HAIVISION

Kraken Encoder/Transcoder
User's Guide

HVS-ID-UG-KRAK-310, Issue 01

Edition Notice

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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

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

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

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

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

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

Obtaining Documentation

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

Getting Service Support

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

This guide describes how to set up, configure, and manage Kraken to encode and transcode live HD video.

For information on installing and connecting to your Kraken appliance or cloud platform, refer to **Quick Start Guides**.

> ⚠ **Important**
>
> Before proceeding, please familiarize yourself with the **Safety Guidelines** in the **Installation Guide** and **Waste Electrical and Electronic Equipment (WEEE) Disposal** notice in the **Preface** (available at **https://doc.haivision.com**).

Introduction

This section provides a brief overview of Haivision's Kraken H.264/HEVC Video Encoder/Transcoder, along with a description of the main hardware components for the appliance.

Topics Discussed

- **What's New for 3.10**
  - **Version History**
- **Product Overview**
  - **Key Capabilities**
- **Kraken Features**
  - **Audio/Video Characteristics**
  - **Transport Characteristics**
  - **SRT (Secure Reliable Transport)**
  - **Console User Interface**
  - **IPv4 and IPv6 Support**
- **Deployment Options**
  - **Kraken Server**
  - **Kraken CR**
  - **Kraken Edge**
  - **Cloud-Based Deployments**
- **Physical Description (Kraken Server)**
  - **System Interfaces**

What's New for 3.10

Kraken v3.10 introduces the following features and enhancements:

- **RTSP Server Support**: Kraken Outputs now supports RTSP streaming for PUSH (send to client) and PULL (Kraken as an RTSP server) modes for compatibility with Video Management Systems (VMS) such as Milestone and Genetec.
  See **RTSP Server Service** and **Configuring RTSP Outputs**
- **IPV6 Support:** Kraken now supports both IPV4 and IPV6 networking and streaming services.
  See **IPv4 and IPv6 Support** and **Configuring Network Settings**
- **HTTP MJPEG Input Support**: Kraken now supports MJPEG video inputs over HTTP and HTTPS for low-latency streaming of camera or AI workflows.
  See **Configuring Inputs** and **Input Settings**

Version History

Kraken v3.9 introduced the following features and enhancements:

- **Network Device Interface (NDI) Input** — Kraken now supports discovery and use of NDI sources on a local network for encoding.
  See Configuring Input Parameters and Input Settings
- **HLS Output** — HTTP Live Streaming (HLS) is a supported output format for bypass streams in MPEG2TS format and is compatible with h.264 encoded streams. An HLS preview player is included within Kraken for admin troubleshooting.
  See Configuring Output Parameters, HLS Live Preview, and Output Settings

Kraken v3.8 introduced the following feature and enhancement:

- **wolfSSL Integration Changes** - wolfSSL allows Kraken appliances to support FIPS cryptographic requirements. The use of wolfSSL is available in version 3.8, but is disabled by default. To manually enable the wolfEngine within Kraken, please contact your Haivision account representative, or our technical support team at tickets@haivision.com.

Kraken v3.7 introduced the following features and enhancements:

- **Security Improvements** — Corrective action to resolve identified security issues affecting certification. Including:
  - **Account Lifecycle —** Core features include:
    - Locking accounts upon multiple failed login attempts
    - Disabling accounts after login inactivity
    - Allowing Administrators to disable accounts from Active or Locked account states, as well as enable accounts from Locked or Disabled account states
    - Prompting users to change password when nearing expiration
    - Allowing administrative adjustment of account settings via configuration file
    - Logging account events including creation, modification, disabling, enabling, and removal
  - **User Sessions —** Core features include:
    - Enforcing security flags on cookies
    - Limiting the number of concurrent login sessions
    - Enforcing logout upon idle timeout
    - Clearing client session data upon logout
    - Allowing administrative adjustment of session settings via configuration file
    - Logging user session events
  - **Password Lifecycle —** Core features include:
    - Enforcing password complexity for length and character types
    - Enforcing a minimum number of character changes between successive passwords
    - Preventing reuse of old passwords over a configurable period
    - Enforcing a minimum and maximum password lifespan
    - Allowing administrative adjustment of password settings via configuration file
    - Logging password creation and modification events
    See Password Requirements.

    > ✅ **Tip**
    >
    > For details on administrative adjustment of account, session, and password settings via configuration file, please contact your Haivision representative.

- **Reverse-Path Filter** — Kraken now has Reverse-Path filtering (a Linux Kernel feature, defined in RFC 3704, designed to ensure that packets that are not routable are dropped). Reverse path

filtering drops packets with source addresses that should not have been able to be received on the interface they were received on. Two options are available: Strict or Loose . See **Managing Security Policies** .

- **Configure Webserver to use specific Network Interface** — Kraken has multiple physical interfaces that are intended to provide redundancy and bandwidth, not network segregation. Because of this, the system will listen on all available physical interfaces regardless of IP address and respond to web requests. This new feature allows configuration of the web server to listen on a specified IP address and port . See **Enabling and Disabling Services**.
- **Introduction of Bypass Licensing** — Kraken Bypass Streams can now be licensed and counted separately from Kraken Transcode Streams. This follows introduction of stream-based licensing in Kraken 3.6 which adjusted how the Kraken runtime stream capacity related to license limits for any stream type (Bypass or Transcode). See **Status Settings** .
- **Deprecate v1 API** — The legacy v1.0 REST API is now deprecated. See **Kraken API v2.0 Integrator's Guide** for information on the v2.0 REST API.
- **Update Webserver Host** — Kraken 3.7 has retired usage of Apache and 32-bit libraries in favor of NodeJS-based microservices.
- **Security Audit** — Kraken 3.7 addresses known vulnerabilities discovered through security scans during development.

Kraken v3.6.1 introduced the following features and enhancements:

- **Configurable Program Clock Reference (PCR)** — Kraken 3.6.1 provides controls to adjust the Program clock Reference (PCR) in outgoing Kraken Transport Streams. See **Transcoder Settings**.
- **MPEG1 Audio with H.264 (AVC) and H.265 (HEVC) Video Codecs** — Audio codec choice is no longer restrained by video codec selection. MPEG1 Layer II may now be selected for all video codecs. See **Transcoder Settings**.
- **Security - Password Length and Complexity** — Kraken 3.6.1 enforces password length and complexity requirements when changing user passwords . See **Password Requirements**.
- **Security - Account Logging (KRAK-2977)** — Kraken 3.6.1 l ogs Local User login, logout, and timeout events.
- **Security - Dependency Updates (KRAK-2497)** — Kraken 3.6.1 addresses known package vulnerabilities with applicable updates.

Kraken v3.6 introduced the following features and enhancements:

- **New Stream Licensing Model** — Kraken v3.6 supports more granular licensing based on stream capacity for Kraken virtual instances on AWS, Azure, and other customer hardware. This enables flexibility for the Kraken Small Form Factor hardware, Virtual Machines, and Cloud offerings to match desired stream throughput.
- **Expanded NVIDIA Support —** Kraken v3.6 enables support for the latest series of NVIDIA devices (for example, updated Cuda version to 11.2 and Nvidia drivers version to 460.32).
- **Kraken on AWS** — A BYOL Kraken offering is now available for the AWS and AWS GovCloud marketplaces. See **Kraken AWS Quick Start Guide**.
- **Ability to enable/disable/configure Services —** Administrators can now control the running state of certain Kraken services. See **Enabling and Disabling Services** .
- **Add SSL/TLS Security Policy Setting —** The Web Interface now provides options to specify which TLS versions are accepted from the HTTPS client. See **Managing Security Policies**.
- **EMS Integration —** Kraken can now be paired with a Haivision EMS (Element Management System) to discover, manage and monitor all of your Haivision devices from one place.
- **Network Device Interface (NDI) Input —** Kraken now supports and encodes video from NDI sources. See **Configuring Input Parameters** .

Kraken v3.5 introduced the following features and enhancements:

- **Support for Encoding GigE Vision Input —** Kraken now supports ingest of GigE Vision input over Ethernet for routing into the supported encoders within the transcoding pipeline. GigE Vision streams can be encoded using H.264/H.265 transport streams and distributed as output from Kraken as transport streams over UDP or SRT. GigE Vision encoding and output is supported across any device that conforms to the GigE Vision 2.1 standard. See **Configuring Input Parameters**.
- **Warning Indication for Unsaved Configurations —** The Kraken Web Interface now displays a warning indication in the title bar when changes to Streams, Inputs, Transcoders, Outputs, or Metadata have been applied but not saved to a preset. The indication is displayed when a user signs out or in to Kraken. See **Saving and Loading Presets**.

Kraken v3.4 introduced the following features and enhancements:

- **Introduction of Kraken Edge** – This new Haivision appliance offers a small form factor transcoder where ruggedization is not required. Setup instructions are provided in the **Kraken Edge Quick Start Guide** .*
- **Kraken UI Branding** – The Kraken Web Interface can now display corporate branding. This "white labeling" allows customers to import their corporate logo for display in the following areas: banner graphic, Sign-in page graphics, browser favicon and title, as well as to switch between dark or light color scheme. For more information, see **Re-Branding the User Interface**.
- **SRT Enhancements** – The Kraken Web Interface now provides SRT statistics and graphs, and allows selection of the network interface for SRT inputs and outputs. New SRT statistics and graphs provide a diagnostic tool for troubleshooting network packet loss issues, and help users to make informed decisions on configuring SRT latency and bandwidth overhead. For more information, see **Viewing Kraken Statistics** .

*QSV encoding is not supported on Kraken Edge in v3.4; however, QSV is supported in the 3.4.1 maintenance release. Please contact your Haivision Account Manager to obtain the 3.4.1 update.

Kraken v3.3 introduced the following features and enhancements:

- **SDI Capture Using SDI SFP adapters with IP Encapsulation - Phase 2** — Kraken may now be used to capture and encode SDI input using an SFP (Small Form-factor Pluggable) SDI-to-IP gateway adapter. Phase 2 of this feature provides support for multiple SDI inputs, interlaced video, audio and ancillary data (KLV, CC).
- **RTMP Bypass Support** — Kraken 3.3 supports RTMP input and output in Bypass mode for transmuxing and stream routing with RTMP .
- **BYOL Kraken for the Azure Marketplace —** Kraken is now available in the Azure marketplace. Streams from a variety of sources may be sent to the cloud-based Kraken for transcoding and routing to other locations.

Kraken v3.2 introduced the following features and enhancements:

- **SDI Capture Using SDI SFPs with IP Encapsulation** — Kraken may now be used to capture and encode SDI input using an SFP (Small Form-factor Pluggable) SDI to IP gateway device. The initial implementation supports Embrionix SDI-SFP devices that support SMPTE 2100 IP encapsulation. Setup instructions are provided in the **Kraken OVA Deployment Guide**.
- **Certificate Management** — Kraken now provides certificate management from the Web Interface. Administrators can now use the Web Interface to generate self-signed certificates and certificate signing requests (CSRs), as well as importing certificates or private keys. See **Managing Certificates**.
- **Improved UI/UX for Software Upgrades** — Kraken 3.2 provides an improved user experience for software upgrades. This includes a more accurate progress indicator, additional status feedback in the Web Interface, and efficiency improvements.

- **Transport Protocol Selection for RTSP Input** — The transport protocol can now be set for RTSP inputs. Users can select from UDP, TCP, UDP Multicast and HTTP. See **Configuring Inputs**.

Kraken v3.1 introduced the following features and enhancements:

- **Enhanced Stream Routing and RTSP Transmuxing** — Ability to bypass the transcoder for transmuxing and stream routing for live streams.

> ⚠ **Note**
>
> If you have an existing stream, you need to delete the stream and create a new one in Bypass mode (i.e., you can't switch an existing stream).

- **New MISB ST 0601.15 tags added to UAS KLV Tag Filtering** — Tags 106 - 141 added to the full 0601 UAS KLV Tag Filtering set on the Transcoders page.
- **New Shutdown button on the Kraken Web Interface** — Users can now shut down Kraken from the Administration>Status page.
- **Kraken VMs now recognize new virtual network interfaces** — Newly added virtual network interfaces are displayed on the Network page after rebooting.

Kraken v3.0 introduced the following features and enhancements:

- **Role-Based User Account Management** — Ability to add, edit and remove user accounts within each user role: A dministrator, Operator and Viewer. See **Role-based Authorization** .
- **API Updates** — Public offering of REST API v2.0 and JSON Web format. API v2.0 provides all functionality from the Kraken Web GUI and is also harmonized with other Haivision appliances. Note that REST API v1.0 is still available and unchanged with this release.
- **NVIDIA Support** — (On qualified hardware) Offloads encode processing from the Kraken transcode pipeline to NVIDIA GPUs. Assumes Kraken is running as a VM in an ESXi 6.5+ environment. See **Configuring Transcoder Parameters** and the **Kraken OVA Deployment Guide**.
- **Infrastructure Upgrades** — Architecture Transition to CentOS 7 64-bit.

Kraken v2.9 introduced the following features and enhancements:

- **KLV Metadata Filtering** — Filter out undesired or unused MISB 0601 UAS KLV metadata tags to reduce the outbound metadata bitrate. This allows more bandwidth to be allocated to video on limited capacity network links. See **Filtering UAS KLV Metadata Tags**.
- **KLV Metadata Decimation** — Configure the transcoder to frame-decimate KLV (Key Length Value) metadata. This can reduce the rate at which metadata is transmitted from Kraken to allow better control of the outbound metadata bitrate. See **Configuring Transcoder Parameters**.
- **Improved System Feedback** — A new feedback component features stream event reporting within the Web Interface with the option to download the stream event log. This feature is intended to aid in diagnostics and debugging sessions. See **Monitoring Stream Health (Events)**.
- **Security** — A continual commitment to security. Updates to the kernel and other related mitigations to ever-evolving vulnerabilities.

Kraken v2.8 introduced the following features and enhancements:

- **SRT 1.3.1** — Integration of the latest SRT 1.3.1 libraries. Expanded configurability of SRT to include MTU, and TTL. SRT Passphrases is now protected in logs and Kraken configuration files.
- **Improved UX** — Enhanced debugging logs per transcode session. Alpha version of v2 API available upon request to Haivision Technical Support.
- **Streaming** — Added MPEG4 (Part 2) Encoding capability. Improved and enhanced the interoperability with RTSP camera sources. Updated underlying QSV libraries.

- **Security** — Continual commitment to security. Updates to the kernel and other related mitigations to ever-evolving vulnerabilities.

Product Overview

> ⚠️ **Note**
>
> Transcoding is defined as the process of converting an encoded media stream or object from one format to another. This may be done in cases where a target device (or workflow) does not support the format, has limited network bandwidth or storage capacity that mandates a reduced stream size, or to convert incompatible or obsolete data to a better supported or modern format.

Originally designed as an IP video transcoder, Kraken is now a comprehensive software-based encoding, transcoding, and stream routing platform that aggregates feeds and optimizes transport of live Full Motion Video (FMV) and metadata. Kraken has evolved and developed to address the challenges inherent to many ISR video distribution topologies, including:

- Unpredictable (and limited) bandwidth in deployed/first mile ISR video contribution systems,
- Preservation of video quality and latency at very low bandwidths in real-time,
- Downstream compatibility, i.e., the need to bridge systems with disparate video capabilities,
- KLV metadata processing requiring advanced processing capabilities.

