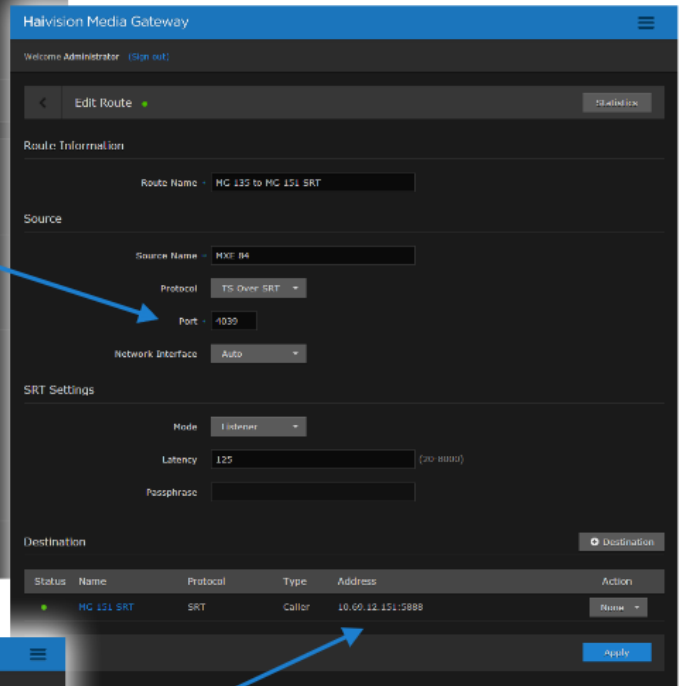
Note

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

Run-Through Example Recap



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



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


Working with Routes

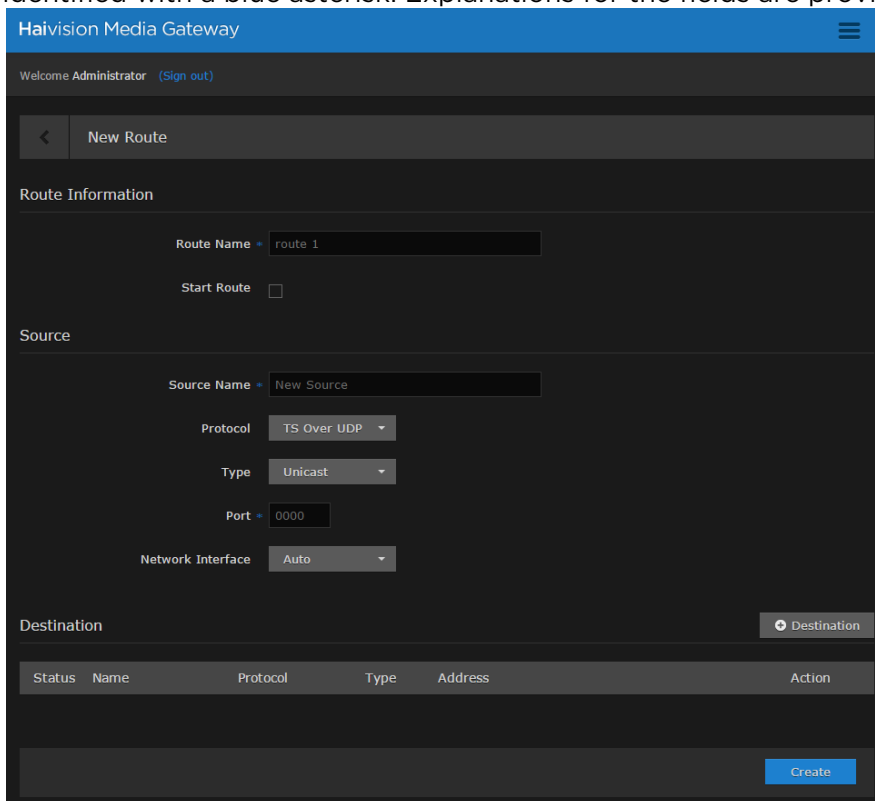
Note

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

Creating a Route

To create a route:

1. Click the  icon and click **Browse Routes**.
2. On the Actions bar, click the **+Route** button.
3. On the New Route screen, provide appropriate settings for the route. The required fields are identified with a blue asterisk. Explanations for the fields are provided in [Available Route Settings](#).



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

Destinations heading in **Available Route Settings**.

6. Checking the **Traffic Shaping** checkbox allows you to manually adjust the maximum bitrate. Traffic Shaping controls the outgoing stream so that the inter-packet time is constrained, in order to reduce the probability that TCP packets are dropped in a session. Enabling Traffic Shaping does *not* dynamically modify the video encoder bitrate.
7. When you have finished entering the required data, click the **Create** button to specify the destination.

Note



The newly created destination is added locally (at this point, no server call is made).

8. When finished entering all your destinations, click **Apply**. Now the configurations, including route, source, and destinations, are saved to the server.

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

















Available Route Settings

Route Setting	Description
Route Information	
Route Name ¹	Name (limited to 60 printable characters). <div style="border: 1px solid green; padding: 5px;"> <p>Tip</p> <p>Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.</p> </div>
Start Route	Check this box to start the route upon creation.
Source	

Route Setting	Description
Source Name ¹	<div style="border: 1px solid green; padding: 5px;"> <p> Tip</p> <p>Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.</p> </div>
Protocol	Select from the drop-down menu one of the available streaming protocols: <ul style="list-style-type: none"> • TS Over UDP • TS Over SRT • TS Over RTP
Type ²	The type of distribution method: <ul style="list-style-type: none"> • Unicast • Multicast
Address/Port ^{1 2}	The address and port on which the server listens.
Network Interface	Identifies the network interface to use for the stream. Available settings depend on the hardware configuration.
SRT Settings ² (Source)	
Mode	Specifies the SRT Connection Mode: <ul style="list-style-type: none"> • 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.
Latency	Specifies the SRT receiver buffer that permits lost packet recovery. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20 - 8000 ms NOTE: Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.
Passphrase	(Only required and accepted if Encryption is enabled on the Destination) Specifies a string used to generate the encryption keys to protect the stream. Range = 10-79 UTF8 characters
Destinations	
Name ¹	<div style="border: 1px solid green; padding: 5px;"> <p> Tip</p> <p>Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.</p> </div>
Protocol	Select from the drop-down menu one of the available streaming protocols: <ul style="list-style-type: none"> • TS Over UDP • TS Over SRT • TS Over RTP • HLS

Route Setting	Description
Address / Port ^{1 2}	<p><i>For TS only:</i> Depending upon the type of SRT settings, this field may require an IP address of transmission and the listening port.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>TS Over SRT only requires the Port field.</p> </div>
Segment Duration	<p><i>For HLS only:</i> Maximum media segment duration (in seconds). A target duration of 10 seconds is recommended, and is the default if no target duration is specified.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>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.</p> </div>
Encryption	<i>For HLS only:</i> Check this box to activate the default HLS encryption (AES-128 using 16-octet keys).
Segments/Key	<i>For HLS only:</i> If encryption is enabled, inserts a new random key file every n media segments (key rotation). Each group of n files is encrypted using a different key.
Link Parameters	
Port ^{1 2}	The port on which the server listens.
Network Interface	Identifies the network interface: <ul style="list-style-type: none"> • Auto • Eth0, Eth1 (may vary; options include other available interfaces)
FEC ²	<p>(Only available on non-SRT streams) Enable Forward Error Correction (FEC). Select either:</p> <ul style="list-style-type: none"> • (None) • Note <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>VF FEC is a proprietary FEC and is not inter-operable with devices outside of the Haivision family.</p> </div>
Traffic Shaping ²	<p>(Only available on non-SRT streams) Check or clear this checkbox to enable or disable Traffic Shaping for the stream. For some limited networks such as satellites or some dedicated network pipes, it may be necessary to enable Traffic Shaping to smooth the traffic and respect the absolute upper limit configured.</p>
Maximum Bitrate ²	(Only available on non-SRT streams) Bitrate upper bound in kbps. Field is editable if the Traffic Shaping checkbox is selected.
MTU	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing data stream.
TTL	(Time-to Live for stream packets) Specifies the number of router hops the Stream packet is allowed to travel/pass before it must be discarded. Value is higher or equal to 1.

Route Setting	Description
ToS	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Value is higher or equal to 0.
SRT Settings ² (Destination)	
Type	The SRT connection (handshake) mode to be used with this destination: <ul style="list-style-type: none"> • Listener • Caller • Rendezvous
Latency	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Note</p> <p>Latency applies to the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.</p> </div>
Bandwidth Overhead	<p>The percentage of the average bandwidth ³ that is used to accommodate SRT controls as well as recovery of lost packets.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Note</p> <p>SRT streams may temporarily overshoot the defined bandwidth overhead limit.</p> </div>
Encryption	The encryption, if any, to be applied to the SRT stream: None, AES-128, or AES-256.

1. Required field.      
2. Field availability depends upon other selections made.         
3. The "average bandwidth" is an internal measurement of the outbound traffic, on a per stream basis. 

Related Topics

- [Editing a Route](#)
- [Starting, Stopping, and Deleting a Route](#)
- [Viewing a Route's Statistics](#)
- [Adding a Route's Destination](#)

Editing a Route

To edit a route:

1. On the Browse Routes screen, click the **Route Name** for the listing you want to edit.
2. In the the Edit Route screen, adjust the settings as desired.
3. Click the **Apply** button to save the new settings.

Related Topics

- [Creating a Route](#)
- [Starting, Stopping, and Deleting a Route](#)

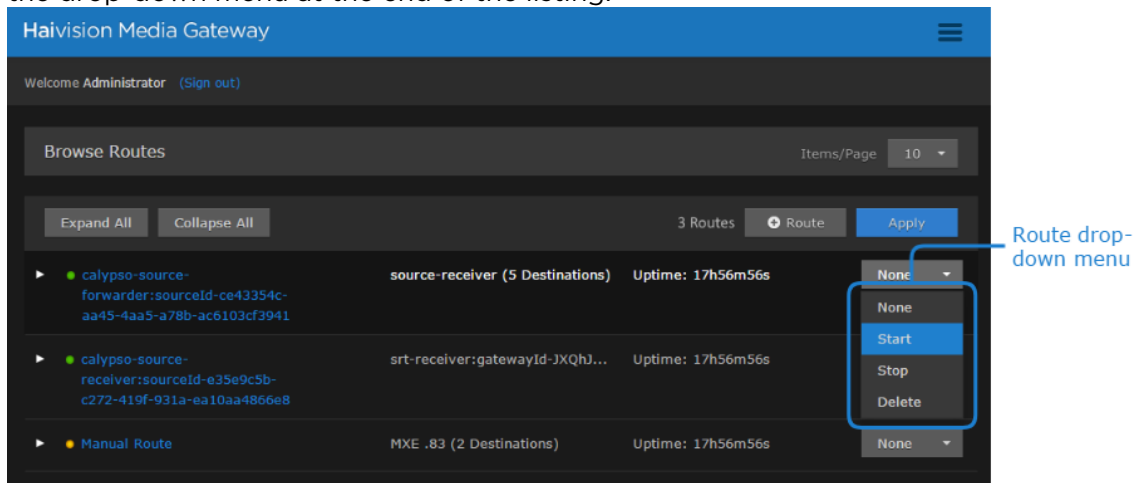
Starting, Stopping, and Deleting a Route

Note

Starting a route also starts its source and destinations.

To start a route:

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



2. Click **Apply**.

Related Topics

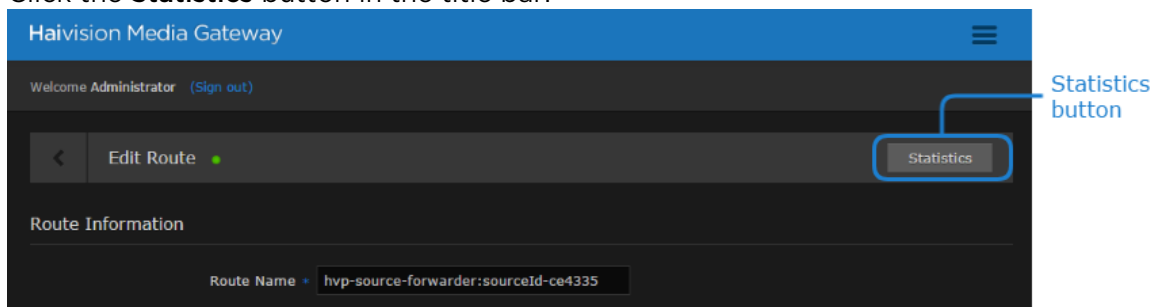
- [Creating a Route](#)
- [Available Route Settings](#)
- [Adding a Route’s Destination](#)
- [Editing a Route](#)
- [Viewing a Route’s Statistics](#)

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 Browse Routes screen, click on the the desired route listing to open the Edit Route page.
2. Click the **Statistics** button in the title bar.



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

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

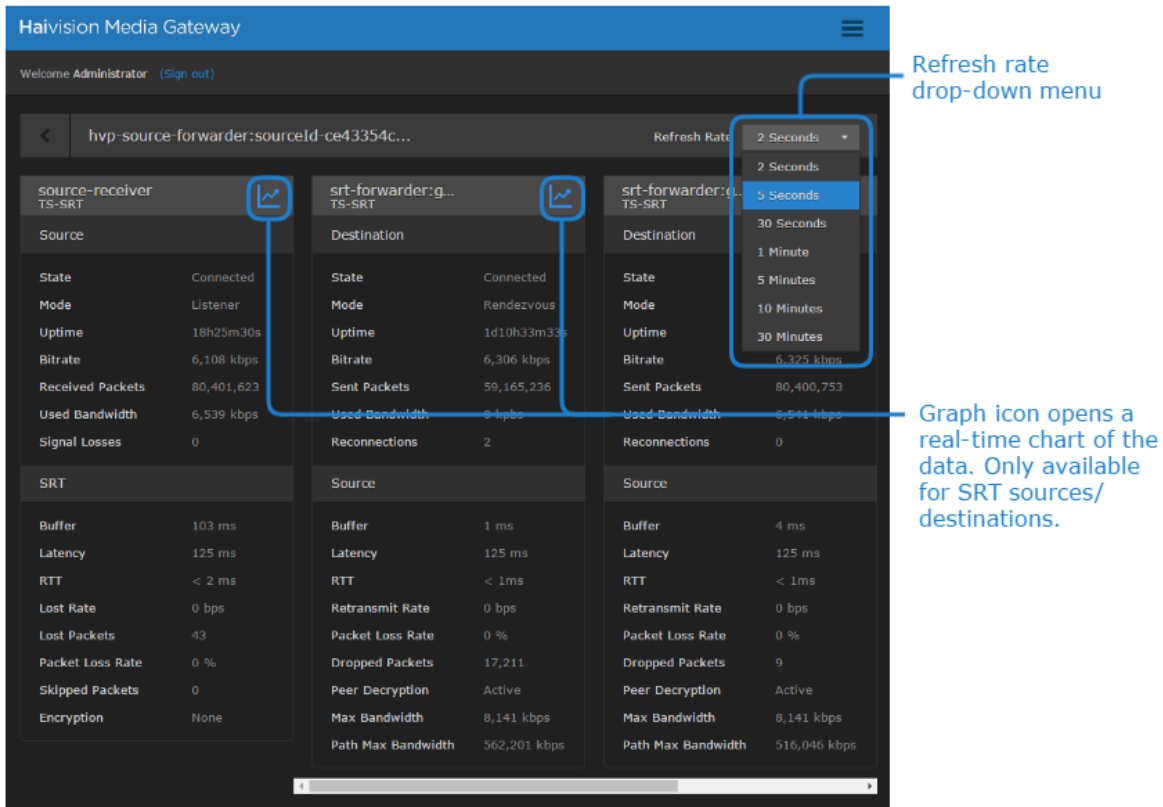
The column sections are organized by Type.

The screenshot shows the 'Haivision Media Gateway' interface. At the top, it says 'Welcome Administrator (Sign out)'. Below that, there's a breadcrumb trail: 'hvp-source-forwarder:sourceId-ce43354c...'. To the right of the breadcrumb is a 'Refresh Rate' dropdown menu set to '2 Seconds'. The main content area is divided into three columns, each with a heading and a refresh icon. The first column is titled 'source-receiver TS-SRT' and contains statistics for the source. The second and third columns are titled 'srt-forwarder:g... TS-SRT' and contain statistics for destinations. Each column lists various metrics such as State, Mode, Uptime, Bitrate, Packets, Bandwidth, and SRT parameters.

source-receiver TS-SRT		srt-forwarder:g... TS-SRT		srt-forwarder:g... TS-SRT	
Source		Destination		Destination	
State	Connected	State	Connected	State	Connected
Mode	Listener	Mode	Rendezvous	Mode	Rendezvous
Uptime	18h25m30s	Uptime	1d10h33m33s	Uptime	1d10h33m33s
Bitrate	6,108 kbps	Bitrate	6,306 kbps	Bitrate	6,325 kbps
Received Packets	80,401,623	Sent Packets	59,165,236	Sent Packets	80,400,753
Used Bandwidth	6,539 kbps	Used Bandwidth	0 kbps	Used Bandwidth	6,541 kbps
Signal Losses	0	Reconnections	2	Reconnections	0
SRT		Source		Source	
Buffer	103 ms	Buffer	1 ms	Buffer	4 ms
Latency	125 ms	Latency	125 ms	Latency	125 ms
RTT	< 2 ms	RTT	< 1ms	RTT	< 1ms
Lost Rate	0 bps	Retransmit Rate	0 bps	Retransmit Rate	0 bps
Lost Packets	43	Packet Loss Rate	0 %	Packet Loss Rate	0 %
Packet Loss Rate	0 %	Dropped Packets	17,211	Dropped Packets	9
Skipped Packets	0	Peer Decryption	Active	Peer Decryption	Active
Encryption	None	Max Bandwidth	8,141 kbps	Max Bandwidth	8,141 kbps
		Path Max Bandwidth	562,201 kbps	Path Max Bandwidth	516,046 kbps

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

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



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

When the Statistics Graph View window opens, it displays the data numerically and graphically for that route. This window opens separately so that you can keep it open for monitoring – even create a dashboard of one or more devices. This window remains open until you manually close it.



6. To save the data for use with another application (such as a spreadsheet), click the **Download CSV** button. Typically, this downloads the data in a comma-separated values text file. For Safari browsers, this displays the file in a new window. Right-click the browser window and select "Save Page as..." to download the file.
7. You can adjust the real-time graph by:
 - Setting the Refresh Rate with the drop-down menu in the title bar.
 - Changing the scale interval using Timescale drop-down menu. This adjusts the x-axis in the graphs. Options include: 5 minutes, 1 hour, and 24 hours.
 - Checking/unchecking the checkboxes of each legend to display/hide data components.
 - Hover your mouse cursor over the graph to reveal the time and value of the selected data point.

Related Topics

- [Creating a Route](#)
- [Available Route Settings](#)
- [Adding a Route’s Destination](#)
- [Starting, Stopping, and Deleting a Route](#)
- [Reports \(Logs\)](#)

Working with Destinations

Note

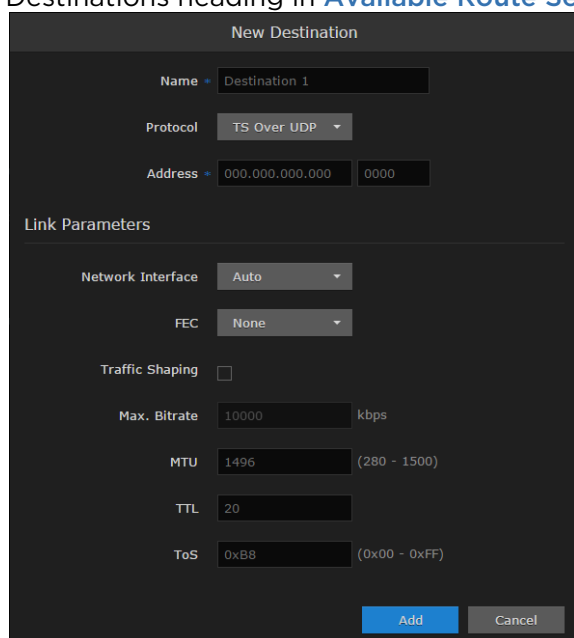
Keep in mind that **route actions**, when applied, override all the Destination states. For instance, performing a stop action on a route, once applied, stops any destinations for the route as well.

Adding a Route's Destination

Destinations are not started automatically.

To add a destination:

1. On the Browse Routes screen, click on a route that you want to add a destination to.
2. On the Edit Route page, click the **+Destination** button.
3. In the New Destination dialog, provide appropriate settings for the Destination. See the Destinations heading in [Available Route Settings](#) for field specifics.



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

! Important

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

Editing the Destination

To change the Destination settings:

1. On the Browse Routes screen, click the individual ► icon or the **Expand All** button to reveal the destination specifics for the route.
2. Locate the destination you want to configure and click it to open the Edit Destination dialog.

- On the Edit Destination dialog, adjust the settings as desired. See the Destinations heading in [Available Route Settings](#) for definitions of the fields.

- Click the **Save** button.

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

Important

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

Starting, Stopping, and Deleting a Destination Node

To start, stop, or delete a destination node:

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

Status	Name	Protocol	Type	Address	Action
●	Dest1 - 123456789	SRT	Listener	0.0.0.0:4444	None
●	Dest3	UDP	Unicast	2.2.2.3:1212	Start Stop Delete

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

Note

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

Performing Admin Tasks

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](#).

Topics Discussed

- [System Activity](#)
- [Reports \(Logs\)](#)
- [Media Platform](#)
- [Licensing](#)
- [Network](#)
- [Presets](#)
- [Exporting and Importing Presets](#)
- [Network Storage](#)
- [Certificates](#)
- [Security](#)
- [Update](#)
- [Accounts](#)


System Activity

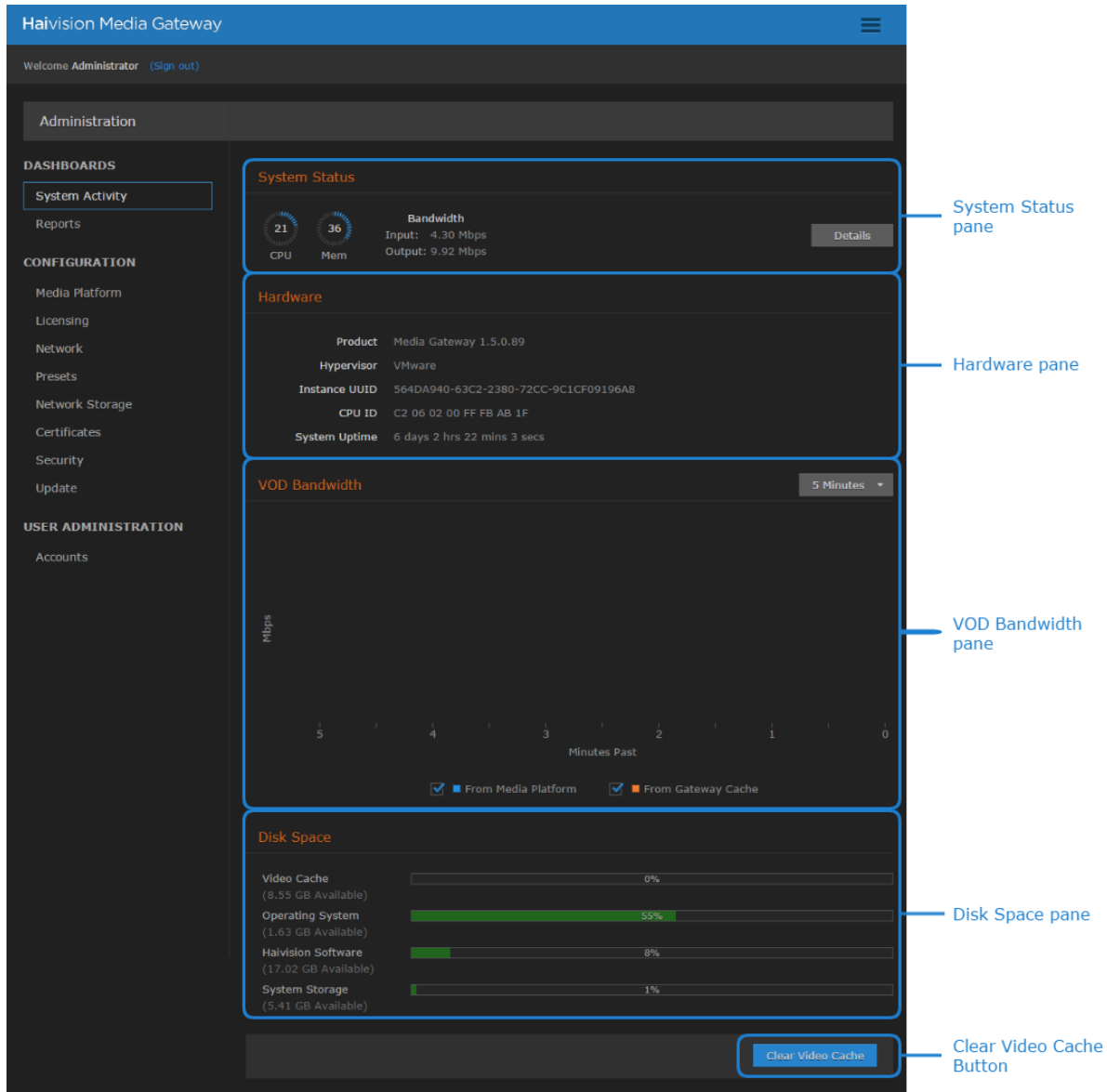
Media Gateway includes dashboards as a management tool to provide a quick view of the overall system health.