Key Capabilities

Although the original Kraken use case was purely transcoding, it is now a multi-purpose media pipeline that can be used to serve multiple functions in multiple parts of a video ecosystem.

Transcoding

Kraken takes an already compressed video stream and manipulates it to meet specific customer requirements, for example, converting streams between formats such as H.264, H.265 (HEVC), MPEG-2, and MPEG-4 Part 2.Media

Routing and Protocol Flipping

To meet an important requirement in ISR and defense video workflows, Kraken converts video streams between container protocols such as SRT, UDP, RTSP, and RTMP. It also translates multicast streams to unicast and vice versa for bridging network domains with varying distribution schemes.

Metadata Processing

Kraken features advanced metadata processing capabilities including filtering and decimation. Filtering enables removal of specific MISB 0601 KLV tags which are not required by PED workflows, while decimation reduces the frequency at which the metadata packets are sent.

Encoding

Kraken can also function as an encoder and can ingest raw video in several different ways. It can encode analog or digital video sources via an integrated capture card as well as accept uncompressed digital video sources using an SFP+ module and can apply compression using any of the supported codec formats.

Kraken Features

Kraken is designed to be used by consumers of HD video who are contending with high bitrate / high quality streams that are either too big to transport over some network segments or too costly for users' end points to render the video smoothly.

As a transcoder, Kraken takes the stream from a source URL, re-encodes the audio/video, and sends it out as a new stream with different encoding characteristics. The characteristics that may be changed include Audio Bitrate, Video Bitrate, Video Resolution, Frame Rate, Group of Pictures (GOP) size, and Maximum Transmission Unit (MTU).

As a baseband encoder (Kraken CR platform), Kraken captures and encodes/processes baseband digital video, digital audio and ancillary metadata.

Kraken may be controlled and managed either through a Web interface or a Representational State Transfer (REST) Application Programming Interface (API). For details on the API, please refer to the **Kraken API v2.0 Integrator's Guide**.

Audio/Video Characteristics

Kraken input streams are MPEG Transport Streams with the following characteristics:

- Video Codecs: MPEG-1, MPEG-2, MPEG-4, H.264 or H.265 (HEVC)
- Audio Codecs: AAC 2 channel, AAC 5.1 channel, AC3 2 channel, AC3 5.1 channel, or MPEG 1 Layer 2

> ⚠️ **Note**
>
> Kraken only supports Single Program Transport Stream (SPTS) inputs. Multi Program Transport Stream (MPTS) inputs are not supported.

Output streams are MPEG Transport Streams with H.264 or H.265 (HEVC) video (Main Profile 4.2 level maximum) and AAC 2 channel stereo audio. Kraken outputs video in progressive format only.

Any input stream that had a mono audio source will have that source replicated into Left and Right stereo channels. Audio may be disabled, which will remove any audio tracks on the output stream.

Transport Characteristics

Kraken input streams may be either UDP unicast (the stream is sent to Kraken), UDP multicast, or TCP unicast (the stream is either sent to Kraken, or Kraken obtains the stream). Input streams may be CBR, VBR or Constant Quantizer (ConstQ). The maximum bandwidth of a single input stream is 20 Mbps.

Output streams may be either UDP unicast (the stream is sent to a third party device), UDP multicast, or TCP unicast (Kraken either listens for a request or sends a stream to a third party device). Output streams are VBR. The maximum single bandwidth for an output stream is 20 Mbps.

Kraken supports downscaling, de-interlacing, and selection of the frame rate in frames per second to allow users to select the exact output frame rate for a transcoder session. Note that "Auto" uses the same frame rate as the source stream.

> ⚠ **Note**
>
> The presence of Referenced B-Frames, streams without a "low-delay" bit set in the stream, and/or streams where the audio and video are not interleaved can cause an increase in latency.

SRT (Secure Reliable Transport)

Kraken supports Haivision's Secure Reliable Transport (SRT) input and output streaming format for interoperability with the Haivision eco-system. This enables end-to-end security and stream resiliency for recording and streaming applications. For more information, please refer to the **SRT Deployment Guide**.

SRT is a transport technology that optimizes streaming performance across unpredictable networks, including the public Internet, for secure, reliable, low latency HD video. SRT as a protocol is included across Haivision's product family.

Console User Interface

A Console UI is available for Kraken appliances which may be accessed directly by connecting a keyboard and monitor to the appliance (either from the front or the back of the appliance), or through SSH. The Console UI allows administrators to perform basic system administration tasks and network tests, as follows:

- Set basic network settings such as the IP address, netmask and default gateway.
- View statistics about the appliance's health, including current IP address, Kraken Version, CPU use, Memory use, and System uptime.

The Console UI requires a username and password. Console UI users will be able to change their password.

> ⚠ **Note**
>
> The Console UI is also available for Kraken cloud-based deployments such as Kraken Azure (see **Signing in to Your Server**) and Kraken AWS (see **Signing in to Your Server**).

Related Topics

- **Using the Console UI with Haivision Hardware**

IPv4 and IPv6 Support

Kraken now supports both Internet Protocol Version 4 (IPv4) and Version 6 (IPv6), as well as dual-stack IPv4/IPv6 networks. You will be able to access the Web Interface via the IPv4 and/or IPv6 addresses assigned to the device. This applies to all Kraken instance types including Server, Small Form Factor, Virtual Machine, and Cloud instances.

Kraken IPv4-IPv6 capabilities include the following:

- Static and dynamic assignment of IPv6 addresses via DHCPv6 or Stateless Autoconfiguration (SLAAC) to Kraken in addition to the existing IPv4 capabilities.
- Dual-stack IPv4 and IPv6 may be used simultaneously for management and video streaming purposes.
- All administration functions may be performed from an IPv4 or IPv6 network client, including upgrade/downgrade, preset import/export, license install, system snapshots and specifying audit servers.
- User functions include creating and starting streams from an IPv4 or IPv6 device.

IPv6 support for Kraken Inputs and Outputs is as follows:

Kraken Inputs	Kraken Outputs
• TS over UDP (multicast and Unicast) • TS over SRT (caller, listener, rendezvous) • RTMP Server • RTSP (Auto, UDP, Multicast, TCP, HTTP) • RTMP Client • HTTP Motion JPEG	• TS over UDP (multicast and Unicast) • TS over SRT (caller, listener, rendezvous) • RTMP Client • HLS

⚠ **Note**

Kraken does *not* support IPv6 for the following input types:
- UDP Multicast with Source Specific Multicast
- ST2110
- GigE Vision
- RAW Motion JPEG
- RTSP Client (PUSH)
- RTSP Server (PULL)

Deployment Options

Kraken is a software-based solution designed to take advantage of Intel QSV and NVIDIA GPU hardware acceleration in order to maximize performance on a variety of platforms. It is available as a rack-mount server, small form factor appliance, or as a virtual machine instance. When installed on third-party hardware as a virtual machine, Kraken can encode from 3G-SDI video inputs using SDI-SFP gateway connectors.

Kraken Server

Kraken rack-mountable servers are performance-tuned appliances available with redundant power supplies. Kraken Server supports stream routing and transcoding of IP-based network video and is available in Premium (2x H.265/8x H.264) and Ultra (4x H.265/16x H.264) channel configurations.

- The **Premium System** provides redundant power supplies, so it can be plugged into redundant power sources, ensuring higher availability. It supports up to either 8x HD H.264/AVC encoding channels or 2x HD H.265/HEVC encoding channels, thereby providing more transcoding channel density, enabling users to transcode more streams and more outputs. It also features a short-depth form factor.
- The **Ultra System** also provides redundant power supplies. It supports up to either 16x HD H.264/AVC encoding channels or 4x HD H.265/HEVC encoding channels, thereby providing the most transcoding channel density. It is full depth.
  The Ultra System also provides redundant Hot Swap Hard drives (RAID 1) and power supplies.

All server appliances are 1RU tall. For more information, see **Physical Description (Kraken Server)**.

Kraken CR

Kraken CR is a small form factor H.264/HEVC encoding/transcoding appliance, supporting capture of Analog Composite Video or HD/SD-SDI digital.

Kraken CR was designed to harmonize the user experience and functionalities between Kraken and the Makito X platform. With the introduction of baseband capture and additional metadata functionalities, ISR customers can use Kraken not only as a GCS (Ground Control Station) transcoder, but also as a source encoder.

> ⚠ **Note**
>
> References to Kraken CR include variants of Kraken CR that provide HEVC hardware acceleration.

For more information, please refer to the **Kraken CR Quick Start Guide**.

Kraken Edge

Kraken Edge is a small form factor appliance, where ruggedization is not required, with optional baseband (HD-SDI, SD-SDI, 3G-SDI) and network stream inputs. The base version supports stream routing and KLV metadata. Kraken Edge can be upgraded through additional licenses to support transcoding through H.265 or H.264 channel licenses, as well as an SDI capture license to support baseband encoding.

Kraken Edge is available in the following options:

- **Kraken Edge Base Media System with KLV Metadata Support** – This option supports stream routing and transmuxing up to 10 streams. Transcoding can be enabled with SWO-KR-H264 or SWO-KR-HEVC transcoding channel licenses.
- **Kraken Edge Base Transcoding System with KLV Metadata Support** – This option includes 1xHEVC / 4xH.264 channels. Additional capacity is enabled with SWO-KR-H264 or SWO-KR-HEVC transcoding channel licenses. SDI capture up to 1080p60 is enabled with a S-KR-SFF-SDI license.

For more information, please refer to the **Kraken Edge Quick Start Guide**.

Cloud-Based Deployments

Kraken VM

Kraken Virtual Machine (VM) provides the ability to deploy low latency encoding/transcoding on existing systems, from tactical communication kits to centralized data centers. Once integrated, the Kraken can easily be added alongside secure communications, networking, encryption, and other applications to groom streams for transmission on any network segment.

For more information, please refer to the **Kraken OVA Deployment Guide**.

Kraken Azure

Kraken is available in the Microsoft Azure cloud as a Bring Your Own License (BYOL) virtual machine. This deployment option takes advantage of Azure with NVIDIA GPUs which allows for transcoding a higher number of streams compared to using the CPU.

For more information, please refer to the **Kraken Azure Quick Start Guide**.

Kraken AWS

A Kraken offering is also available for the Amazon Web Service (AWS) marketplace as a Bring Your Own License (BYOL) virtual machine. This deployment option takes advantage of AWS with NVIDIA GPUs which allows for transcoding a higher number of streams compared to using the CPU.

For more information, please refer to the **Kraken AWS Quick Start Guide**.

Physical Description (Kraken Server)

Kraken Server comes delivered as an enterprise-ready, ultra-compact appliance made for single-tier architectures. Following is a description of the Kraken appliance interfaces.

> ⚠ **Note**
>
> For information on installing and connecting to your Kraken appliance, please refer to the **Kraken Server Quick Start Guide**.

> ✅ **Tip**
>
> For information on other Kraken hardware platforms such as Kraken CR and Kraken Edge, please see **Quick Start Guides**.

System Interfaces

Kraken Server provides 10/100/1000 Gigabit Ethernet ports for both traffic and management. The RJ-45 connectors are located on the rear of the appliance.

Premium System Appliance   Ultra System Appliance

Premium System Appliance
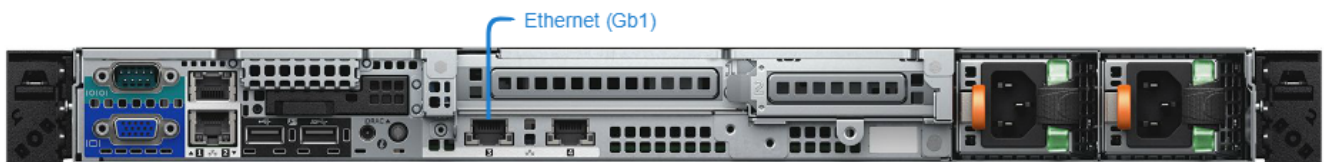
Premium System Appliance   **Ultra System Appliance**

Ultra System Appliance
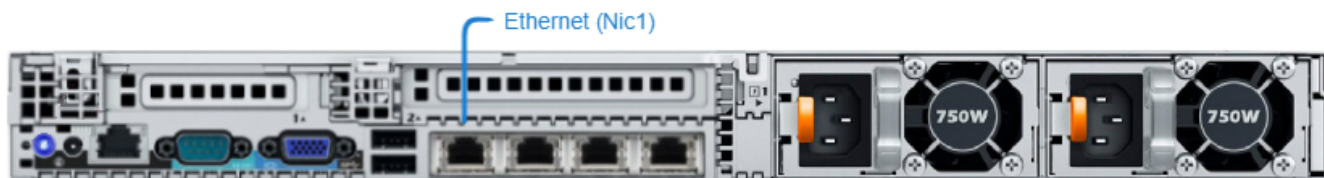
Related Topics

- **Connecting Kraken Server**

- **Getting Started with the Web Interface**

Getting Started with the Web Interface

This section provides system access control information, followed by a basic overview of the Kraken Web interface.

Topics Discussed

- **Signing in to the Web Interface**
  - **Role-based Authorization**
- **Exploring the Web Interface**
- **Changing Your Password**
  - **Password Requirements**
- **Signing Out**

Signing in to the Web Interface

> ✅ **Tip**
>
> Make sure that your browser is configured to accept cookies.

To sign in to the Kraken configuration Web page:
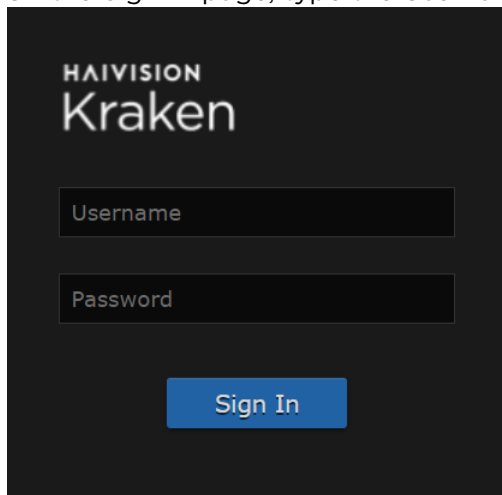
1. From your computer, open a Web browser.
2. Type the Kraken's IP Address in the browser's address bar and press **Enter**.

> ⚠️ **Note**
>
> The appliance's IP address is set by Haivision prior to delivery. Please refer to the *Important Notice* for the default IP address and administrative user information. The *Important Notice* postcard is shipped with the device or available from the **Download Center** on the Haivision **Support Portal**.
>
> The Web Interface is available over HTTPS only, port 443 TCP. HTTP traffic will be redirected to HTTPS.

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

Please refer to the *Important Notice* for the default sign-in credentials.

Kraken provides three predefined user accounts. For information, see **Role-based Authorization**.

Role-based Authorization

Kraken uses role-based authorization control to secure the Web interface. Administrators can create new accounts and thus allocate an account to each user of the system.

Kraken provides three defined account roles to assign privileges to users:

Role	Default Username	Privileges
`Viewer`	`user`	Read-only access to the system.
`Operator`	`operator`	All rights to configure A/V and stream settings, start/stop streams, etc. Does *not* include rights to reboot or upgrade the system, modify the network settings, install licenses, or manage accounts.
`Administrator`	`haiadmin`	All access rights and Administrator privileges.

All three roles provide Web interface access to the system. Please refer to the *Important Notice* (postcard included in the box or available from the Download Center on the Haivision Support Portal) for the default sign-in credentials.