Viewing the System Activity Dashboard

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

To view the system's activity dashboard:

1. Click the  icon on the toolbar and click Administration. Click System Activity in the sidebar.
The System Activity dashboard appears.



The *System Status* pane provides the following information:

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

Clicking the **Details** button in the System Status pane opens a new browser window showing graphs of the network bandwidth and CPU and memory usage. 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.



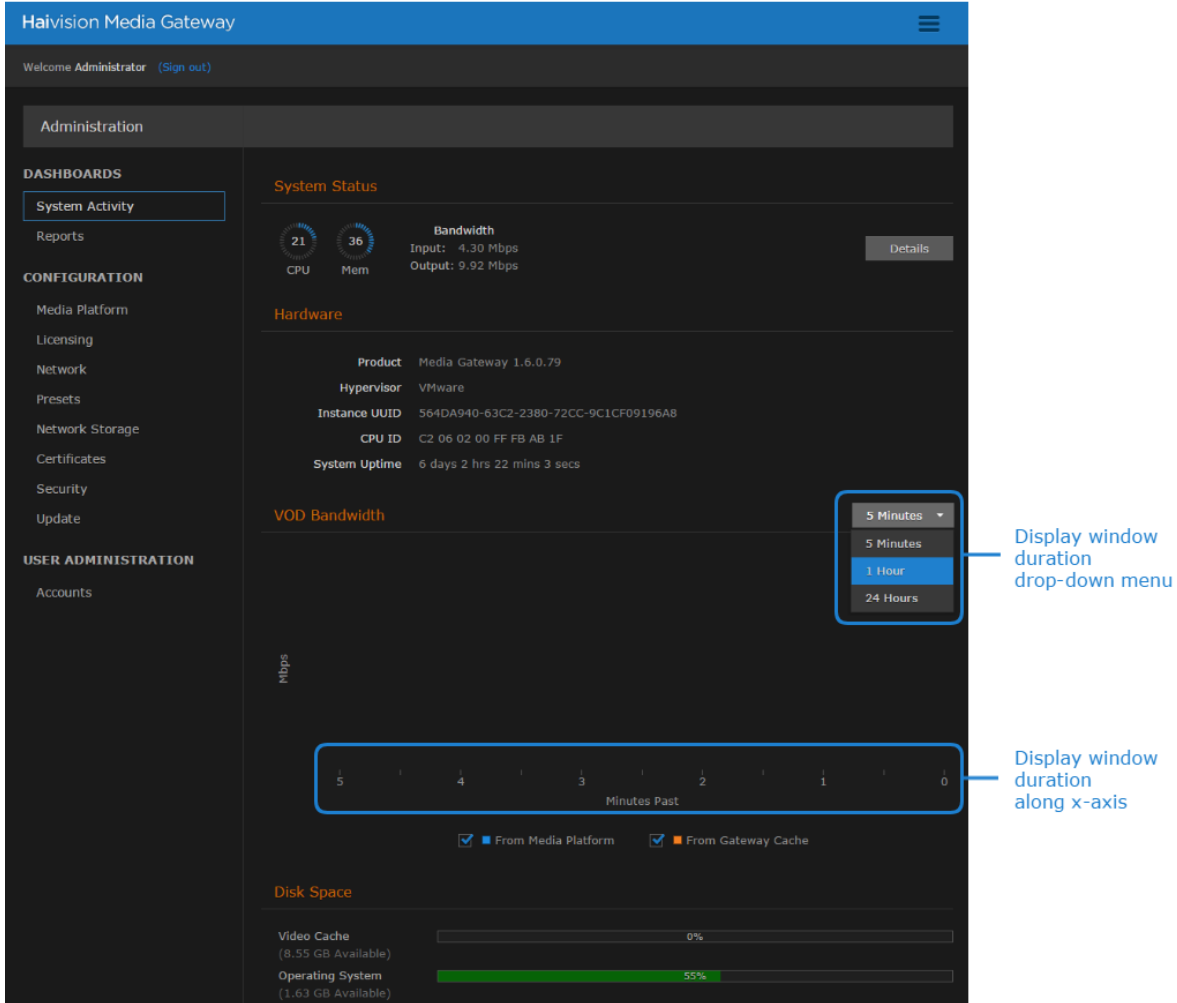
The Hardware pane provides the following information:

- Media Gateway version
- VMware information (if applicable)
- System uptime

When paired with a Haivision Media Platform, the VOD Bandwidth pane appears and charts usage in Mbps. The checkboxes below the graph allow you to tailor the display to include information from Media Platform, the cache, or both.

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

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




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

Disk Space	Corresponding Directory/Partition Location
Video Cache	If Network Storage is disabled (default), <code>/assets</code> . If Network Storage is enabled, NFS mount location.
Operating System	<code>/</code>
Haivision Software	<code>/opt</code>
System Storage	<code>/var</code>

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

Bar Color	Indicates Usage Threshold
●	0-74% of the space is in use. <i>Only 25% remains available.</i>
●	75-90% of the space is in use. <i>Only 10% remains available.</i>

Bar Color	Indicates Usage Threshold
	90-100% of the space is in use.

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](#)
- [Network Storage](#)
- [Viewing the Status of a License](#)
- [Downloading System Updates](#)
- [Viewing the Media Gateway Version Number](#)

Clearing the Video Cache

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

To clear the video cache:

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

Related Topics

- [Viewing a Route's Statistics](#)
- [Network Storage](#)

Reports (Logs)

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

Log Name	Description
All Logs	All system and application logs. Includes the Media Gateway logs and System messages.
System Messages	Operating system messages. Includes /var/log/messages.
Media Gateway	Log data from the Media Gateway processes. Including: <ul style="list-style-type: none"> • <code>madra_log_query</code> — logs from the past week. • <code>/opt/haivision/var/log/kulabyte</code> — KB Encoder logs, if present.

Enabling Diagnostic Logging

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

To enable logging:

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

! Important

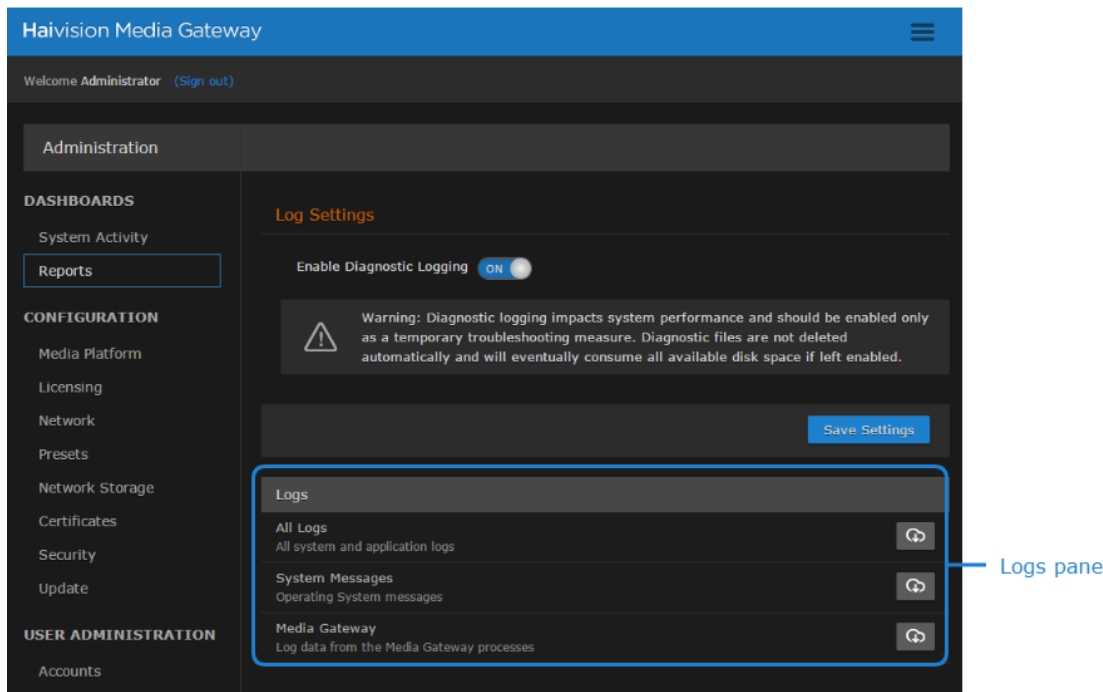
Diagnostic logging impacts system performance and should be enabled only as a temporary troubleshooting measure. Diagnostic files are not deleted automatically and eventually consumes all available disk space if left enabled.


Viewing Reports (Logs)

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

To view a log:

1. On the Administration screen, click **Reports** on the sidebar.
2. The view pane consists of the Logs pane.



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

```
Media_Gateway > opt > haivision > var > log
```

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

Related Topics

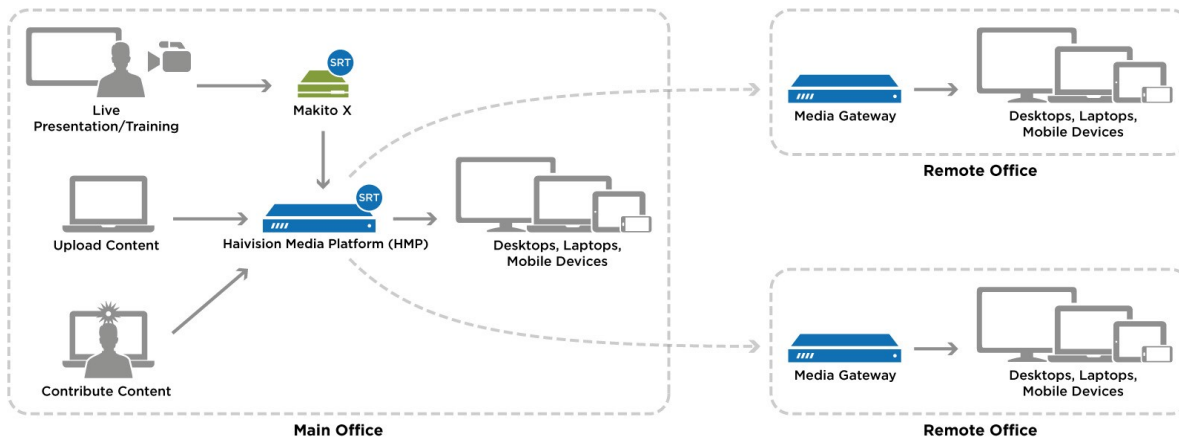
- [Viewing a Route's Statistics](#)
- [Viewing the Status of a License](#)
- [Downloading System Updates](#)

- [Viewing the Media Gateway Version Number](#)

Media Platform

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

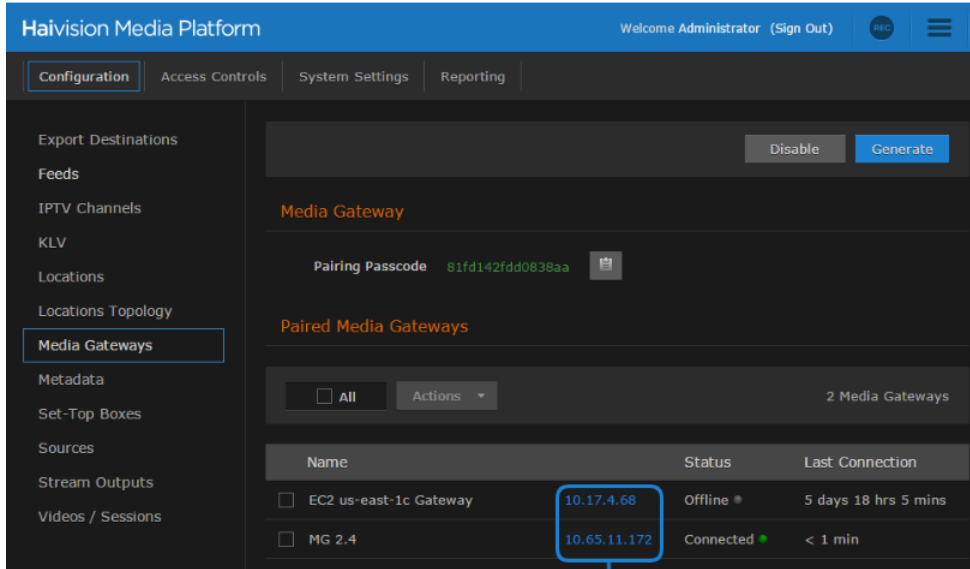
Use browser tabs to switch easily between the Media Platform server and Media Gateway interfaces.