> ⚠️ **Caution**
>
> For security purposes, Haivision strongly advises you to change the default password for all accounts during initial configuration.

Administrators can create, delete, and change the password for all accounts from the Accounts page (see Managing User Accounts). Operators and viewers can manage their password from the My Account page (see Changing Your Password).

> ⚠️ **Note**
>
> Any changes to the default passwords, created accounts, and deleted default accounts will be lost after a Factory Reset or a firmware downgrade. Factory Reset restores the default accounts and passwords.

Related Topics

- **Managing User Accounts**
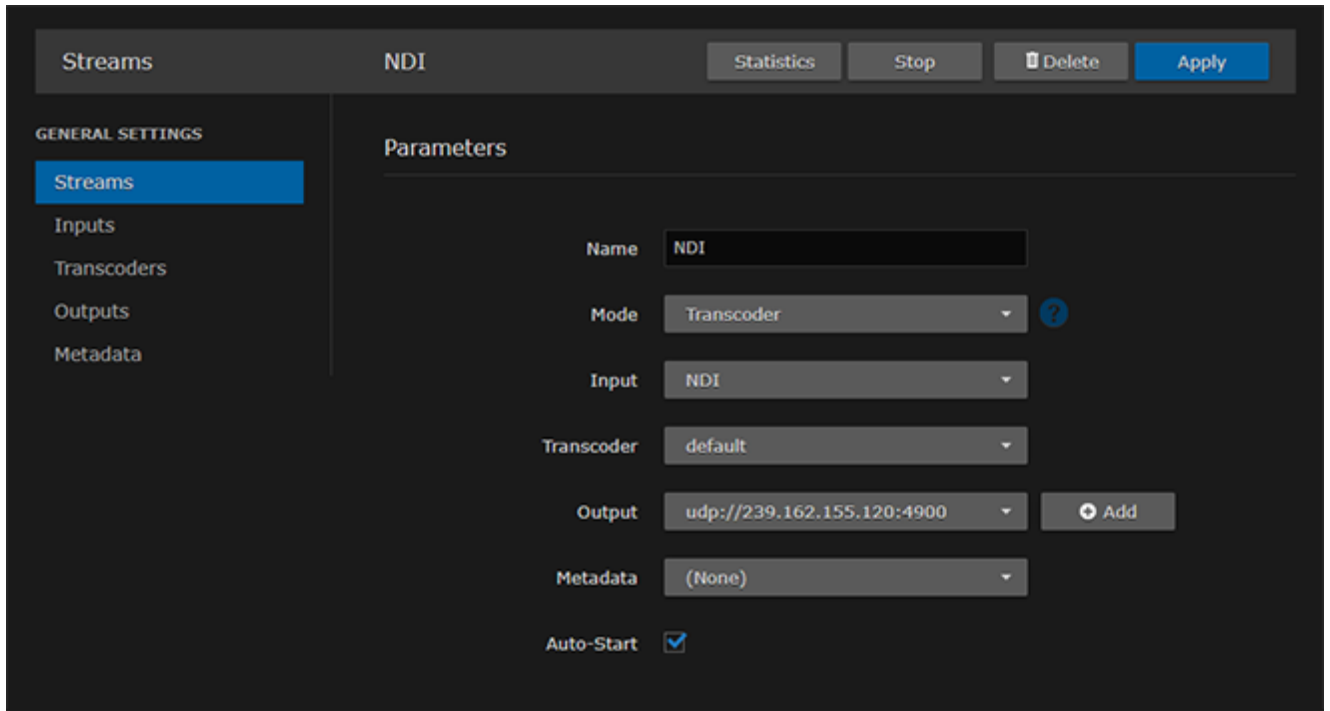- **Changing Your Password**

Exploring the Web Interface

After logging in to the Web configuration interface, you will have access to the appliance configuration settings.

Navigational Menus

Once you have successfully signed in, the Kraken Web interface opens to the Streams List View. Your account information is displayed on the toolbar (along the top).
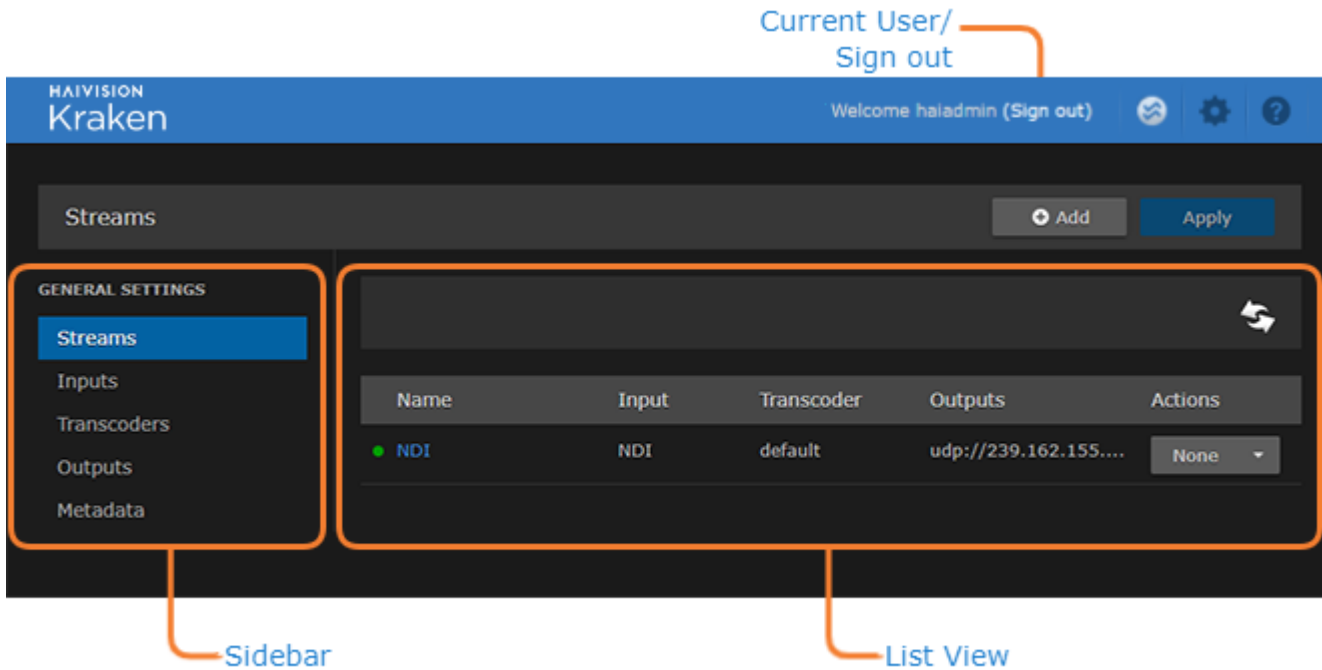
- To set up stream-based transcoding or encoding, select the configuration option from the sidebar, for example, **Streams**, **Inputs**, **Transcoders**, or **Outputs**.
- To open the Detail View (from the List View), click a link (any line) in the table. For example, on the Streams List View (shown above), click a link to open the Streams Detail View (shown following).

- To access the administration settings, click the ⚙ **Administration** icon on the toolbar and then select the option from the sidebar, for example **Accounts**, **Network**, or **Presets**.
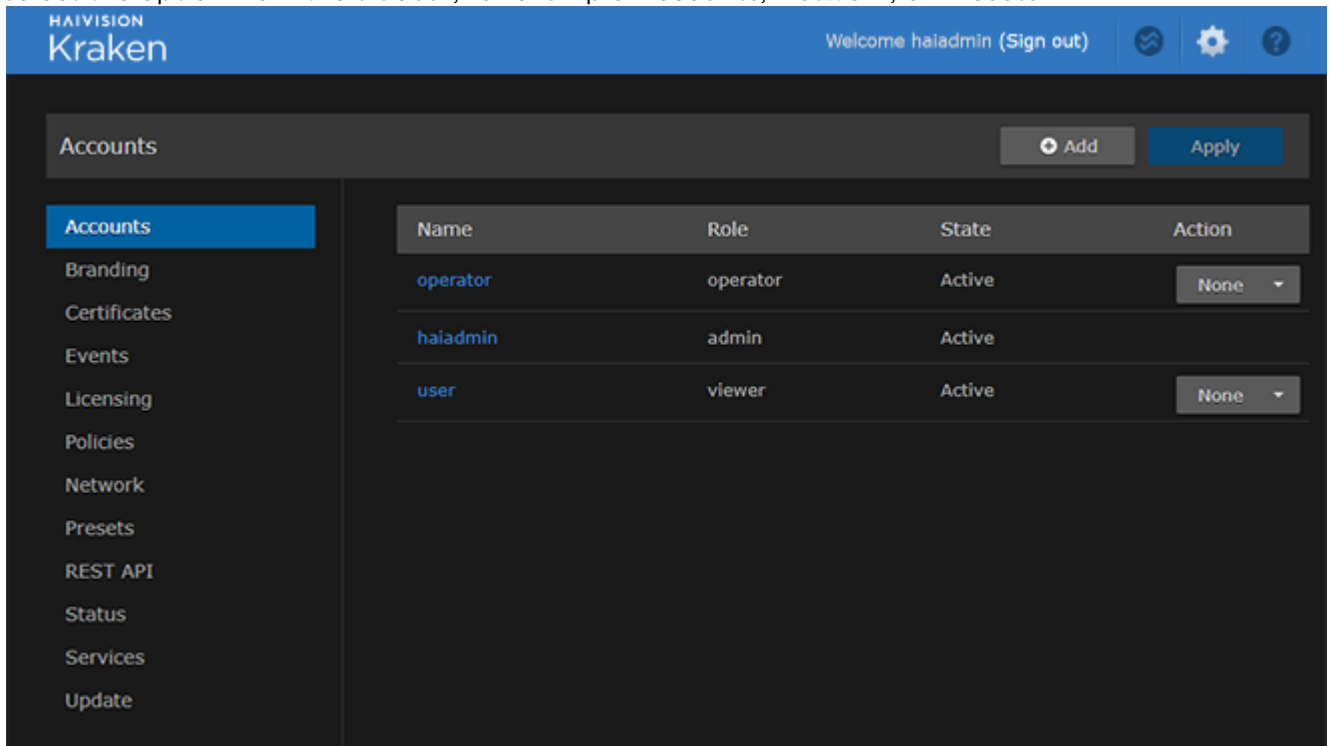
Changing Your Password

> ⚠ **Important**
>
> For security purposes, be sure to change the default password!

If you are logged in as a non-administrative user, you can change your own password from the My Account page, as described in this section. This is useful when logging into a Kraken on which the factory defaults have not been changed.

> ⚠ **Note**
>
> The My Account page is available to users assigned either `Operator` or `Viewer` roles.
>
> Administrative users may change their passwords from the Accounts page. For the privileges assigned to accounts, see **Role-based Authorization**.

To change your password:

1. Click the ⚙ **Administration** icon on the toolbar and then click **My Account** on the sidebar. The My Account page opens as shown in the following example.
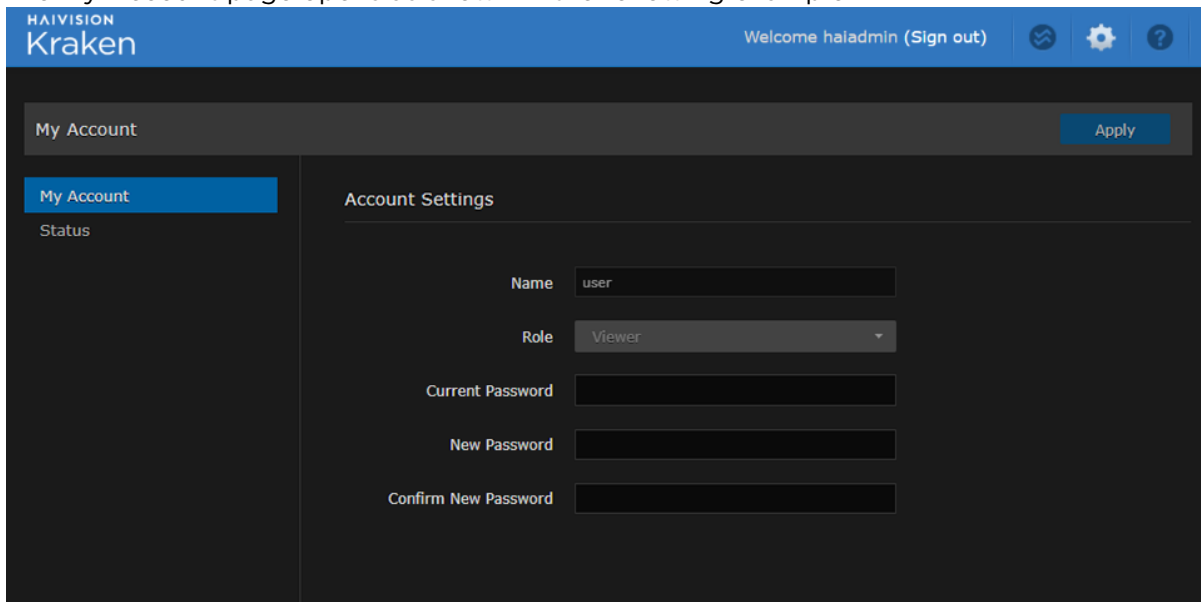
2. Type your current password in the Current Password field.
3. Type the new password in the New Password field and again in the Confirm New Password field.
4. Click **Apply**.
   The new password will take effect immediately.

Password Requirements

> ⓘ **Tip**
>
> For details on administrative adjustment of password settings via configuration file, please contact your Haivision representative.

Password Length and Complexity

Kraken can be configured by an administrator to enforce password length and complexity requirements when changing passwords of existing user accounts, or creating a new Kraken local user. Password requirements include:

- minimum length of 15 characters
- at least one lower case character: a .. z
- at least one upper case character: A .. Z
- At least one number: 0 .. 9
- at least one special character from the set: ! @ # $ % ^ & *

Passwords may be up to 80 characters and composed of any combination of upper and lower case letters, numbers, and special characters, e.g., "CXAdminManager123!".

Password Lifecycle

Successive changes or modifications to a Kraken local user password have rules which are configurable by an administrator.

Configurable Password Lifecycle features include:

- Enforcing a minimum number of character changes between successive passwords
- Preventing reuse of old passwords over a configurable number of password generations
- Enforcing a minimum and maximum password lifespan (to prevent changing when within the minimum, and force changing when past the maximum)

Signing Out

After you finish using Kraken, be sure to sign out. To do so, click **Sign out** from the toolbar.

Signing out prevents misuse and unauthorized access to the appliance.

Managing Kraken from the Web Interface

This section explains how to set up real-time stream-based transcoding and/or encoding using the Web interface.

> ✅ **Tip**
>
> To set up transcoding, you need to define:
> - **Inputs** – the source URL, or an SDI or Analog Composite Input (applicable hardware server or appliance, cloud or virtual machine instance) for baseband input encoding
> - **Transcoders** – audio and video characteristics to change
> - **Outputs** – one or more output URLs
> - **Streams** – select from defined Inputs, Outputs, Transcoders, and (optionally) Metadata sources.
>
> You may optionally configure Kraken to capture KLV or CoT **Metadata** from a UDP network source or from the SDI or Serial Input interface.

Topics Discussed

- **Configuring Streams**
  - **Streams List View**
  - **Configuring Stream Parameters**
  - **Stream Settings**
  - **Viewing Kraken Statistics**
- **Configuring Inputs**
  - **Inputs List View**
  - **Configuring Input Parameters**
  - **Input Settings**
  - **Input Statistics**
  - **Connecting an RTMP Input Source**
- **Configuring Transcoders**
  - **Transcoders List View**
  - **Configuring Transcoder Parameters**
  - **Filtering UAS KLV Metadata Tags**
  - **Transcoder Settings**
  - **Advanced Shaping Settings**
- **Configuring Outputs**
  - **Outputs List View**
  - **Configuring Output Parameters**
  - **Output Settings**
- **Configuring Metadata Capture**
  - **Metadata List View**
  - **Configuring Metadata Parameters**
  - **Configuring CoT Retransmission**
  - **Configuring KLV Metadata Insertion**
  - **Metadata Settings**

- **Recording a Stream**

Configuring Streams

A Kraken stream typically consists of a user-defined stream Name, Input, Transcoder, Output(s), and (optionally) Metadata source(s).

From the Streams pages, you can define an unlimited number of Kraken streams. However, the number of active streams supported by Kraken depends on your Kraken hardware and Haivision licensing applied to that hardware.

From the Streams Statistics page, you can view statistics for the Stream as well as the configured Input, Decoder, Encoder, and Output. In addition, for SRT streams, the Statistics page includes links to SRT Input and Output Statistics graphs.

Stream Routing

Kraken supports three stream routing modes:

Mode	Stream Routing	Description
Transcoder	Input, Transcode and Output(s)	This is the traditional transcoding workflow (i.e., the only option pre-Release 2.5).
Transcoder + Passthru	Input with Retransmission, Transcode, and Output(s)	This transcodes the input stream (similar to the **Transcoder** workflow) but also re-transmits the stream to another destination (i.e., to "pass through" the system and be rerouted to a different remote IP address).
Bypass	Input and Output(s)	This mode does *not* transcode the input stream, but simply re-transmits it to the outputs without any manipulation of the content.

Streams List View

The Streams List View displays a status icon along with the Stream Name, Input, Transcoder, and Output(s) for each defined stream. It also provides options for you to start, stop or delete a stream.

To open the Streams List View:

1. Click the ⊗ **Streaming** icon on the toolbar, and then click **Streams** on the sidebar.
   The Streams List View opens, as shown in the following example.
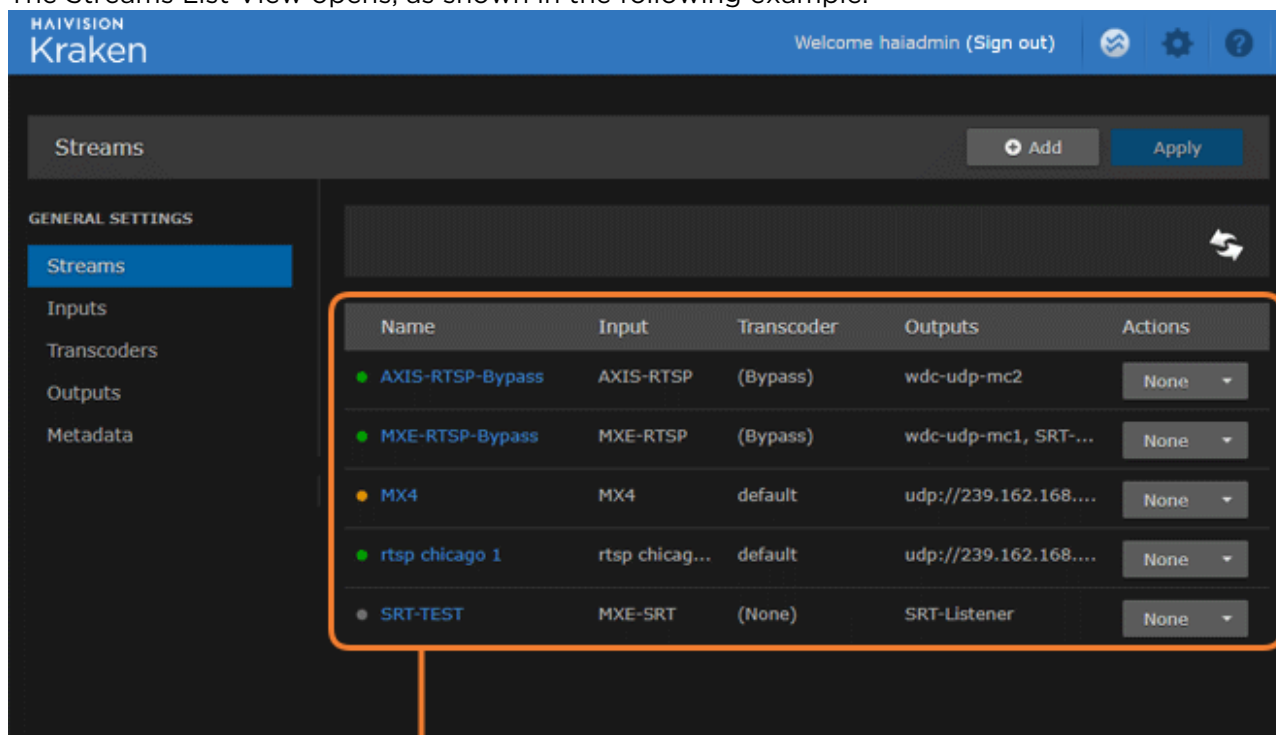
2. From here, you can perform the following tasks:
   - To add a stream, click the ⊕ **Add** button.
   - To view details or modify the components of a stream, click a line in the table to open the Streams Detail View.
   - To change the status for a stream, click the drop-down list under **Actions** and select either Start/ Stop (as applicable) or Delete.
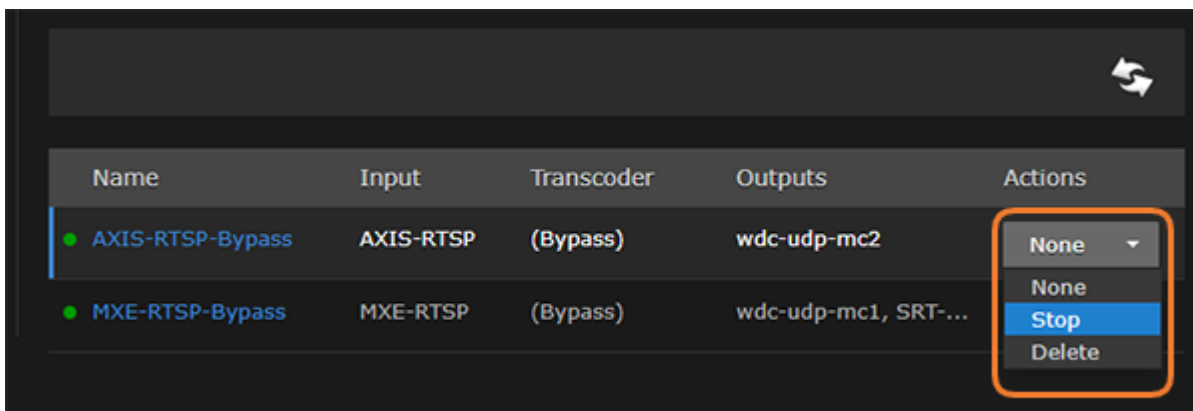
3. To apply your changes, click **Apply**.

Related Topics

- **Configuring Stream Parameters**

Configuring Stream Parameters

> ⚠ **Note**
>
> You must first define the Inputs, Transcoders, Outputs, and (optionally) Metadata sources before you can define a Stream.

The Inputs, Transcoders, Outputs, and Metadata sources that you have previously defined will be selectable when you add or modify a stream.

To view and configure Stream parameters:

1. From the Streams List view, click the ⊕ **Add** button or click any line in the table for an existing stream.
2. On the Streams Detail View, type in a unique name for the stream.
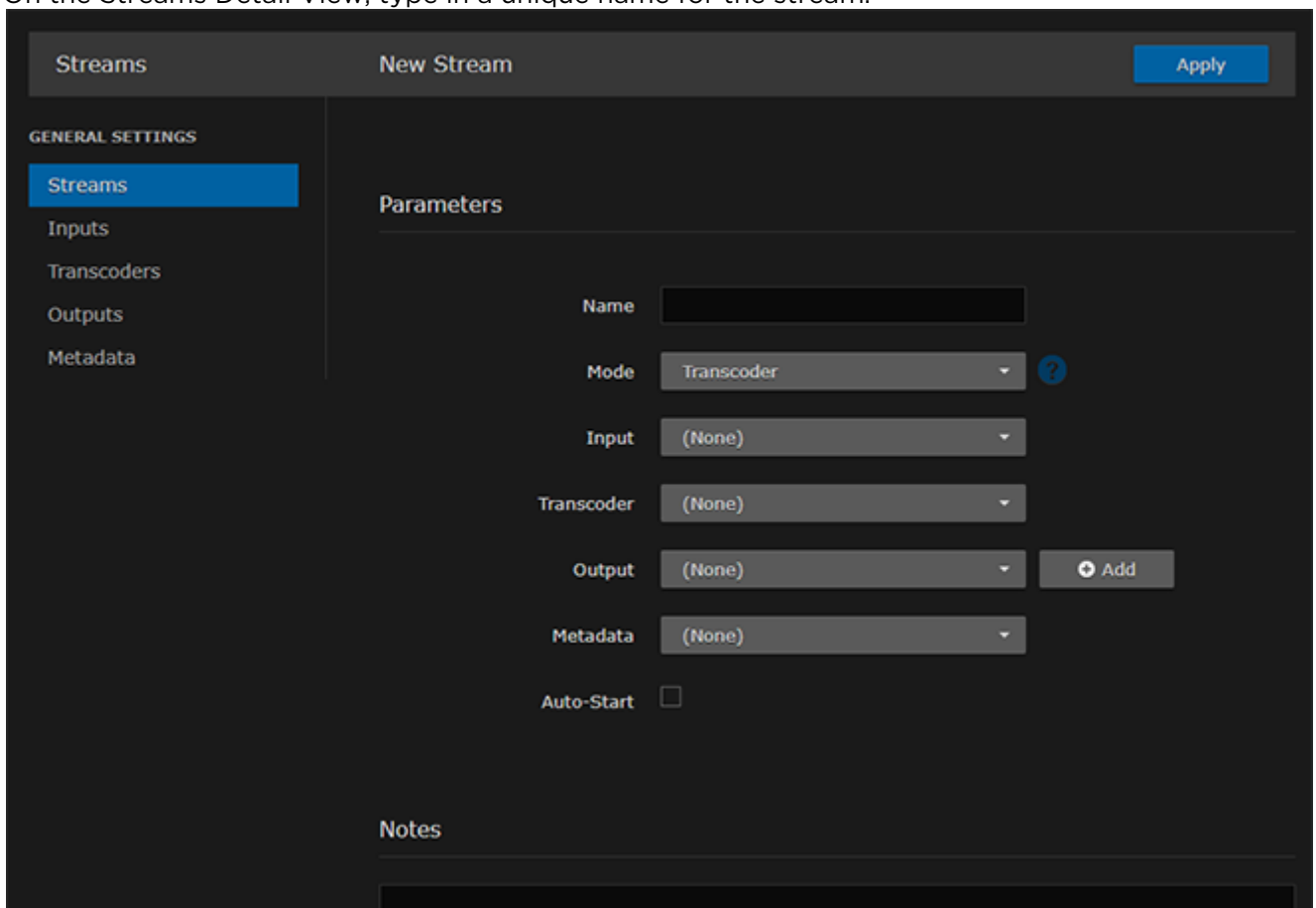
3. (Optional) To configure alternate stream routing modes, such as "Transcoder + Passthru" or "Bypass", select the stream routing mode. See **Stream Routing**.
4. Select an Input, Transcoder, one or more Outputs, and (optionally) one or more Metadata sources to define the stream. See **Stream Settings**.
5. To apply your changes (to the current session only), click **Apply**.
   The changes will take effect immediately but will not be saved and will be lost after a reboot.

> ⚠ **Note**
>
> You must click **Apply** in order for your changes to take effect. However, your changes will not be saved and will be lost after a reboot. To save the current settings, open the **Administration** > **Presets** page. See Saving and Loading Presets.
> The **Start/Stop** and **Statistics** buttons become available after you click **Apply**.

The new stream is added to the Streams List.
6. To start or stop the stream, click **Start** or **Stop** (as applicable).
   Or click **Streams** from the sidebar to return to the Streams List View.
7. To view streaming statistics, click **Statistics**. For details, see Viewing Kraken Statistics.
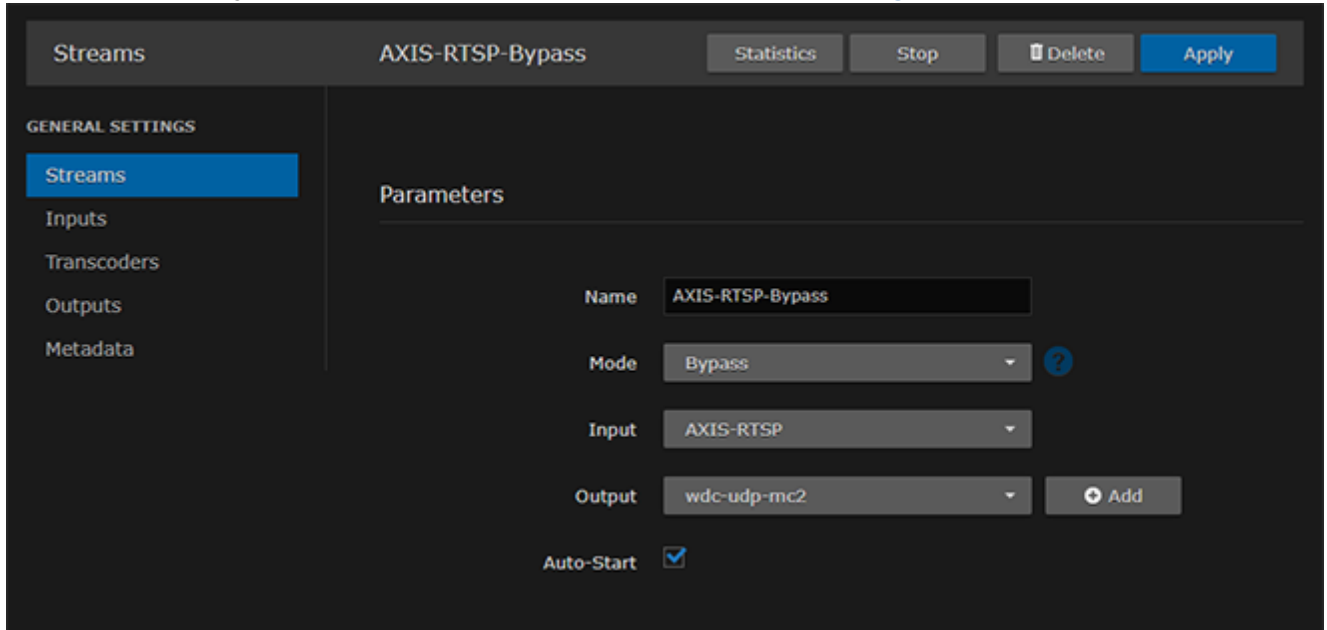
> ⚠ **Note**
>
> • With MPEG TS or RAW Motion JPEG inputs, Kraken takes the source URL, re-encodes the audio/video, and sends it out as a new stream with different encoding characteristics.
> • With SDI or Analog Composite inputs, the Kraken CR captures and encodes/processes baseband video and ancillary metadata.