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.



Action links open a tab to their corresponding Media Gateway

Acquiring a Pairing Passcode

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

To acquire the passcode:

1. In your Media Platform browser tab, click the icon and click **Administration**.
2. Click **Media Gateways** in the sidebar.
3. If the Pairing Passcode field is empty or disabled, click **Generate** to create a new pairing passcode.
4. Copy the pairing passcode to the clipboard.
5. Make note of the Media Platform address and port. If there is a cross-domain address, make a note of it as well.

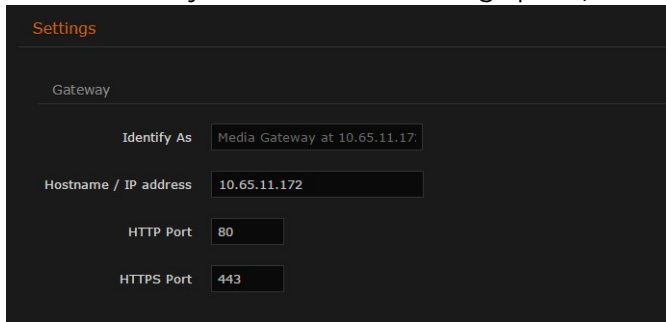
Pairing the Devices

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](#).

To pair the devices:

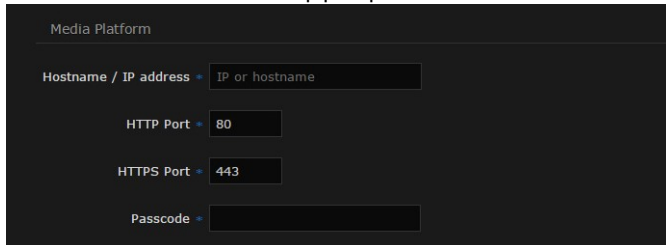
1. In your browser tab of the Media Gateway you wish to pair with the Media Platform, click the icon and click **Administration**.
2. Click **Media Platform** in the sidebar.

3. In the Gateway section of the Settings pane, enter the Media Gateway information as needed:



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

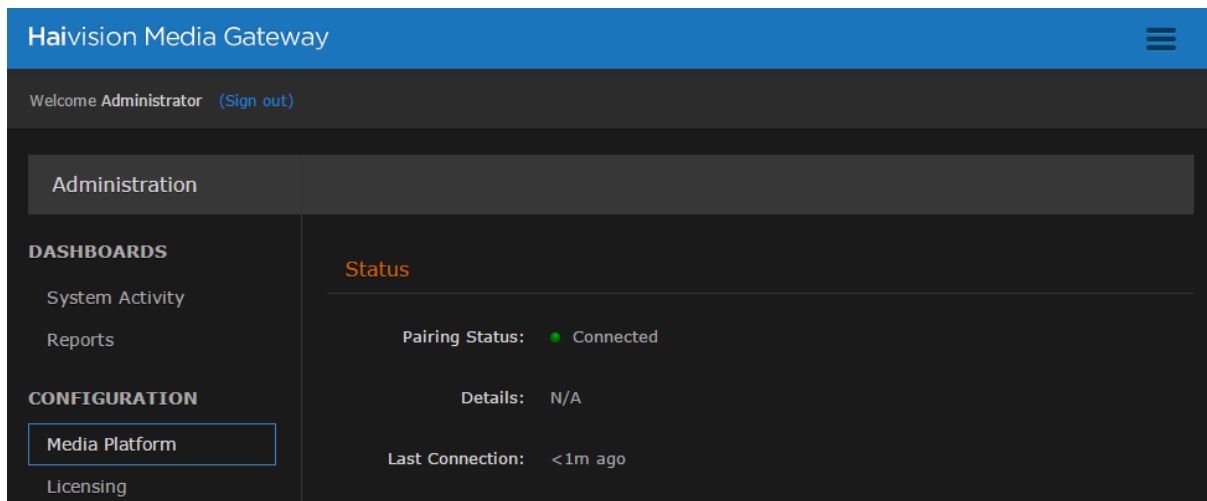
4. In the Media Platform section of the Settings pane, enter the Media Platform information that you noted earlier into the appropriate data fields:



- **Address** — the URL that the Media Gateway uses to connect with the Media Platform server; that is, the private (inside the firewall or VPN) IP/hostname for the Media Platform.
- **Cross-DomainAddress** — the address used to host the Media Platform to the end users; that is, the public-facing IP/hostname for the Media Platform. Typically only necessary when deploying.
- **HTTP Port**
- **HTTPS Port**
- **Passcode** — Paste the passcode from your clipboard into the Passcode field.

5. Click **Pair**.

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



Tip

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

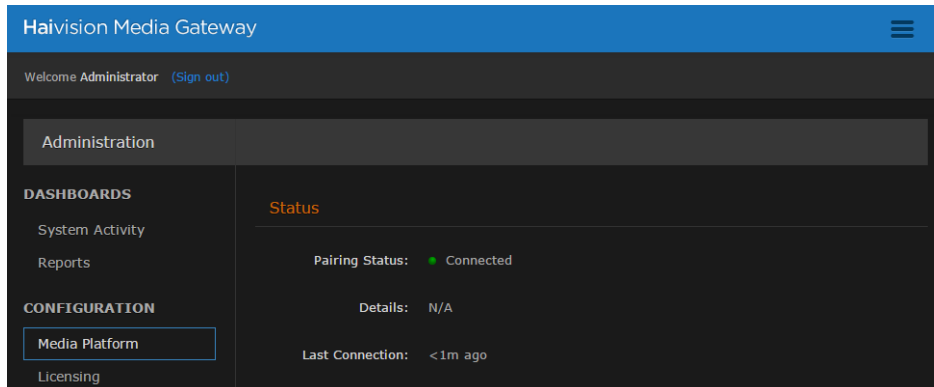
If the Pairing Status on the (Media Gateway) Media Platform screen displays the message "Pairing timeout", this may be an indication the Media Platform server is unavailable. Try the following:

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

Viewing the Status of Media Gateway Connections


To determine the status of a Media Gateway connection:

1. On the (Media Gateway) Media Platform screen, hover your cursor over the status icon or use the following color codes:
 - — Connected (Poll requested succeeded within the last 5 minutes).
 - — Warning (Pairing is pending, or some potentially transient error).
 - — Error (Last poll request failed due to authorization, 404, or pairing timeout).
 - — Disconnected (Last poll response was received over 5 minutes ago).
2. The Media Platform screen also tracks the connection’s duration in the Last Connection field.




Blocking New Media Gateway Connections

To block any new Media Gateway connections:

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

Updating the Media Platform Server


To update the Media Platform server:

1. In your Media Gateway browser tab, click the  icon and click **Administration**.
2. Click **Media Platform** in the sidebar.
3. Change one of the settings, such as update the "Identify As" name to something new.
4. Click **Update** 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 and the pairing status returns to "Not paired".

To clear the Media Platform server:

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

Disconnecting from a Media Platform Server

To disconnect from a Media Platform server:

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

Licensing

Important

Please contact Haivision Technical Support to obtain a valid license key if needed. 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 to the Media Gateway server requires administrator privileges and a license key.

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

Licensing Media Gateway

Note

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

1. After signing into the web interface, if you see a License Required dialog, click **Add License**.
-or-
Click the  icon, click **Administration**, and click **Licensing** in the sidebar.
2. Click the  icon to copy the current product details to the clipboard.
3. Contact Haivision Technical Support with this information to request a license key.
4. After you receive a license key, paste the license string in the License text box.
5. Click **Update** to load the license.

Note

For information on licensing, please refer to the *Media Gateway Administrator's Guide*.

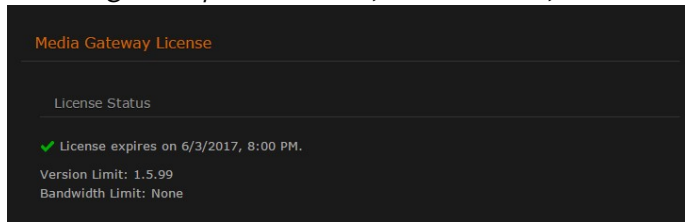
Adding a Media Gateway License

To license Media Gateway:

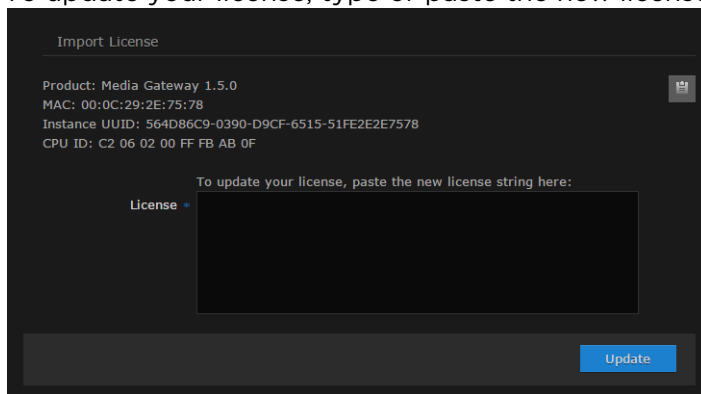
1. After signing into the web interface, if you see a License Required dialog, click **Add License**.
-or-

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

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




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



3. Click **Update** to load the license.

 **Tip**

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


Related Topics

- [Viewing the Status of a License](#)

Viewing the Status of a License

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

To view the status of a Media Gateway license:

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

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

Related Topics

- [Adding a Media Gateway License](#)

Viewing the Media Gateway Version Number

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

Option 1:


1. Click the  icon and click About Media Gateway.

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

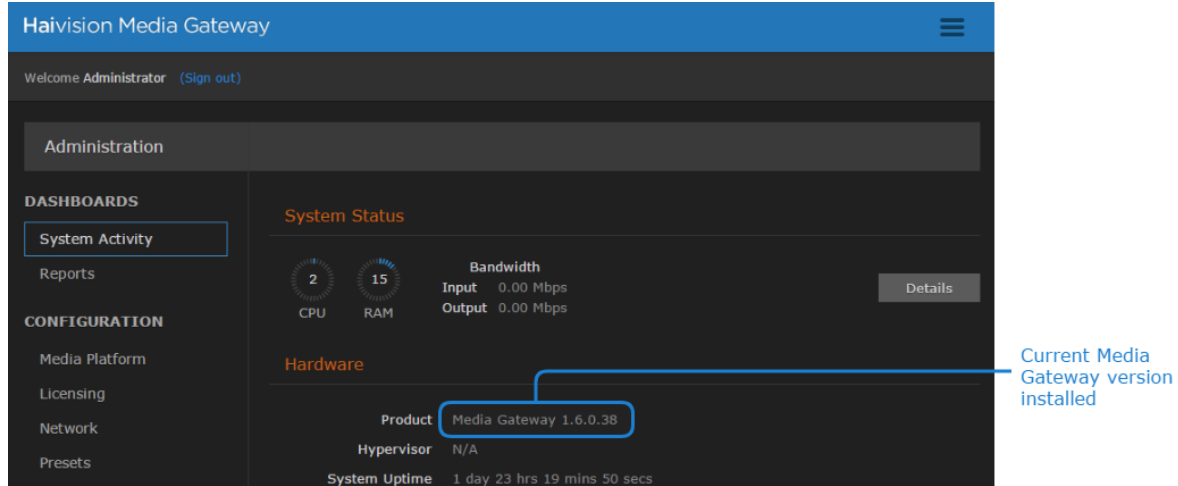


2. When finished, click **Close** to exit the dialog.


Option 2:

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

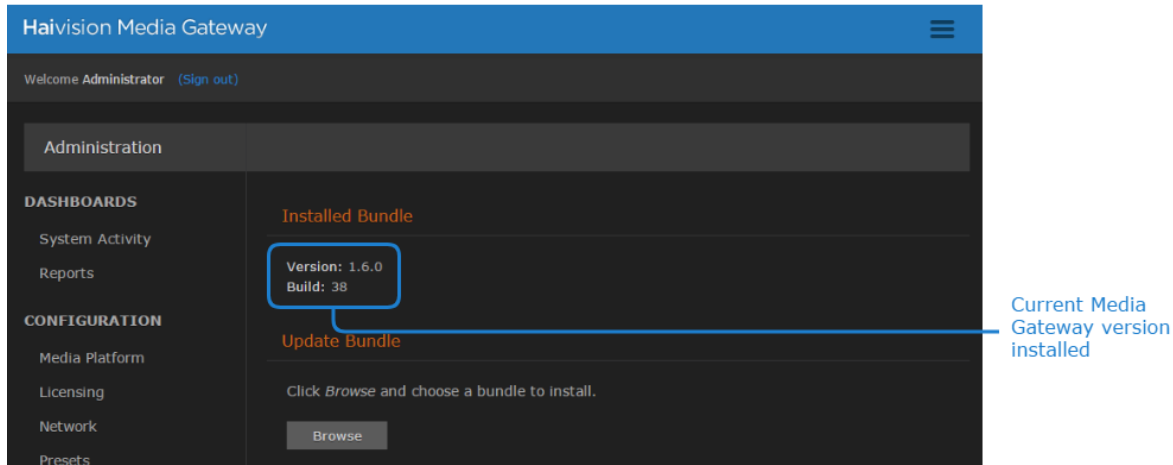
The Media Gateway version is listed under System Status.



Option 3:

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

The Media Gateway version is listed under Installed Bundle.



Related Topics


- [Downloading System Updates](#)
- [Installing/Updating a Package \(HaiBundle\)](#)

Network

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

Configuring the Network

To configure the network:

1. Click the  icon and click **Administration**.
2. Click **Network** in the sidebar menu.
The available network configuration settings are listed in the view pane along with Interfaces and Static Routes.
3. Fill in the fields as appropriate. See [Network Settings](#) for more information.
4. To configure multiple network interfaces, after you complete eth0, select the next interface (for example, eth1) and repeat the configuration.
5. To add a bond interface, see [Creating a Bonded Interface](#) for more information.
6. To add a Static Route, click **+Route** and provide the necessary data in the Add Static Route dialog.

The 'Add Static Route' dialog box is shown with the following fields and controls:

- Destination**: A text input field with a dropdown arrow on the left.
- Subnet Mask**: A text input field with a dropdown arrow on the left.
- Gateway**: A text input field.
- Interface**: A dropdown menu currently showing 'eth0'.
- Buttons**: 'Cancel' and 'Add Route' buttons at the bottom.

7. Click **Add Route**. The Static Route is added to the listings on the Network Configuration screen.

8. Click the **Save Settings** button.
9. Click the **Reboot** button to have your network configuration changes take effect.

Network Settings

Network Setting	Description
General	
Hostname	The hostname to be assigned to the Media Gateway. Specify the hostname as a fully-qualified domain name (FQDN). For example: myserver.mycompany.com
Default Interface	The default Ethernet interface is eth0.
DNS Servers	(Optional). The Internet Protocol version 4 (IPv4) address(es) of the Domain Name Server(s) to use.
Search Domains	(Optional). The search strings to use when attempting to resolve domain names.
NTP Server	(Optional). If the Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server.
SNMP	Enable/Disable Simple Network Management Protocol (SNMP).
Read-Only Community	SNMP string to be used when making read-only information requests.
SNMP Trap Servers	IPv4 or FQDN of a server to send SNMP traps to.
Interfaces	
eth0 eth1 eth2 ...	Allows for multiple interfaces. Select the appropriate tab to view and configure.
Bond Interface	Bonding enables an administrator to use more than one physical network port as a single connection. This can be used to increase performance or redundancy of a server.
Addressing	Choose whether the interface uses a static or dynamic IP address: <ul style="list-style-type: none"> • 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	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter an IP address in dotted-decimal format.</p> </div>
Subnet Mask	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.0.0).</p> </div>
Gateway	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter the gateway address in dotted-decimal format.</p> </div>


Network Setting	Description
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).
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. <ul style="list-style-type: none"> • Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance. • Active Backup: Only one NIC slave in the bond is active at a time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance. • XOR Sequential: Transmits based on XOR formula. (Source MAC address is XOR'd with destination MAC address). This mode selects the same NIC slave for each destination MAC address and provides load balancing and fault tolerance. • Broadcast - Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance. • IEEE 802.3ad Dynamic Link Aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification. This mode is similar to the XOR mode above and supports the same balancing policies. The link is set up dynamically between two LACP-supporting peers. • (Adaptive) Transmit Load Balancing (TLB): The outgoing traffic is distributed according to the current load and queue on each slave interface. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave. • (Adaptive) Active Load Balancing (ALB): This includes <i>balance-tlb + receive load balancing (rlb)</i> 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.
Static Routes	
Destination	Each static route requires a destination.
Subnet Mask	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.0.0).</p> </div>

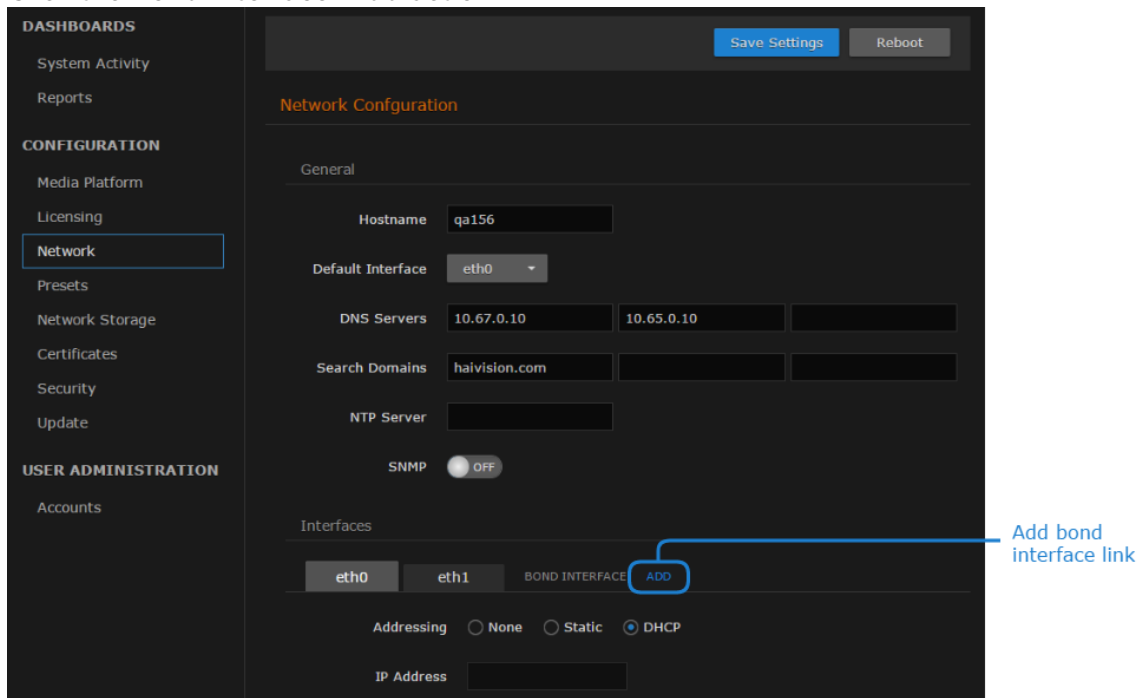
Network Setting	Description
Gateway	This is the gateway that is used when no other gateway matches. This address must be reachable on your local subnet. If DHCP is disabled, you may enter the gateway address in dotted-decimal format.
Interface	The interface associated with the static route. Use the drop-down menu to make your selection.

Creating a Bonded Interface

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

To create a bonded interface:

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



5. In the Default Interface drop-down menu, select **bond0**.
6. Click the **Bond0** tab to reveal the bonding-specific fields (such as Bonding Mode and Slave Interface). 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. Click the  icon and click **Administration**.


2. Click **Network** in the sidebar menu.
3. Verify that the correct bonded interface you wish to remove (for example, bond0) is currently selected.
4. Click the **Bond Interface: Remove** action link. The selected interface tab is removed.
5. Click the **Save Settings** button.
6. Click **Reboot** to have your changes take effect.

Presets

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


Exporting and Importing Presets

To export a preset:

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

The browser downloads a .hmg file.

To import a preset:

1. Click the  icon and click **Administration**.
2. Click **Presets** in the sidebar menu.
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
 - it must contain at least one route configuration
 - a route must have a source
 - route name, source name and destination name are required and route name must be unique
6. If an error occurs, an error message is displayed. If validation passes, then it starts applying the preset.
7. While the system is applying the preset, a message "Applying preset..." is displayed with a progress bar.
8. When complete, a message of "# routes created" is displayed.

Network Storage

Network Storage is a licensed option that enables you to use a Network-Attached Storage (NAS) device to host the Media Gateway's video cache through a Network File System (NFS) connection.

Important

The NFS share must be hosted on a dedicated disk or partition to ensure that HMG can control disk utilization.

Note


For more information on obtaining a license for the Network Storage option, please contact Haivision Sales.

Enabling Network Storage

Note

The NFS server must be configured on your network storage host before connecting to it on the Media Gateway.


To enable network storage:

1. Click the  icon and click **Administration**.
2. Click **Network Storage** in the sidebar.
3. Toggle the NFS button to **On**.
4. Fill in the remote host IP address and path.
5. To test the connection from HMG to the defined NFS server, click **Test Settings**.
6. Click **Save Settings** to save the connection.
7. Click **Reboot** to restart the Media Gateway for the new settings to take affect.

After the reboot, any newly cached video segments are stored on the remote NFS server instead of locally on the Media Gateway.

Disabling Network Storage

To disable network storage:

1. Click the  icon and click **Administration**.
2. Click **Network Storage** in the sidebar.
3. Toggle the NFS button to **Off**.
4. Click **Save Settings** to save the connection.
5. Click **Reboot** to restart the Media Gateway for the new settings to take affect.

After the reboot, the video cache is stored locally on the Media Gateway.

Related Topics

- [Viewing the System Activity Dashboard](#)
- [Clearing the Video Cache](#)

Certificates


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

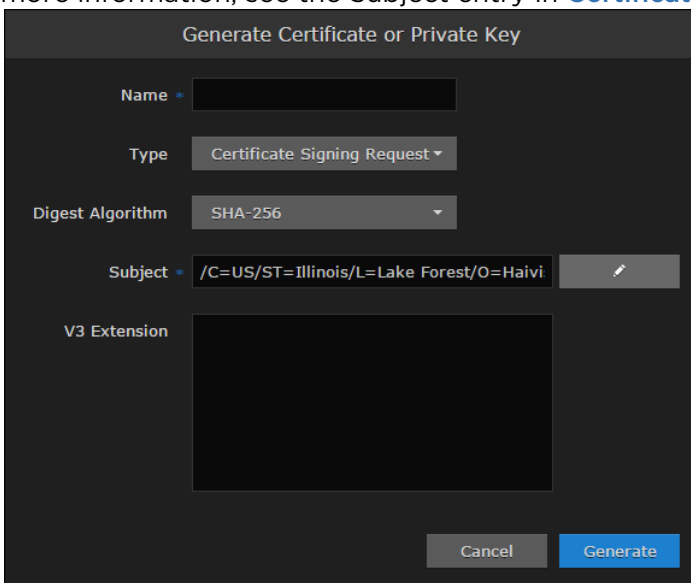
The Certificates page lists the Identity Certificates available on Media Gateway. An Identity Certificate identifies the device during the authentication process when trying to establish a TLS connection in HTTPS session startup. Its Common Name or Alternate Subject Names must match its IP address and/or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

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

Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR):

1. Click the  icon and click **Administration**.
2. Click **Certificates** in the sidebar.
The Certificates page lists any certificate signing requests generated on Media Gateway. The active certificate is indicated with a blue check.
3. Click the **Generate** button.
4. On the Generate Certificate or Private Key dialog:
 - a. Type in a name for the certificate.
 - b. Make sure the Type is Certificate Signing Request and fill in the remaining fields. See [Certificate Settings](#).
 - c. For the subject, type in information about the device that the Identity Certificate represents. For more information, see the Subject entry in [Certificate Settings](#).