Related Topics

• Stream Settings

Stream Settings

The following table lists the Kraken Stream settings:

| Stream Setting	Description/Values
Name	Enter a unique name for the stream.
Mode	Select the stream routing mode: See **Stream Routing**. • Transcoder (default): The Input will be transcoded to one or more Outputs. • Transcoder + Passthru: The Input will be transcoded and also re-transmitted to another destination. • Bypass: The Input will not be transcoded, but simply copied (as is) to the Outputs. ⚠ **Note** • Bypass mode supports RTSP in addition to TS/UDP and TS/SRT input stream types. Bypass mode may be used to transmux RTSP input to TS/UDP or TS/SRT output. • Bypass supports multiple outputs whereas Passthru supports only one. • RTSP inputs may be configured with Transcoder or Bypass Mode. • Mode is restricted to "Bypass" when an RTMP input and/or output is selected.
Input	Select the Input for the stream.
Passthru Output	(Mode must be Transcoder + Passthru) Select the Output for the re-transmitted stream.
Transcoder	(Mode *cannot* be Bypass) Select the Transcoder to apply to the stream.
Output	Select the Output for the transcoded or bypassed stream. ⚠ **Note** To specify multiple Outputs, click Add and select from the list.
Metadata	(Mode must be Transcoder or Transcoder + Passthru) Select the Metadata source for the transcoded stream.
Auto-Start	Check this checkbox to auto-start this stream when a Preset is loaded via the Administration Preset page or applied after a reboot.
Notes	(Optional) Type in any related information or comments.

Related Topics

• **Viewing Kraken Statistics**

Viewing Kraken Statistics

From the Streams Statistics page, you can view statistics for the Stream as well as the configured Input, Decoder, Encoder, and Output. In addition, for SRT streams, the Statistics page includes links to SRT Input and Output Statistics graphs.

To view Kraken statistics:

1. From the Streams List view, click any line in the table to open the Detail View for an active stream.
2. On the Detail View, click **Statistics**.
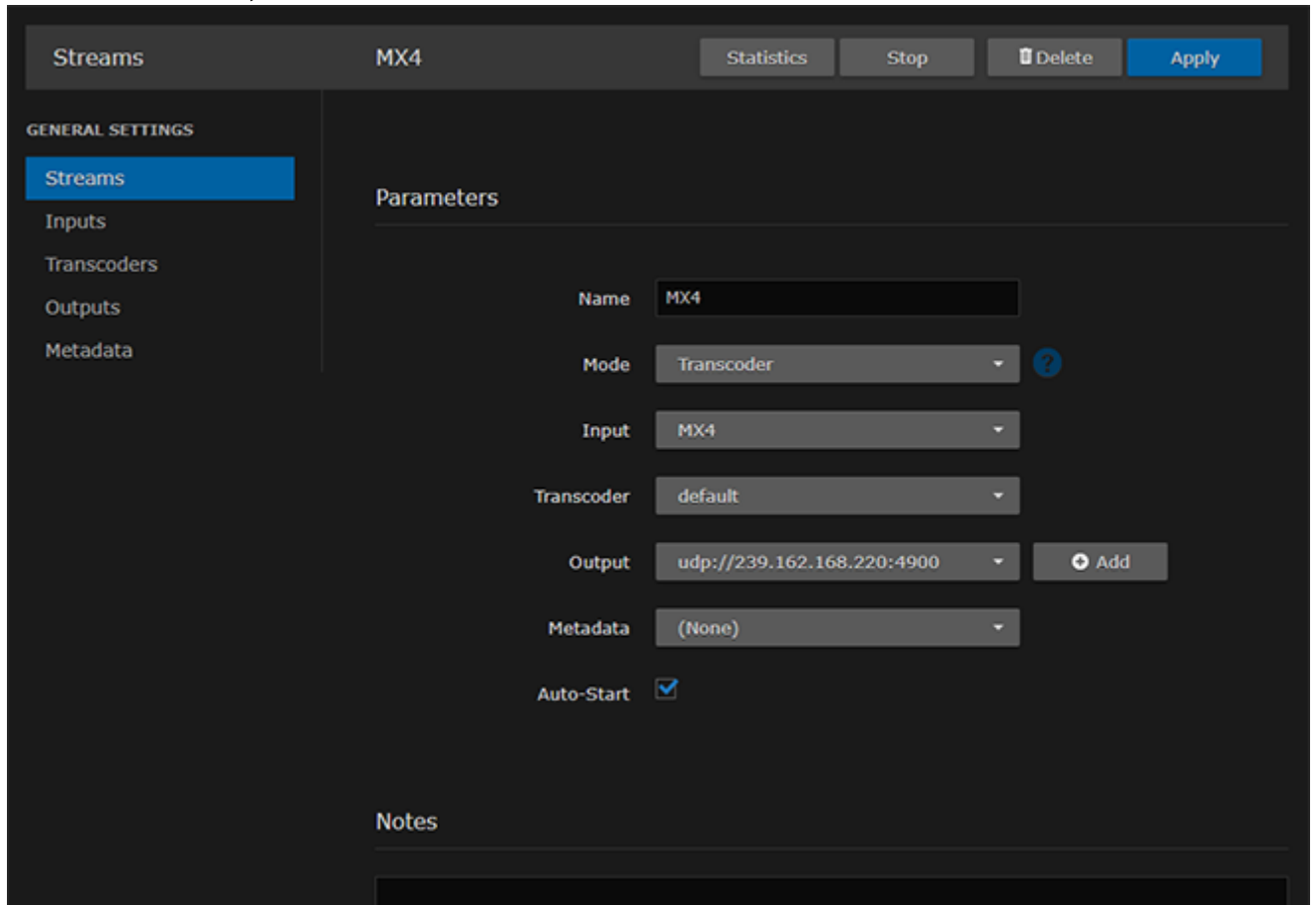
The Statistics page opens in a separate tab.
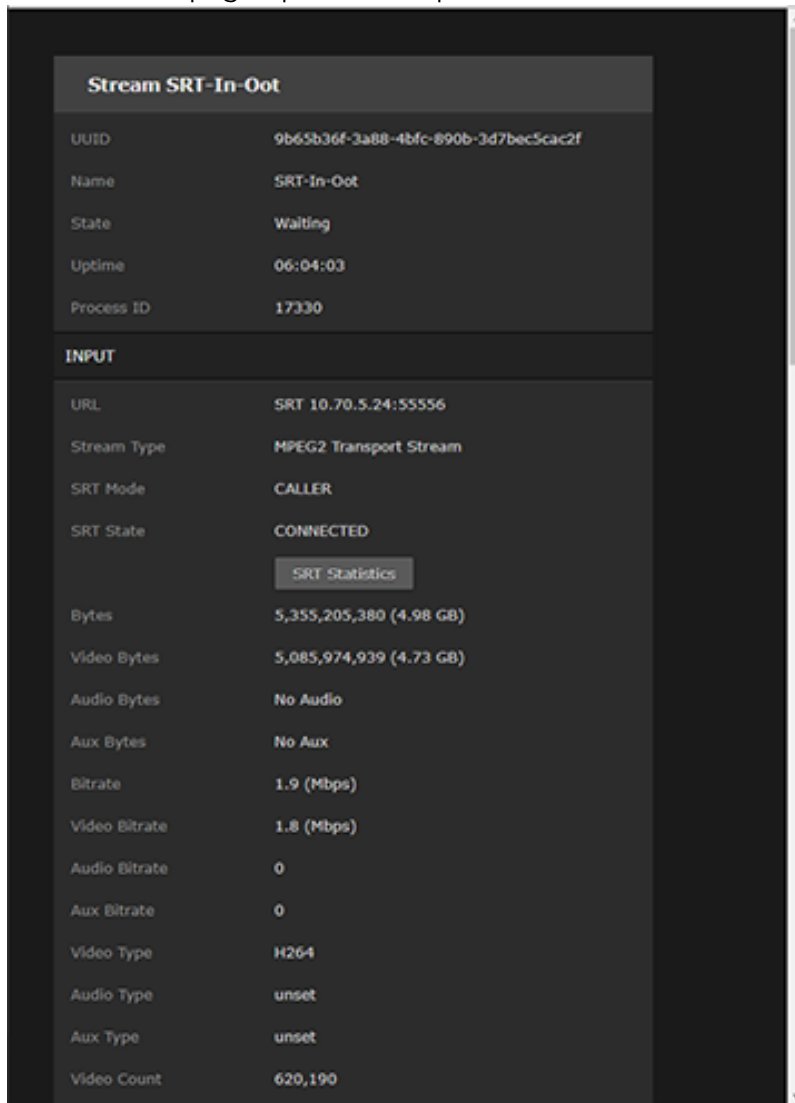
3. Scroll down to view the statistics.
4. For SRT streams, to view the SRT Input or Output Statistics graphs, click the **SRT Statistics** link in either the Input or Output section.
   The selected SRT Statistics graph opens in a new tab. See SRT Statistics for detailed descriptions of each statistic.

   As shown in the following examples, the graphs track Delays (in ms) and Bandwidth Used (in kbps).
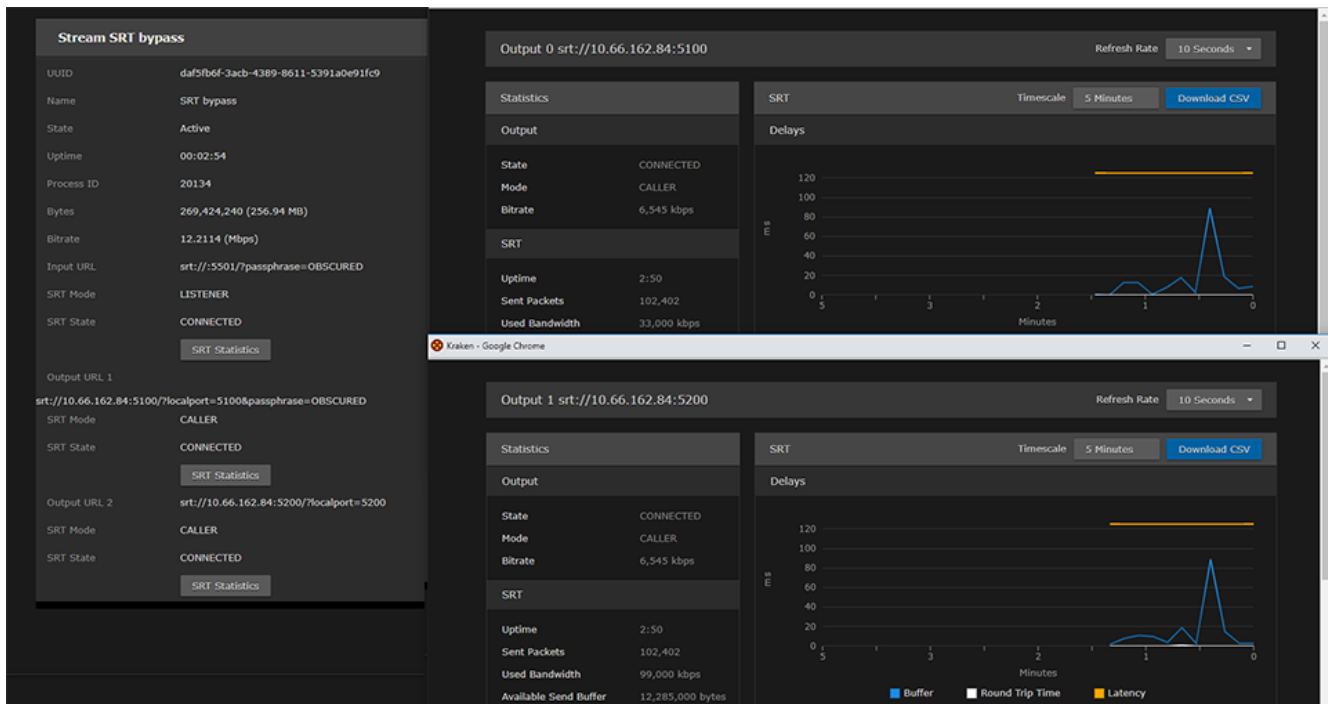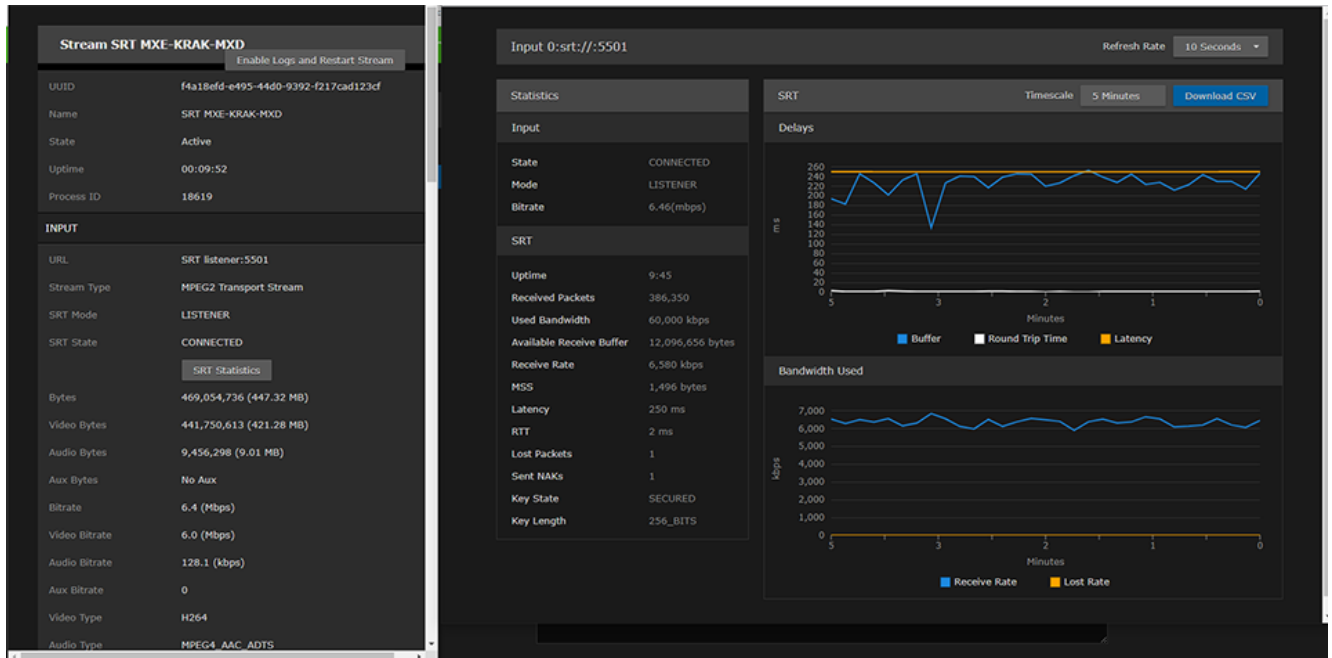
The **Delays** section provides a graphical overview of how the SRT stream buffers are handling the traffic.

The **Bandwidth Used** section provides a graphical overview of how the network bandwidth available to the SRT stream is actually being used, in terms of the rate at which packets are sent, received, resent and lost, as well as the data volume (rate × time).