5. Click the **Generate** button.

 **Note**

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


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

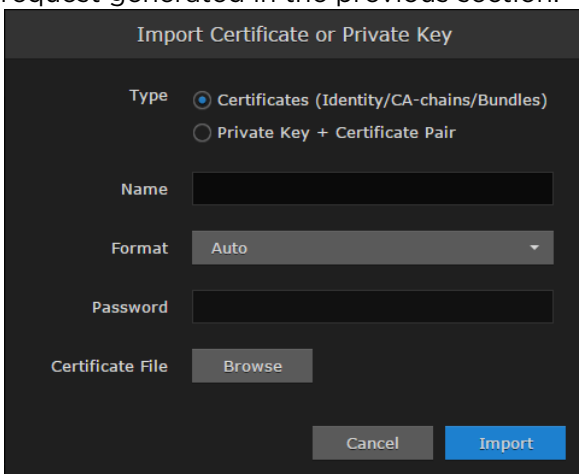
 **Tip**

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

Importing and Activating a Certificate

To import and activate a certificate:


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



5. Click **Import**.
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** if you have changed the active certificate.

Generating and Importing a Private Key

To generate a private key:

1. Click the  icon and click **Administration**.
2. Click **Certificates** in the sidebar.
3. Click the **Generate** button.
4. On the Generate Certificate or Private Key dialog:
 - a. Type in a name for the certificate.
 - b. For the Type, select **Self-Signed**.
 - c. Check the **Create New Private Key** checkbox.

d. Fill in the remaining fields. See [Certificate Settings](#).

5. Click **Generate**.

⚠ Caution

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

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

7. Click **Reboot**.

To import a Private Key:

1. Click the icon and click **Administration**.
2. Click **Certificates** in the sidebar.
3. Click the **Import** button.
4. On the Import Certificate or Private Key dialog:
 - a. For the Type, select **Private Key + Certificate Pair**.
 - b. Type in the password for the private key.
 - c. To update your security certificate, click **Browse** and select the new SSL Certificate and SSL Certificate (Private) Key, and optionally an SSL Intermediate Certificate Bundle file.

5. Click **Import**.
On the Certificates page, the newly imported files are added to the list.
6. Click **Reboot**.

Certificate Settings

Note

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

Certificate Setting	Description
Generate Certificate or Private Key	
Name	Type in a unique name under which the certificate will be stored on the Media Gateway as well as listed on the Certificate page.
Type	<p>Select the Signature Type:</p> <ul style="list-style-type: none"> • Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates. • Certificate Signing Request: A request will be generated, and its name will be added to the list of Identity Certificates. The request will be located in your home directory (accessible through the CLI), or you may export it by clicking on the View button and copying the content into a new file in a text editor. <p>In its generated form, this certificate is still a request and cannot be used as an Identity Certificate before it is signed by a CA, and imported back.</p>
Digest Algorithm	<p>Select the digest algorithm (Secure Hash Algorithm):</p> <ul style="list-style-type: none"> • SHA-256 • SHA-384 • SHA-512
Subject	<p>The Subject identifies the device being secured, in this case, the Media Gateway.</p> <p>The special value "auto" used with Generate sets the Subject Common Name to the device's FQDN if DNS is set, or the IP address otherwise. Also, for self-signed certificates, the Subject Alternative Name extension is also set to FQDN, hostname, and IP Address of the device (there is no other method to set the Subject Alternative Name).</p> <p>Type in the subject in the form: <code>"/C=US/ST=Maine..."</code> where the most common attributes are:</p> <ul style="list-style-type: none"> • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Tip</p> <p>For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device.</p> </div>
V3 Extension	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	


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

Security

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

- **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.
- **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.

To configure appliance security:

1. Click the  icon and click **Administration**.
2. Click **Security** in the sidebar menu.
3. To configure Media Gateway for use in a high-security environment, toggle the **High Security (STIG) Environment** button to On.
4. To configure a banner, toggle the **Advisory Notice** button to On, and enter the desired banner text in the Message textbox
5. Click the **Save Settings** button.
6. Click the **Reboot** button to have your security configuration changes take effect.

Update

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 Upgrades** link.
3. Download the Media Gateway upgrade package you wish to install.
4. Save the selected .zip file to your local computer or network.
5. Extract the update file from the .zip file using a zip file utility.

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

Related Topics

- [Viewing the Media Gateway Version Number](#)
- [Viewing the Status of a License](#)
- [Installing/Updating a Package \(HaiBundle\)](#)


Installing/Updating a Package (HaiBundle)

Updates are provided via a HaiBundle. You can find the latest HaiBundles in the Support Portal as described in [Downloading System Updates](#).

Note

Your system restarts after it installs the updates.

To install a HaiBundle:

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

Related Topics

- [Downloading System Updates](#)

Accounts


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

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

Viewing the Available User Accounts

User account information includes the name and role.

To view the available user accounts:

1. Click the  icon and click Administration.
2. Click **Accounts** in the sidebar.


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

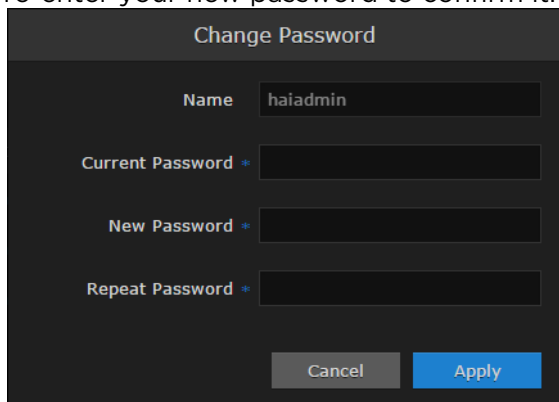
Field	Value
Account Name	The user name for the account. Built-in accounts set up at the factory include: <ul style="list-style-type: none"> • haiadmin — Built-in Administrator account. • haioperator — Built-in Operator account. • haiobserver — Built-in Observer account
Role	The role assigned to the account. Roles for built-in accounts are read-only. Available roles include: <ul style="list-style-type: none"> • Administrator — All access rights and administrator privileges. • Operator — All rights to create and configure routes. Does not include rights to the Administration page. • Observer — Read-only access to the system. Does not include the rights to the Administration page.

Changing an Account's Password

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

To change an account password from the web interface:

1. Click the  icon on the toolbar and click **Administration**.
2. Click **Accounts** from the sidebar.
3. Click the **Account Name** whose password you want to change.
4. When the Change Password dialog opens, enter your current password and a new password. Then re-enter your new password to confirm it.



5. Click **Apply**.

Note

The `haiadmin` password can also be changed in the Console UI. See [Changing the haiadmin Password](#) for details.

The `hvroot` password can only be changed in the Console UI. See [Changing the Current User's Password](#) for details.

Related Topics

- [Viewing the Available User Accounts](#)

- Changing the haiadmin Password
- Changing the Current User's Password

Using the Console UI

Note

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

Topics Discussed

- [Accessing the Console UI](#)
- [Showing General Information](#)
- [Editing Network Settings](#)
- [Testing the Network Settings](#)
- [Viewing System Logs Available through the Console UI](#)
- [Changing the Current User's Password](#)
- [Changing the haiadmin Password](#)
- [Opening a Console UI Terminal Window](#)
- [Setting the Clock](#)
- [Setting the Timezone](#)
- [Rebooting or Shutting Down](#)
- [Logging Out of the Console UI](#)

Accessing the Console UI

Accessing the appliance Console UI requires administrator privileges and password.

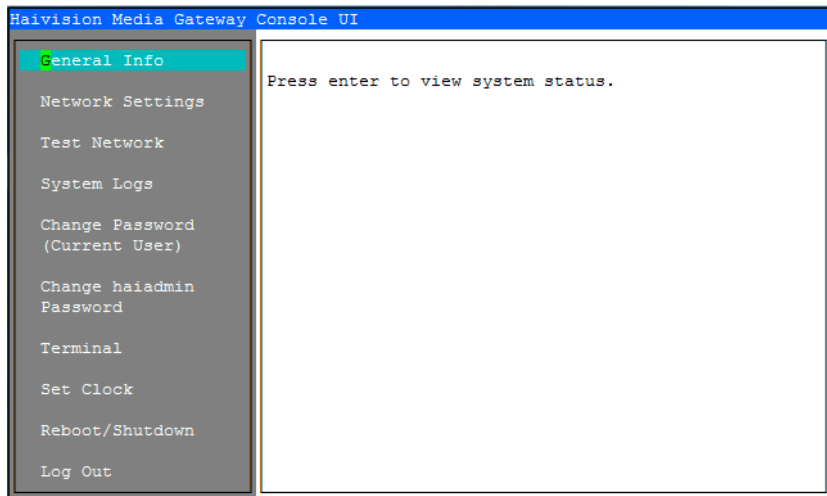
To access the Console UI:

1. Connect a keyboard and monitor to the appliance, if applicable, and boot the appliance.
or
Initiate a Secure Shell (SSH) connection to the IP address of the server using an SSH client (for example, PuTTY).
2. Log in using the `hvroot` username and password. Refer to the *Important Notice* document that accompanied your device for the default password.

Note

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

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



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

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

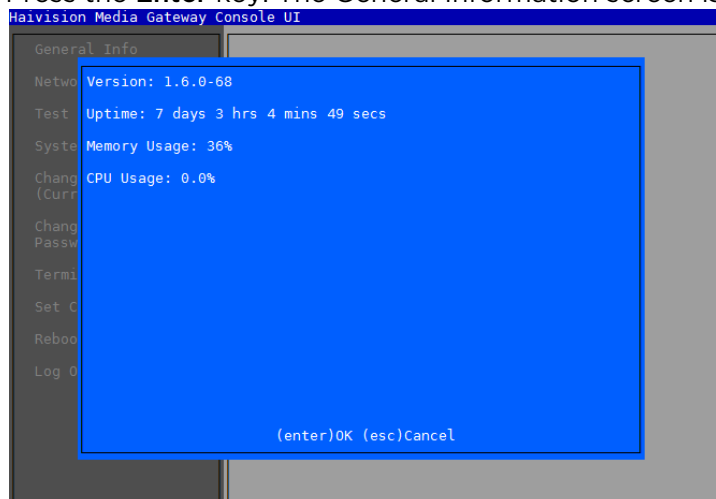
Showing General Information

Note

This is a read-only screen.

To show the current system status:

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



3. When you are finished reviewing the information, press **Enter** or **Esc** to exit to the main screen.

Related Topics

- [Accessing the Console UI](#)
- [Logging Out of the Console UI](#)

Editing Network Settings

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

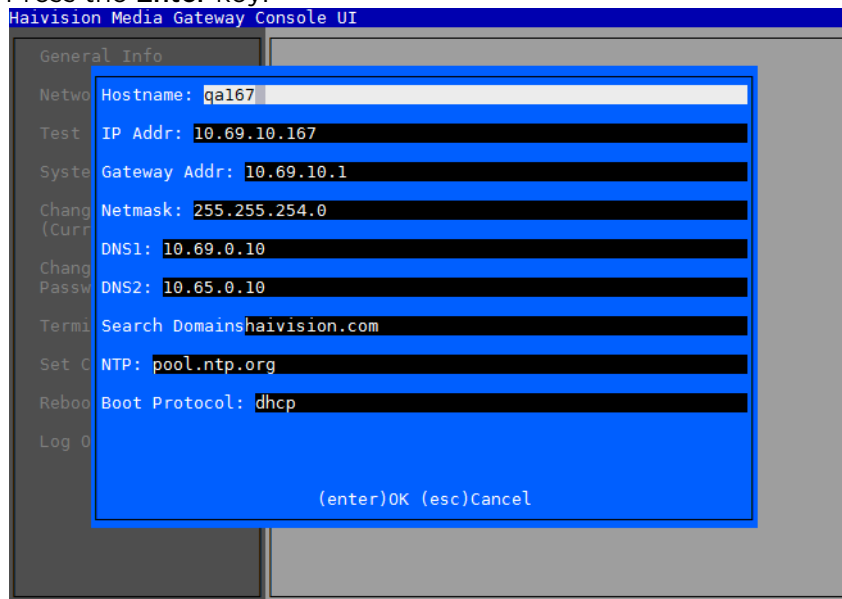
- Hostname
- IP Address
- Gateway Address
- Netmask
- DNS Server Address 1
- DNS Server Address 2 (Must be set to a valid DNS address. Can use DNS1 if only one DNS server is available)
- Search Domains
- Network Time Protocol (NTP) Server Address (*optional*)
- Boot Protocol (DHCP or Static)

Note

These settings can also be changed in the web interface. See [Configuring the Network](#) for details.

To change network settings:

1. In the navigation sidebar, use the $\uparrow\downarrow$ (up and down arrow) keys to highlight **Network Settings**.
2. Press the **Enter** key.



3. To change a setting:
 - Use the Tab or $\uparrow\downarrow$ (up and down arrow) keys to navigate to the field you want to change.
 - Use the Delete/Backspace key to delete the existing contents and then type in your modifications.
4. When finished editing the information, press **Enter** to save your changes and exit to the main screen. Or, press the **Esc** key to exit without saving any changes.

Related Topics

- [Testing the Network Settings](#)

- [Configuring the Network](#)

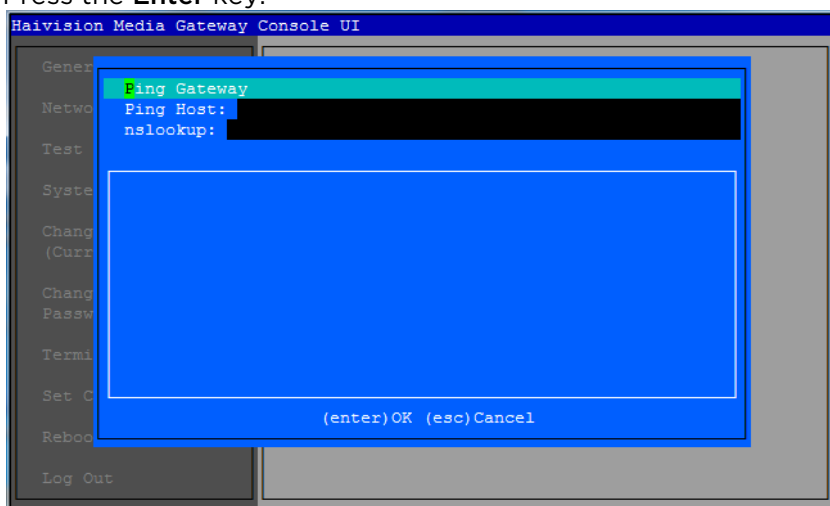
Testing the Network Settings

Tip

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

To test the network settings:

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

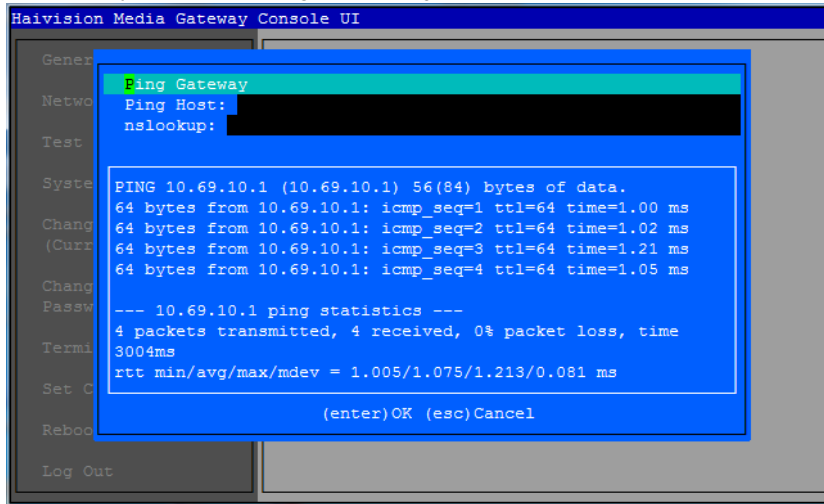


3. The Test Network screen provides four possible network setting tests:

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

4. To perform a network test:
 - Use the **Tab** or ↑↓ (up and down arrow) keys to navigate to the test you want to perform.
 - In the text entry field for your selected test, use the Delete/Backspace key to delete any existing contents, then type in your modifications, and press **Enter**.

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



5. When finished, press **Esc** to exit to the main screen.

Related Topics

- [Editing Network Settings](#)

Viewing System Logs Available through the Console UI

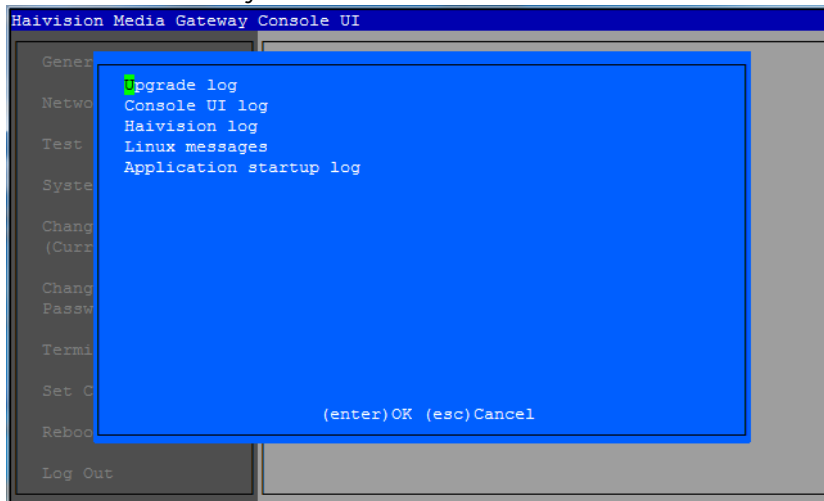


Tip

System logs are also accessible via the Media Gateway web interface. See [Viewing Reports \(Logs\)](#) for details.

To view a system log:

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



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

Log	Description
Upgrade Log	Provides log entries regarding installations, packages, plugins, and so forth.
Console UI Log	Provides log entries console sessions, authentications, boot protocol, and the like.
Haivision Log	Provides log data.
Linux Messages	Provides kernel messages regarding initialization, process, commands, among other things.
Application Startup Log	Provides information regarding application startup.

- To review a particular log, use the **Tab** or $\uparrow\downarrow$ (up and down arrow) keys to navigate to the log you want to view.
- Press **Enter**, and the log file is displayed on the screen.
- When finished, press **Esc** to exit to the main screen.

Related Topics

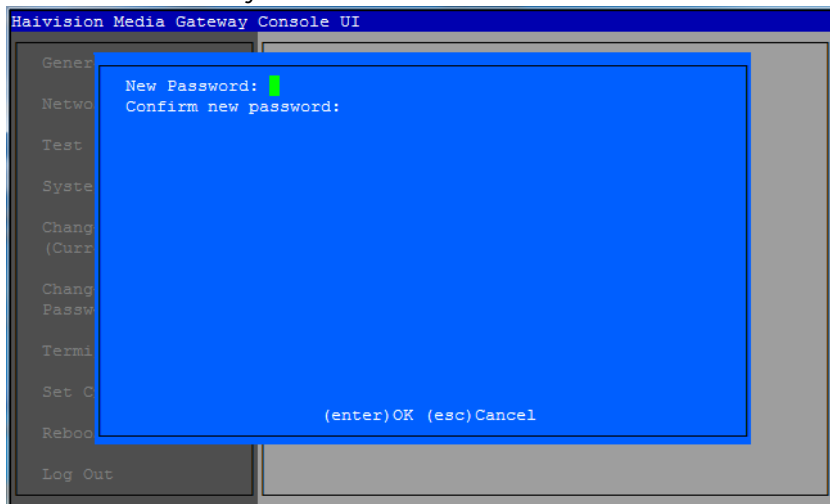
- [Viewing Reports \(Logs\)](#)

Changing the Current User’s Password

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

To change the password for the current user:

- In the navigation sidebar, use the $\uparrow\downarrow$ (up and down arrow) keys to highlight **Change Password (Current User)**.
- Press the **Enter** key.



- Type in the new password.
- Press **Tab** or the $\uparrow\downarrow$ (down arrow) and type the password again in the Confirm new password line.
- Press **Enter**. Upon success, the prompt confirms that the password has been changed and then returns to the main screen.

Related Topics

- [Accessing the Console UI](#)

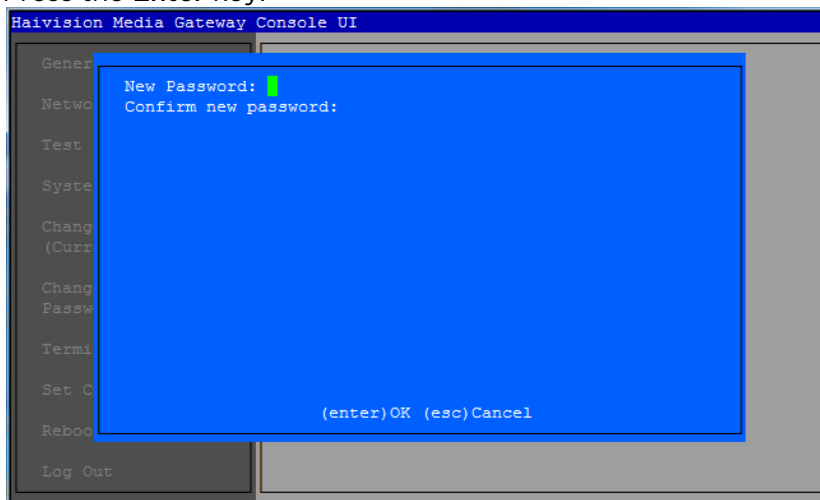
Changing the haiadmin Password

Tip

The haiadmin password can also be changed in the Media Gateway web interface. See [Changing an Account's Password](#) for details.

To change the haiadmin password:

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



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

Related Topics

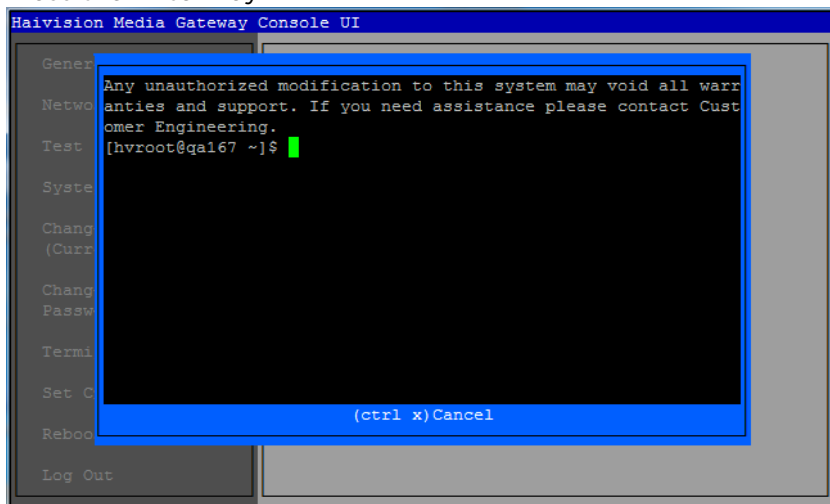
- [Changing the Current User's Password](#)

Opening a Console UI Terminal Window

To open a terminal window:

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

2. Press the **Enter** key.



3. When the bash shell opens, enter your commands.
4. When finished, press **Ctrl+x** to exit to the main screen.

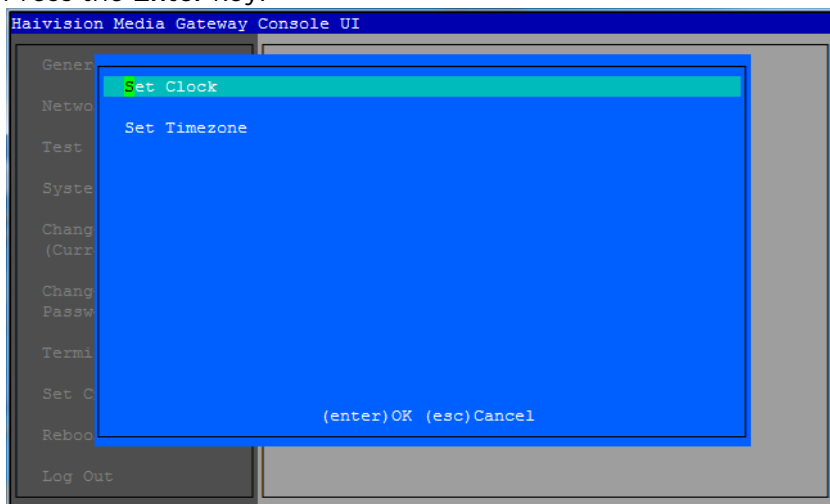
Related Topics

- [Accessing the Console UI](#)
- [Logging Out of the Console UI](#)

Setting the Clock

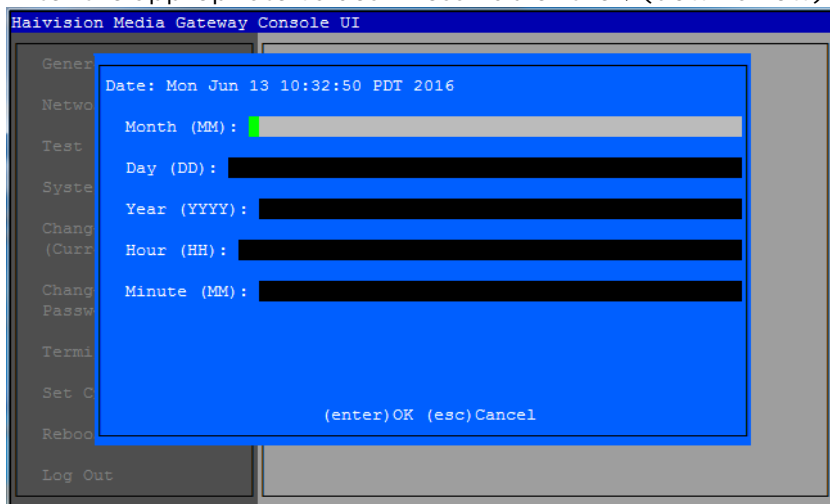
To change the time and date:

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



3. Press **Enter** again to select **Set Clock**.

4. Enter the appropriate values. Press **Tab** or the ↓ (down arrow) to move between the fields.



5. Press **Enter** to set the new time and date.

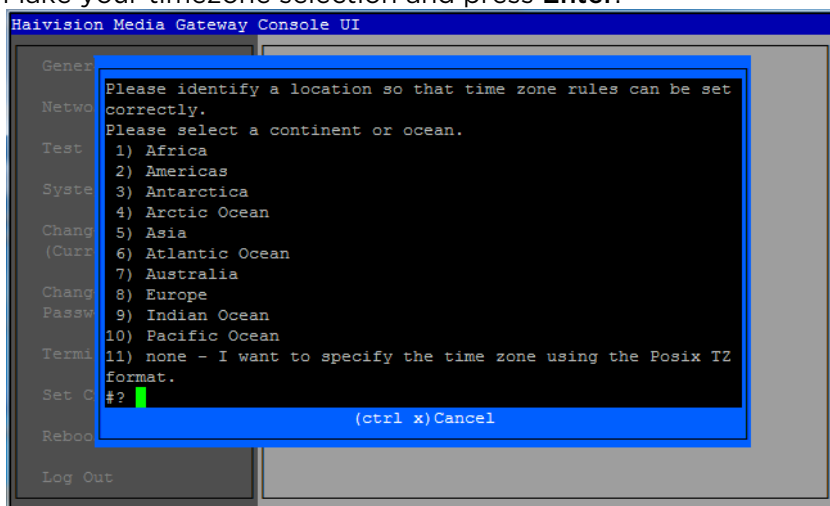
Related Topics

- [Setting the Timezone](#)

Setting the Timezone

To change the timezone:

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



Note

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

```
TZ = local_timezone +/- hours to UTC
```

For example, TZ='CST-6'

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

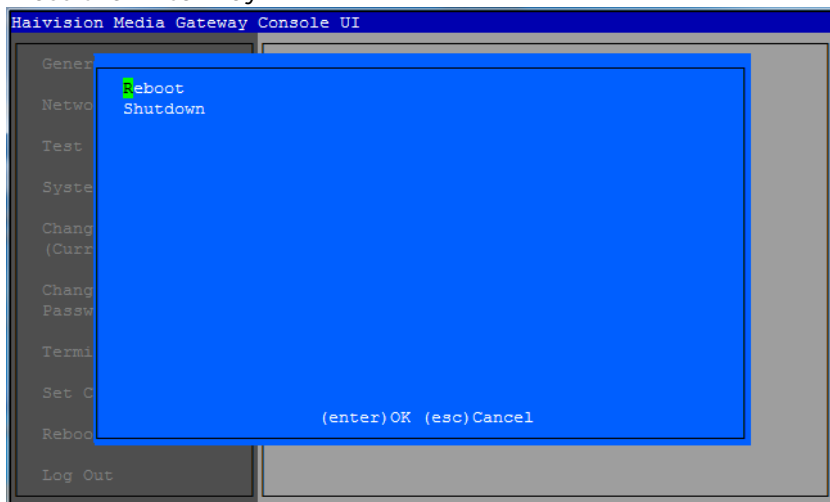
Related Topics

- [Setting the Clock](#)

Rebooting or Shutting Down

To reboot or shut down:

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



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

Note

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

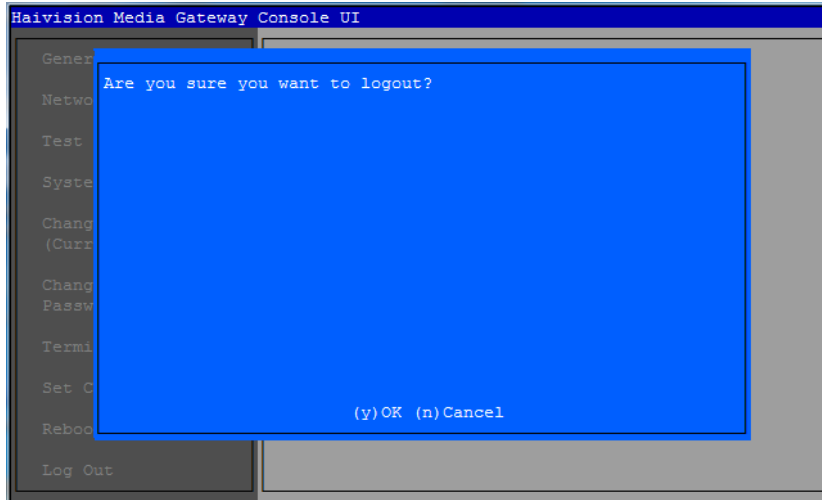
Related Topics

- [Accessing the Console UI](#)

Logging Out of the Console UI

To log out of the Console UI:

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



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

After logging out, you are redirected to the login screen.

Related Topics

- [Accessing the Console UI](#)

Troubleshooting

Known Issues and Solutions

To view a list of additional known issues, solutions, and recommended practices, visit: <https://support.haivision.com>

Erratic Behavior after a Recent Update

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

Cannot start the Web-Based Interface

- To start the web-based interface, in your browser enter the *base URL*. For example: `http://127.0.0.1`

The Web-Based Interface Sign-in isn't Working

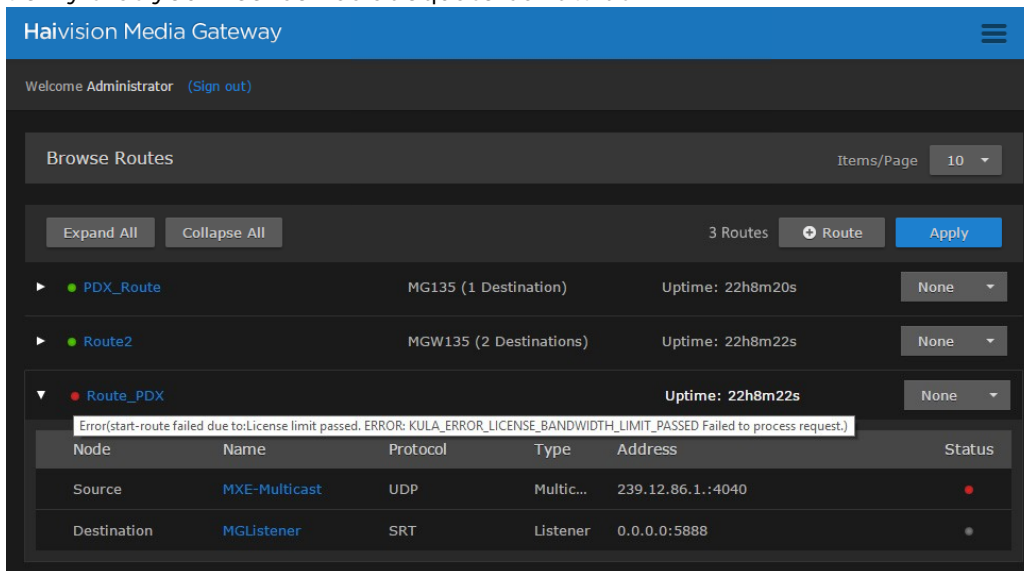
- Ensure the Caps Lock key is not On.
- Ensure that you have cookies enabled in your browser.

Identifying your Software Version from the Interface

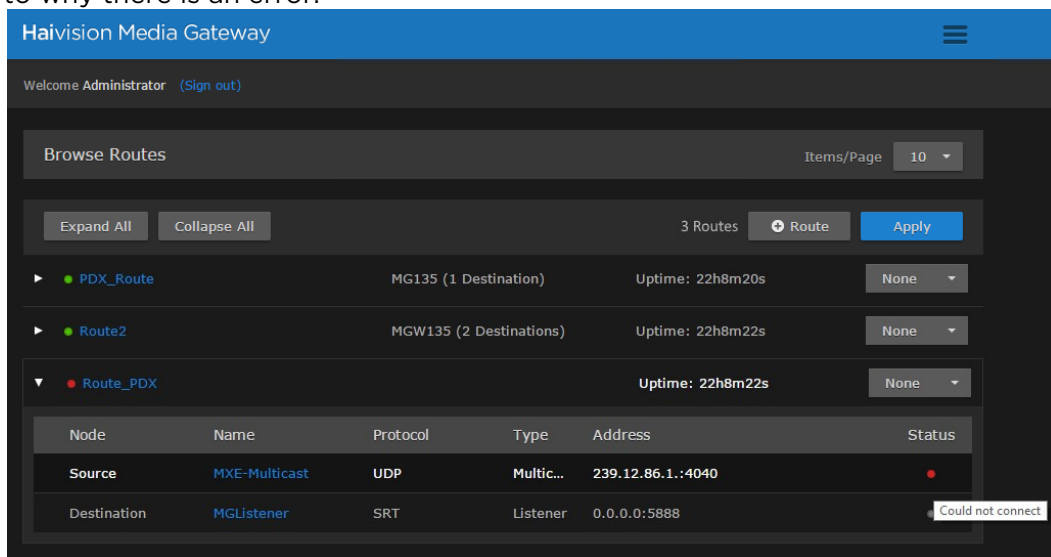
- To view the current release number for your Media Gateway installation, click the  icon and select **About Media Gateway**.

Status Indicator is not Green

- Verify that your license has adequate bandwidth.



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



Error Message states Failed to receive segment_cross domain request denied

- Verify that you have entered the cross-domain address correctly. See [Pairing the Devices](#).

Warranties

1-Year Limited Hardware Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

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

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

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

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

OBTAINING WARRANTY SERVICE

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

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

APPLICABLE LAW

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

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

EULA - End User License Agreement

READ BEFORE USING

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

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

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

SLA - Service Level Agreement

1. Introduction

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

2. Definitions

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

3. Service Levels for the Video Content Management System

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

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

4. Exceptions to Availability for the VCMS

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

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

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

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

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

5. Credits for Downtime for the VCMS

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

6. Support Services for the VCMS

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

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

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

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

7. Service Levels for Haivision Streaming Media Service

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

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

Agents and Polling Frequency

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

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

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

8. Credits for Outages of Haivision Streaming Media Service

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

9. No Secondary End User Support

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

Getting Help

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