• You can adjust the **Timescale** and **Refresh Rate** for the graph.
• For the **Delays**, you can show or hide the **Buffer**, **Round-Trip Time** or **Latency** statistics.
• For the **Input Bandwidth**, you can show or hide the **Receive Rate** and/or **Lost Rate**.
• For the **Output Bandwidth**, you can show or hide the **Sending Rate** and/or **Retransmit Rate**.

> ⚠ **Note**
>
> **Kraken also** supports multiple SRT graphs on Output.
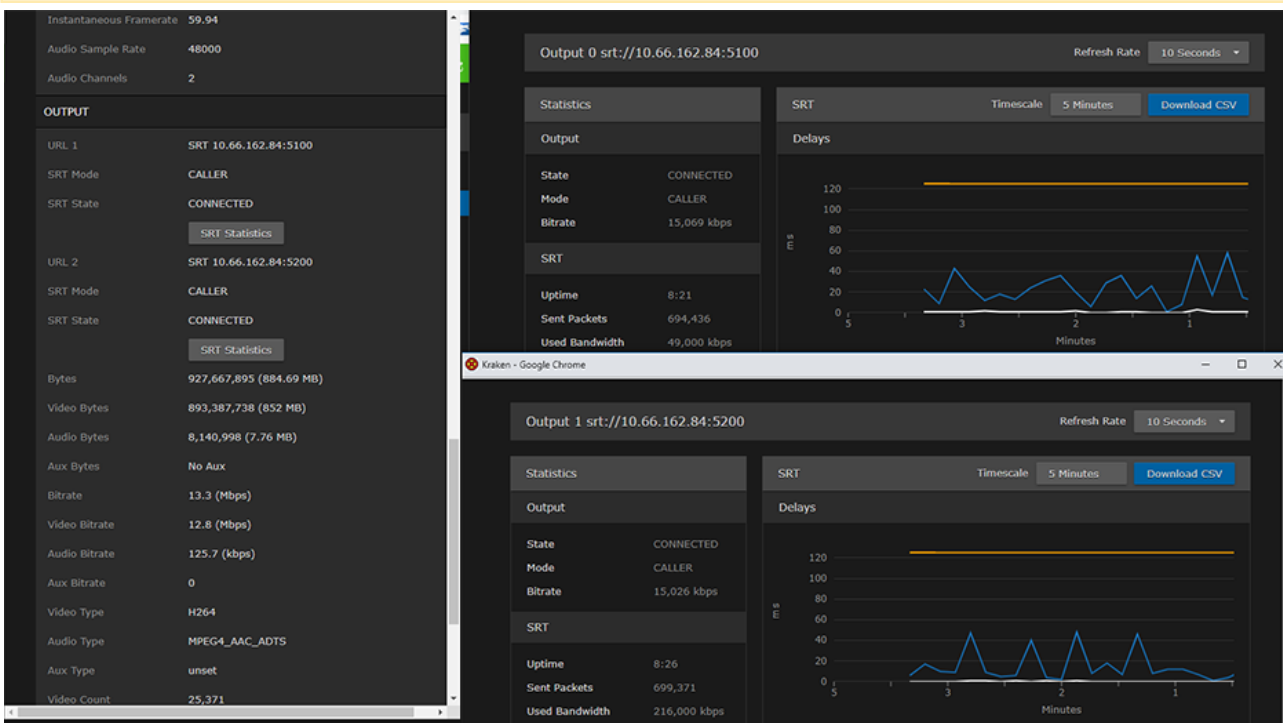
5. To download the statistics in a CSV file, click **Download CSV**.

Related Topics:

- **SRT (Secure Reliable Transport)**
- **SRT Statistics**

HLS Statistics

To view HLS statistics:

1. From the Streams List View, click any stream with an HLS Output to open the Detail View.
2. From the Detail View, click **Statistics**.
3. The statistics for the HLS stream will open in a separate tab, as in the following example:

Related Topics:

- **SRT Statistics**
- **Configuring Output Parameters**
- **HLS Live Preview**

SRT Statistics

The following table lists the SRT Statistics for Kraken Inputs and Outputs:

Statistic	Description/Values
State	The current operating status of the Input or Output, either Connected, Connecting, Connection established, or Disconnected.
Mode	SRT Connection Mode, either Caller, Listener, or Rendezvous.

Bitrate	The stream bitrate (in kbps).
SRT	
Uptime	The elapsed running time of the Input or Output.
Received Packets (Input) Sent Packets (Output)	Number of packets received/sent for the Input or Output.
Used Bandwidth	Bandwidth used.
Available Receive Buffer (Input) Available Send Buffer (Output)	Available Input or Output buffer size in bytes. SRT buffers are the stream packets waiting to be received or sent. This statistic shows the portion of the buffers up to the first missing packet. In other words, the remaining time to transmit the missing packet before it's too late. The level of the buffer in absence of packet loss is just below the latency value. In presence of packet loss, it is between 0 and the latency value. ✅ **Tip** If the Buffer goes to 0 often, then there is most likely insufficient BW to support the desired bitrate. In this case, decrease your bitrate. If the Buffer occasionally goes to 0, then the SRT Latency should be increased.
Receive Rate (Input) Send Rate (Output)	Rate at which the Input or Output is receiving or sending stream packets in megabits per second.
MSS	(Maximum Segment Size) Maximum amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.
Latency	The maximum buffer size (ms) available for managing SRT packets. SRT Latency can be set on both the Input and Output. The higher of the two values is used for the SRT stream.
RTT	Measured round-trip time. Round Trip Time (RTT) is the time it would take for a packet to travel from a specific source to a specific destination and back again. In SRT, this is measured as the time it takes for the destination device to send an acknowledgment (ACK) packet, and then receive a corresponding confirmation (ACKACK) packet.
Lost Packets	Number of SRT packets reported missing on the UDP connection. For each "hole" detected in the packet sequence, a request to re-transmit the lost packet is sent to the sender. This lost packet may (or may not) be re-covered by the re-transmit request. ⚠️ **Note** This is the raw number of packets dropped by the network. Most are recovered by retransmission at the source and so do not necessarily result in any artifacts.
Sent NAKS (Input) Received NAKS (Output)	Total number of negative acknowledgment packets sent from the source device or received from the destination device.
Max Bandwidth (Output)	Maximum bandwidth used by the Kraken SRT Output stream (i.e., the current total of audio/video bit rate plus ancillary data plus the SRT bandwidth overhead).
Key State	Indicates status of AES Encryption (if enabled), either Secured or Unsecured.
Key Length	Indicates the specified key length for AES encryption, in bits: 128, 256, or Unset.
Lost Rate (Input) Retransmit Rate (Output)	Rate at which the Input is receiving lost packets, or the Output is resending lost packets in bits/s. See the "Lost Packets" description (above) for more details.

Configuring Inputs

You must first define one or more Inputs before you can define a Stream. Inputs can either be a source URL, an SRT source, or other input (such as an SDI or Analog Composite encoding source):

- For transcoding, each Input consists of a valid source URL with an optional name and notes. In addition, with TS over UDP, you can select the network interface to input streams from any of the available Network Interface Cards (NICs).
- The default stream type for the Input is MPEG TS over UDP. You may also select TS over SRT, RTSP, Raw Motion JPEG (MJPEG), or RTMP.

> ⚠ **Note**
>
> Bypass mode may be used to transmux RTSP input to TS/UDP or TS/SRT output.
> As of Release 3.3, Kraken supports RTMP input and output in Bypass mode.

- To configure encoding/processing of baseband video or uncompressed video over IP, you may select an SDI, Analog Composite, ST2110 (SFP SDI to IP gateway), GigE Vision, or Network Device Interface (NDI) input.

Inputs List View

The Inputs List view displays a summary of defined inputs for Kraken, including the Input Name, Connection (source) URL, and Status for each input. It also provides an option for you to delete an input.

To open the Inputs List View:

1. On the Streaming page, click **Inputs** on the sidebar.
   The Inputs List view opens, as shown in the following example.
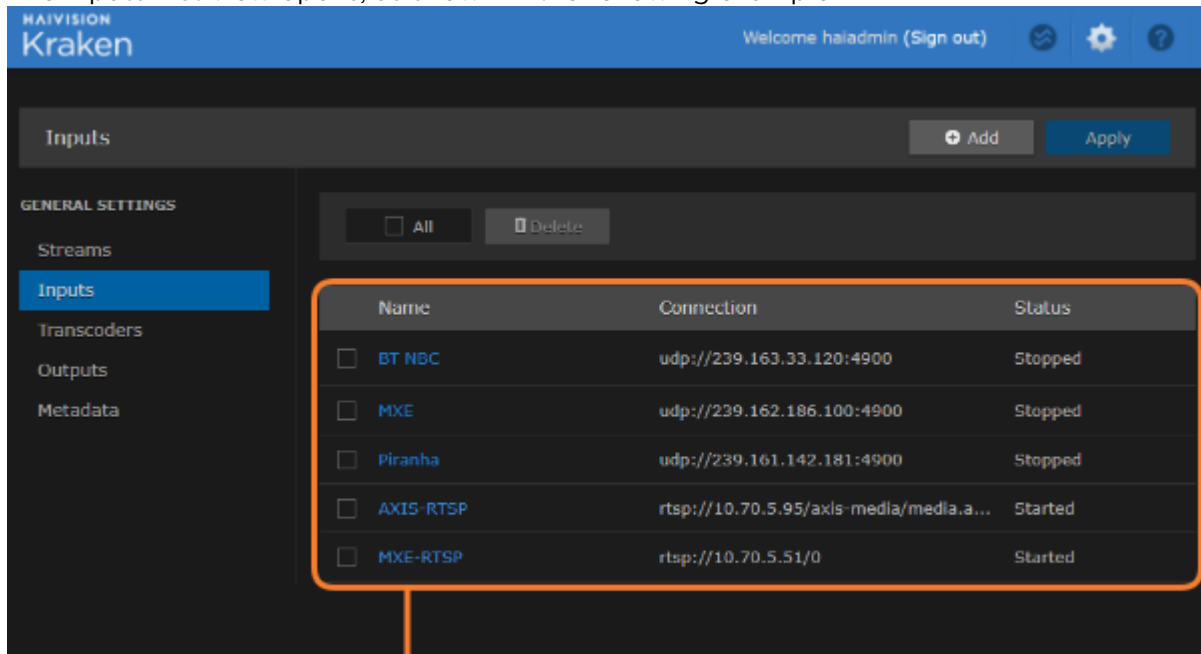
Click link to open Detail View

- To add a new input, click the ⊕ **Add** button.
- To view details or modify the settings for an input, click a line in the table to open the Inputs Detail View.
- To delete an existing input, check the checkbox next to the item in the list and click the 🗑 **Delete** button.
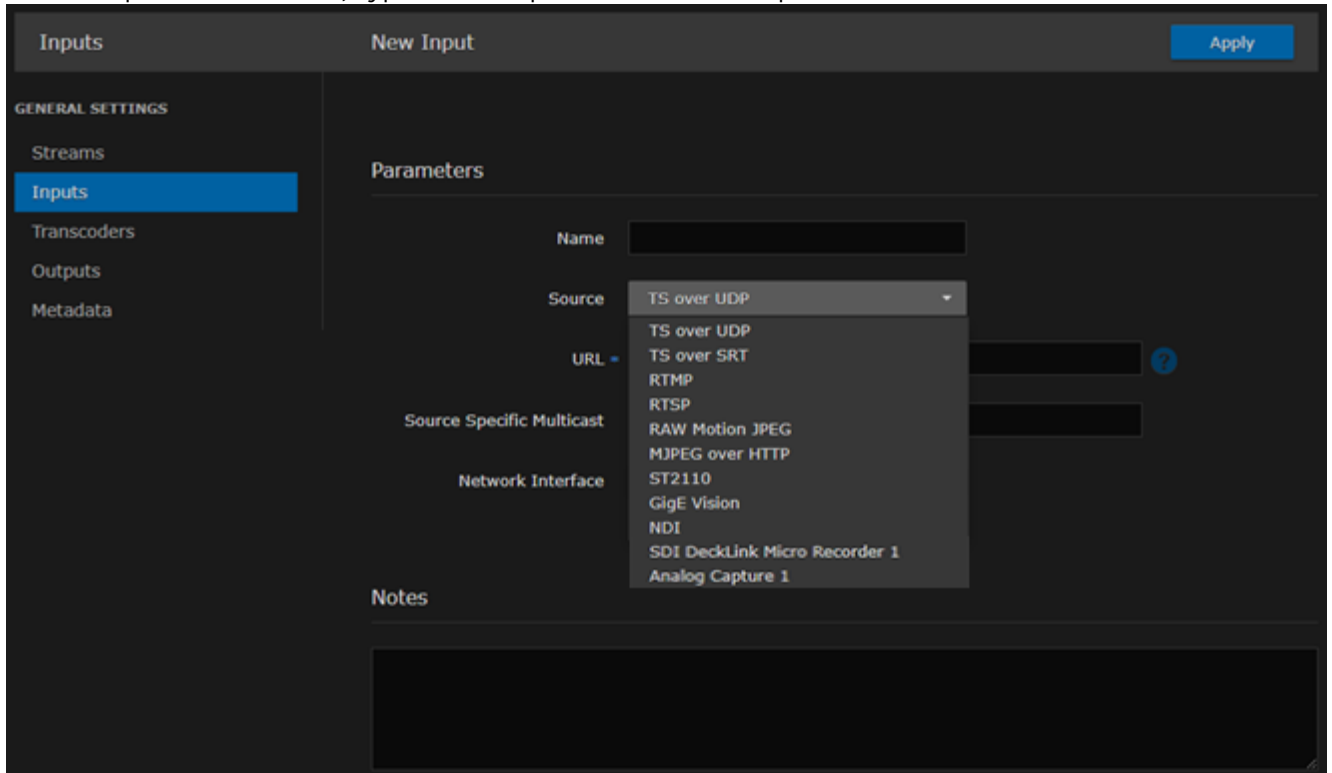
2. To apply your changes, click **Apply**.

Related Topics

- **Configuring Input Parameters**
- **Transport Characteristics**

Configuring Input Parameters

To view and configure Input parameters:

1. From the Inputs List view, click the ⊕ **Add** button or click any line in the table.
2. On the Inputs Detail View, type in a unique name for the input and select the Source.

3. Select or enter values in the fields to define the input. For details, see Input Settings.
4. The Input parameters vary depending on the hardware setup of the appliance (or VM or cloud service, if applicable) and the Input Source selected.
   - For transcoding, select either TS over UDP (default), TS over SRT, RTSP, Raw Motion JPEG (MJPEG), RTMP, or MJPEG over HTTP. For further details, see Input Settings.
   - To configure video encoding, select either ST2110, GigE Vision, Network Device Interface (NDI), SDI DeckLink Micro Recorder 1, or Analog Capture 1 input.
5. To configure SRT input, select TS over SRT for the Source and then complete the additional fields under SRT Settings. See SRT Input Settings

   Encoding Sources
   - **ST2110:** (Kraken running as VM on hardware with SFP SDI to IP gateway installed and ST2110 input licensed) To capture and encode uncompressed video over SDI, select ST2110 for the Source and then complete the additional fields. See "ST2110 Capture" (under Input Settings).
   - **GigE Vision:** (Kraken appliance or VM with GigE Vision input licensed) To capture and encode video from a GigE Vision camera, select GigE Vision for the Source and then complete the additional fields. See "GigE Vision Capture" (under Input Settings).
   The camera must be GigE Vision 2.1 compliant, and the camera IP address must set up on same network as Kraken for access.

- **NDI:** (Kraken appliance or running as VM with NDI input licensed) To capture and encode Network Device Interface video, select NDI for the Source and then select the NDI Source Name. See "NDI" (under **Input Settings**).

> ⚠ **Note**
>
> NDI sources may interfere with Kraken inputs from other sources. For best performance we recommend running NDI streams on a separate Kraken appliance, or using a port range beneath 5959 to allow the dynamic port range usage of NDI to co-exist with other streams.
> For more information on port selection, see "NDI" (under **Input Settings**).
> NDI input in Kraken leverages mDNS on port 5353 for NDI source discovery on a local network. On networks where Kraken and NDI sources co-exist, ensure that traffic on port 5353 is allowed. The mDNS service is turned on internally when NDI service is on, and will turn off automatically when NDI is turned off.
> To configure NDI services see **Enabling and Disabling Services**.

- **SDI DeckLink:** (Kraken appliance with SDI capture card installed) To capture and encode HD/SD-SDI video, select SDI DeckLink Micro Recorder 1 for the Source and then select the Capture Mode. See "DeckLink Mode" (under **Input Settings**).

> ✅ **Tip**
>
> For HD/SD-SDI encoding, begin by using "Autodetect" for the DeckLink Mode. If this does not work correctly on your system, refer to "DeckLink Mode" (under **Input Settings**) for details on manually selecting the DeckLink Mode.

- **Analog Capture:** (Kraken appliance with Analog Composite capture card installed) To capture and encode Analog Composite video, select Analog Capture 1 for the Source and then select the Capture Mode. See "Analog Capture Mode" (under **Input Settings**).

6. To apply your changes, click **Apply**.
7. The new input is added to the Inputs List.
8. To view statistics for SDI (DeckLink) or Analog Capture encoding inputs, click **Statistics**. For details, see **Input Statistics**.

> ✅ **Tip**
>
> You can view statistics for other input types from the Streams Statistics page, including SRT Statistics graphs. For more information, see **Viewing Kraken Statistics**.

Related Topics

- **Input Settings**
- **Transport Characteristics**

Input Settings

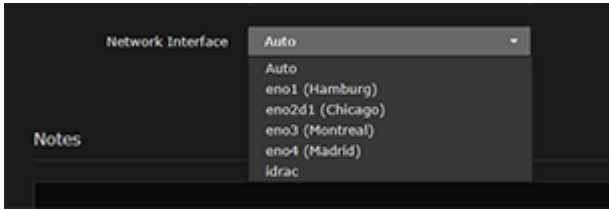The following table lists the Kraken Input settings:

General   SRT Inputs   Encoding Inputs

General Input Settings

Input Setting	Description/Values
Name	Enter a unique name for the input. This name will be selectable from the list of Inputs when you define a stream. ⚠️ **Note** The Input name is not required. Kraken will use the Input URL as the name if none is provided.

Input Setting	Description/Values

Source (Transcoding)	Select the Source for the Input:
	• **TS over UDP**: MPEG2 Transport Stream over UDP (no RTP header, default)
	
	⚠️ **Note**
	On networks with multiple sources targeting the same Kraken TS over UDP Input on either:
	a. the same multicast address and port simultaneously, or,
	b. the address and port of the Kraken instance simultaneously,
	Kraken will automatically latch onto one available source and ignore the other sources. If the current latched source is idle for 10-15 seconds, Kraken will select an alternate source. This functionality applies to both unicast and multicast reception.
	
	• **TS over SRT**: Haivision's Secure Reliable Transport. See SRT (Secure Reliable Transport).
	• **RTSP**: (Real Time Streaming Protocol) Select to configure Kraken to interoperate with ISR "sensors" such as wearable IP cameras, which are typically H.264 RTP/RTSP. See NOTE: below.
	  • As of Release 3.1, you may configure Kraken to transmux RTSP input to TS/UDP or TS/SRT output using Bypass mode.
	
	⚠️ **Note**
	Previous Kraken releases supported RTSP Input for H.264 video only under the following conditions:
	• Stream authentication through RTSP URL (username and password)
	• H.264 video instance selection through RTSP URL
	
	  • As of Release 3.2, you can select transport options equivalent to `ffplay` command line arguments for RTSP input including TCP, UDP Multicast and HTTP tunneling.
	• **Raw Motion JPEG**: Allows you to input a Motion JPEG (MJPEG) live stream and transcode the payload into a standard H.264 or HEVC video within an MPEG Transport Stream.
	• **RTMP**: (Real-Time Messaging Protocol) Select to configure Kraken to input RTMP streams in Bypass mode. See Connecting an RTMP Input Source.
	• **MJPEG over HTTP**: Allows you to input MJPEG video streaming over HTTP.
	To configure MJPEG over HTTP, select MJPEG over HTTP as the Source and then enter the URL. Both IPv4 and IPv6 URLs are supported, and they must contain either 'http://' or 'https://' as part of the string.
	
	⚠️ **Note**
	MJPEG over HTTP inputs are only compatible with transcoder mode, and cannot be used in a stream if the mode is set to Transcoder+Passthru or Bypass.

Input Setting	Description/Values
Source (Encoding)	• **ST2110**: Select to capture and encode SDI input using an SFP (Small Form-factor Pluggable) SDI to IP gateway device on Kraken running as a VM on third party hardware. Setup instructions to route data from the SFP device to Kraken are provided in the **Kraken OVA Deployment Guide**. • **GigE Vision**: Select to support the GigE Vision input (Kraken must be licensed for GigE Vision). ⚠ **Note** The GigE Vision standard specifies that only one client can control a GigE Vision device. Please ensure that other software applications are not controlling the GigE Vision device specified in the Kraken input. • **NDI**: Select to support Network Device Interface input (Kraken must be licensed for NDI input). To select the appropriate port for your NDI input, consult the following table: **[Port table below]** ⚠ **NDI Sources** NDI sources may interfere with Kraken inputs from other sources. For best performance we recommend running NDI streams on a separate Kraken appliance, or using a port range beneath 5959 to allow the dynamic port range usage of NDI to co-exist with other streams. • **SDI DeckLink Micro Recorder 1** (Kraken CR or SDI capture card must be installed): Select to capture HD/SD-SDI video for baseband input encoding. • **Analog Capture 1** (Kraken CR or Analog Composite capture card must be installed): Select to capture Analog Composite Video for baseband input encoding.

NDI port table (within the Source row):

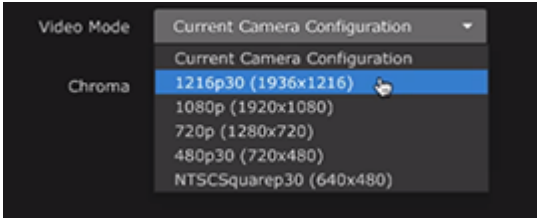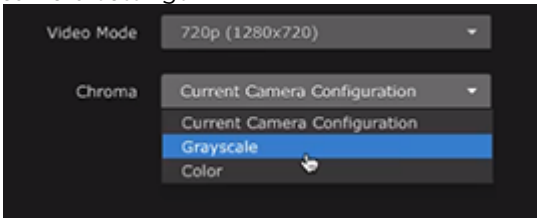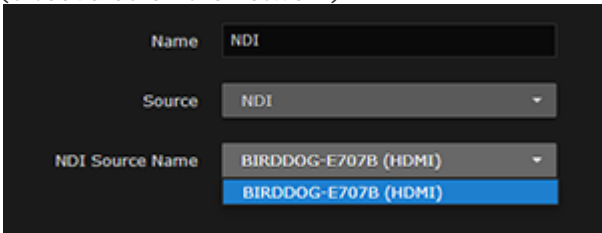| Port Number	Type	Use
5353	UDP	Standard mDNS port used to scan for NDI hosts on the local network and report their hostnames.
5959	TCP	Used by NDI Discovery Server as an alternate means to mDNS.
5960	TCP	NDI hosts listen on this port for configuration/status. Used for remote queries of NDI sources on this listening host.
5961+	TCP	Base TCP connection for each NDI stream for configuration/status. One port is used for each current connection.
5960+	UDP	Used for reliable UDP connections for configuration/status. Port range also used in NDI Connection Sharing.
6960+	TCP/UDP	NDI hosts receive data from one port within this range for each connection.
7970+	TCP/UDP	NDI hosts send from this one port within this range for each connection.

Input Setting	Description/Values
URL	(Source must be TS over UDP, RTSP, RAW Motion JPEG, or MJPEG over HTTP) Type in the source URL for the Input, for example, `udp://239.100.100.100:5000` Examples of supported input formats: • `udp://239.100.100.100:5000` = multicast UDP to 239.100.100.100 port 5000 • `udp://:5000` = unicast UDP. Allows an inbound stream to be sent to this server's IP address on port 5000 • `tcp://10.66.132.20:4045` = unicast TCP on 10.66.132.20 port 4045 • `rtsp://10.66.162.133/axis-media/media.amp` = RTSP input • `http://192.168.0.202:9000` = MJPEG over HTTP input to 192.168.0.202 on port 9000 • `rtmp://mediaserverdemo.leadtools.com:80/vod/sample.mp4` ⚠ **Note** Kraken input streams may be UDP unicast or multicast, or TCP unicast.
Source Specific Multicast	(Source must be TS over UDP or Raw Motion JPEG, and source IP address must be IPv4) Type in a specific source device IP address. ⚠ **Note** Kraken supports IGMPv3 Source Specific Multicast reception, which allows input streams to join a multicast group and filter the input streams based on a specific source IP address. Only streams originating from the specified source IP will be forwarded to Kraken. This allows Kraken to quickly and easily select an input stream in environments with many sources sharing a common multicast IP. When the receiving device specifies a source device IP address, the IGMP protocol will filter out devices that use the same multicast group address and only forward the traffic with the specified source IP address as well the destination IP multicast address to the requesting destination device.
Network Interface	(Source must be TS over UDP) Select the network (Ethernet) interface for the Input, either: • Auto (default): Uses static route, if defined; otherwise uses the default • eth0 • eth1 • ... ⚠ **Note** Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/..., pNp1/pNp2/..., or em1/em2/.... To configure customized names for the network interfaces, as shown in the following example, see "User Description" under **Network Settings**. ⚠ **Caution** Because input multicast listening routes are based on IP addresses, do not reuse the same address even if it is assigned to different NICs. Doing so would produce corrupted output in all associated sessions.

Input Setting	Description/Values
Transport	(Source must be RTSP) Select the transport mode for the Input, either: • Auto (default): • UDP • TCP • UDP Multicast • HTTP
Mode	(Source must be RTMP) Select either Client or Server depending on the RTMP source. See **Connecting an RTMP Input Source**.
Port	(Source must be RTMP and Mode set to Server) Type in the source port number for the Input.
IPv6	(Source must be RTMP and Mode set to Server) Check the checkbox to enable IPv6 addresses.

General   **SRT Inputs**   **Encoding Inputs**

SRT Input Settings

Input Setting	Description/Values
Mode	Select the SRT Connection Mode: • Caller: Kraken acts like a client and connects to a server listening and waiting for an incoming call. • Listener (default): Kraken acts like a server and listens & waits for clients to connect to it. • Rendezvous: Allows calling and listening at the same time. ⚠ **Note** To simplify firewall traversal, Rendezvous Mode allows Kraken and the encoder to traverse a firewall without the need for IT to open a port.
Address	(Caller and Rendezvous Connection Modes) Type in the destination IP address for the SRT stream. ✅ **Tip** You can also enter a Fully Qualified Domain Name (FQDN).
Source Port	(Caller Connection Mode) Specifies the UDP source port for the SRT stream. If not filled in, a (default) source port will be assigned. ⚠ **Note** This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.
Destination Port	(Caller and Rendezvous Connection Modes) Specifies the UDP destination port for the SRT stream.
Port	(Listener Connection Mode only) Specifies the UDP local port for the SRT stream.
Latency	Specifies how long Kraken will buffer received packets. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20-8000 ms; Default = 125 ms Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.
Passphrase	(Optional, must match encoder passphrase) This parameter is required if the stream is encrypted and is used to retrieve the cryptographic key protecting the stream. Range = 10-79 UTF-8 characters
Notes	(Optional) Type in any related information or comments.

General   **SRT Inputs**   **Encoding Inputs**

Encoding Input Settings

Input Setting	Description/Values
ST2110 Capture	
Address	(Source must be ST2110) Type in the IP address or hostname of the SFP SDI→IP gateway.
IP Port	(Source must be ST2110) Type in the IP Port of the SFP SDI→IP gateway. Range: 0, 65535
Device Port	(Source must be ST2110) Type in the Device Port of the SFP SDI→IP gateway. Range: 1,4
Connection	Displays the connection status as the remote source device ethernet IP, the device IP port, and device interface port (`device_address : device_ip_port (device_port)`) when connected to a stream.
GigE Vision Capture	
Device Address	(Source must be GigE Vision) Type in the GigE Vision camera IP address or hostname. Kraken then registers the device and populates the Video Mode and Chroma options. Note that there can only be one input configuration per device (camera).
Video Mode	(Source must be GigE Vision) Select the video mode from the drop-down list of available resolutions and frame rates, or use the current camera settings.
Chroma	(Source must be GigE Vision) Select the chroma value from the drop-down list, or use the current camera settings.
Connection	Displays the connection status as the remote source device address (`gigevis_address`) when connected to a stream.
NDI (Network Device Interface)	
NDI Source Name	(Source must be NDI) Select the NDI source name from the drop-down list of NDI devices (discovered on the network).

SDI DeckLink Capture	
DeckLink Mode	(Source must be DeckLink) Select the capture card mode, either: • Autodetect (default) ⚠️ **Note** DeckLink inputs start up and match the input regardless of whether Autodetect is set or the chosen inputs match. When set to Autodetect, Kraken attempts to detect the input resolution and frame-rate. If the input resolution and frame-rate cannot be detected, then you have the option of providing a resolution and frame-rate hint to the DeckLink card so as to allow the DeckLink card to lock on the input signal. The selected DeckLink input resolution and frame-rate must match the actual input resolution and frame-rate for the signal to be correctly recognized and processed. ✅ **Tip** Autodetect may not work correctly for some cameras. For instance the capture card may detect a wrong mode. Also the capture card may not detect all sources for all modes. For instance, it may correctly detect a certain camera when it is in 720-60p but not when it is in 720-50p. Therefore, we recommend that you use Autodetect mode when possible and when it works, and use the manual mode selection if necessary. Also, some capture cards do not support "Autodetect" in which case only the supported modes of the capture card will be listed and can be selected. • Manually select the resolution.
Analog Capture	
Analog Capture Mode	(Source must be Analog Capture) Select the capture card mode, either: • Autodetect (default) • Manually select the display system (NTSC, PAL, etc.)

Related Topics

- **Input Statistics**
- **Connecting an RTMP Input Source**

Input Statistics

The Input Statistics page shows statistics for the selected SDI (DeckLink) or Analog Capture encoding input.

> ✅ **Tip**
>
> You can access statistics for other input types from the Streams Statistics page, including SRT Input Statistics graphs. For more information, see **Viewing Kraken Statistics**.

Connecting an RTMP Input Source

Kraken supports RTMP input and output in Bypass mode. When installed as a VM and deployed to Azure, Kraken can now serve as a stream router for local distribution within industrial complexes as well as across the public internet to serve remote monitor sites.

> ⚠ **Note**
>
> RTMP input and output are *not* supported in "Transcode" or "Transcode + Passthru" mode.

Kraken supports either server or client RTMP input streams:

- Server — Stream sent directly to the Kraken's IP address
- Client — Stream available for Kraken to access on an RTMP server

The procedure for configuring an RTMP server input is shown below:

1. On your source streaming device, output an RTMP stream with the following URL format:

   `rtmp://<IP>:1935/live/<stream_name>`

   where, `<IP>` is the IP address of the Kraken and `<stream_name>` is the desired name of the stream.

   > ⚠ **Note**
   >
   > For RTMP Server mode, the port must be 1935 and the Application Name must be "live".

2. On Kraken, create a new input. See **Configuring Input Parameters** for more details. On the New Input screen:
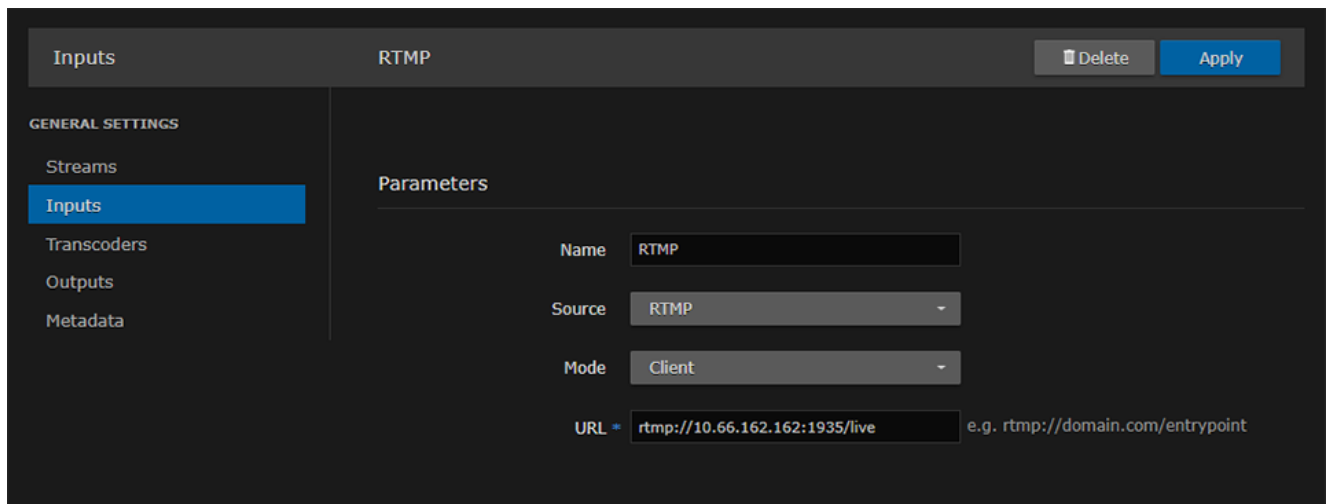
   a. Type in the input name and select **RTMP** for the Source.
   b. Select either **Server** or **Client** for Mode depending on the RTMP source.

   > ⚠ **Note**
   >
   > In Client mode, you need to enter your own RTMP URL. In Server mode, it is constructed internally by Kraken.

   c. Enter the URL of the RTMP stream created in Step #1 above.

3. Click **Apply**.

Configuring Transcoders

You must first define one or more Transcoders before you can define a Stream. Each Transcoder is a user-defined set of parameters to apply when re-encoding the audio/video.

> ⚠ **Note**
>
> Transcoding is defined as the process of converting an encoded media stream or object from one format to another. This may be done in cases where a target device (or workflow) does not support the format, has limited network bandwidth or storage capacity that mandates a reduced stream size, or to convert incompatible or obsolete data to a better supported or modern format.

Transcoders List View

The Transcoders List view displays a summary of defined transcoders for Kraken, including the Name, Resolution, Video Bitrate, Group of Pictures (GOP) size, Audio enable setting, and State for each transcoder. It also provides an option for you to delete transcoders.

To open the Transcoders List View:

1. On the Streaming page, click **Transcoders** on the sidebar.
   The Transcoders List View opens, as shown in the following example.
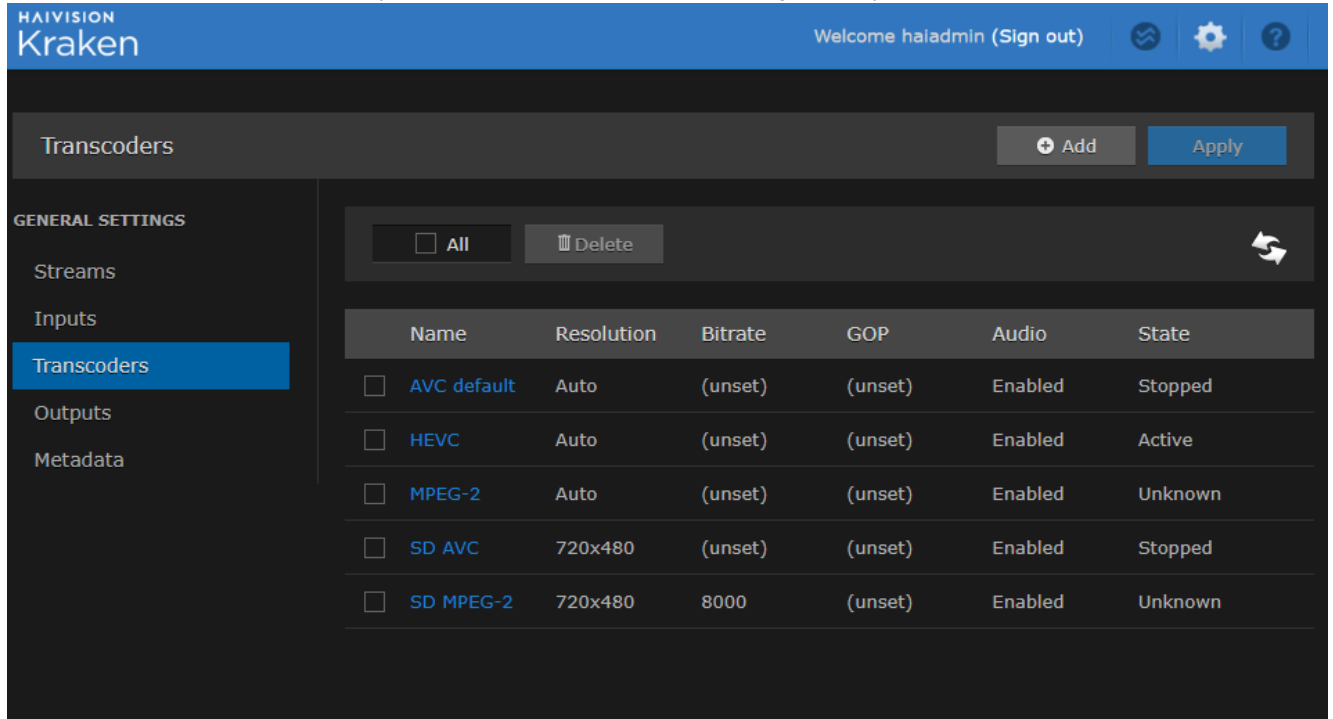
- To refresh the page, click ⟳.
- To add a transcoder, click the ⊕ **Add** button.
- To view transcoder details or add a transcoder, click a line in the table to open the Transcoders Detail View.
- To delete one or more existing transcoders, check the checkbox(es) next to the item(s) in the list and click the 🗑 **Delete** button.
2. To apply your changes, click **Apply**.

Related Topics

- **Configuring Transcoder Parameters**

Configuring Transcoder Parameters

Transcoder Settings include the Encoder (processor), Format (video compression standard), Video Bitrate and Resolution, KLV Metadata pass-through, Frame Rate, GOP size, Audio Bitrate, Stream Shaping, and Output Pacing. Optional advanced settings are available to fine-tune Stream Shaping. The parameters vary depending on the Encoder and Format selected.

> ⚠ **Note**
>
> If the Resolution fields are left blank or unchanged in the Transcoders section, the resolution of the source stream will remain intact in the outbound stream. However, the GOP Size and Bitrate are set to a default value based on the resolution.

KLV Options

With KLV (Key Length Value) input, you can also configure the transcoder to reduce the KLV data rate by frame-decimating the KLV metadata and/or filtering out data fields from MISB 0601 UAS KLV metadata. This is useful to lower the amount of bandwidth consumed by metadata and thereby allow higher video bitrates within bandwidth-constrained ISR workflows.

- KLV Rate Decimation causes Kraken to ingest KLV metadata at one KLV frame rate and decimate it to another rate. You select the factor (1:N, N=1..60), and then (N-1/N) metadata frames are dropped and only 1/N frames are passed through to the Output Stream. (See "KLV Decimation" under **Transcoder Settings**)
- KLV Tag Filtering filters out selected data fields from MISB 0601 UAS KLV metadata. You select either a 0601 minimum UAS metadata set or a 0601 minimum security set, or you can define a custom set by removing tags for fields deemed not relevant to your operation. (See **Filtering UAS KLV Metadata Tags**)

> ⚠ **Note**
>
> KLV metadata insertion and KLV decimation/filtering are mutually exclusive. If metadata insertion is specified, it will override KLV tag filtering.

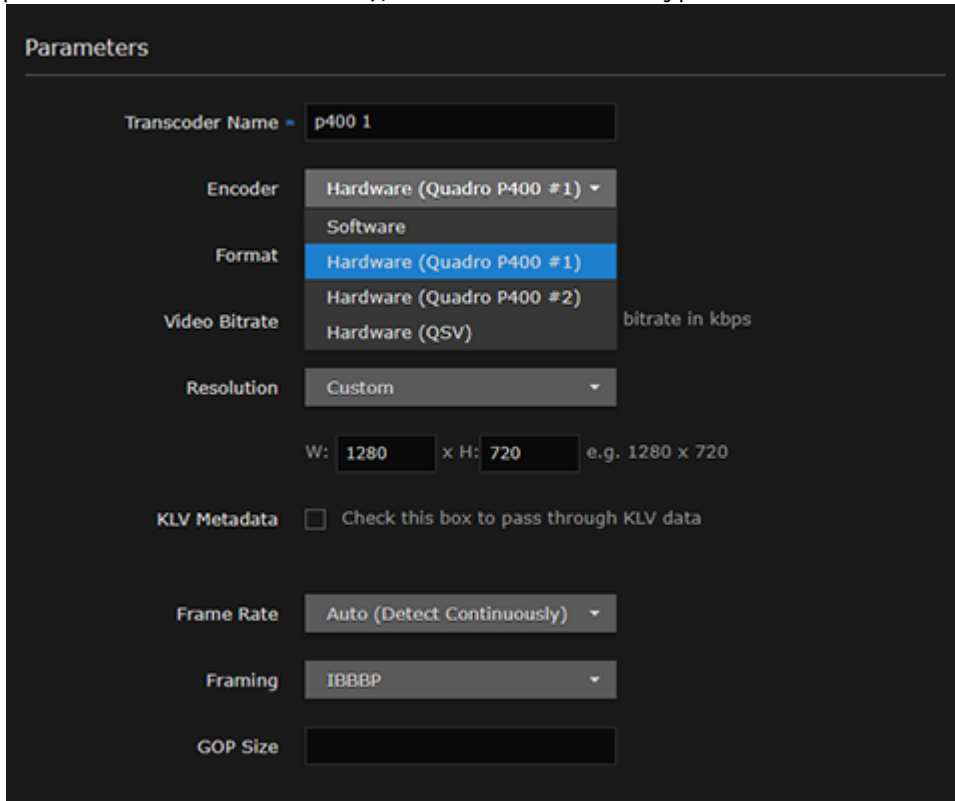To view and configure Transcoder parameters:

1. From the Transcoders List view, click the ⊕ **Add** button or click any line in the table.

2. On the Transcoders Detail View, type in a unique name for the transcoder.

3. (Optional) To enable hardware acceleration on qualified hardware (such as QSV-capable processors or NVIDIA GPUs), select the Encoder type.

4. Select or enter values in the fields to define the transcoder (i.e., to change in the outbound stream), for example, the Format, Video Bitrate, or Resolution. For details, see **Transcoder Settings**.
5. To pass through KLV data, check the KLV Metadata checkbox.
6. To enable audio on the outbound stream, check the Audio checkbox.
7. Select or enter values for the Advanced Parameters. For details, see **Advanced Parameters** in **Transcoder Settings**.
8. (Optional) If Transport Stream Shaping is enabled (under Advanced Parameters), you can define additional parameters, as shown in the following example. For details, see **Advanced Shaping**
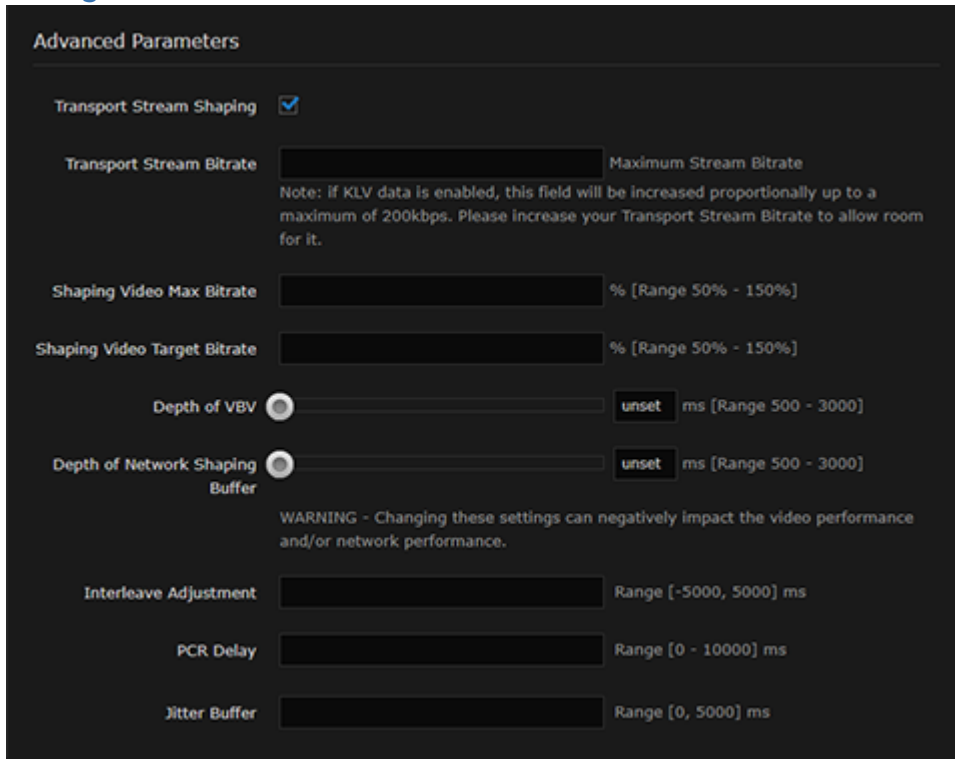
Settings.

9. To configure KLV Rate Decimation, select By Factor for Decimation and then select the factor from the drop-down list. See "Decimation" (under "KLV Decimation Settings") in Transcoder Settings.
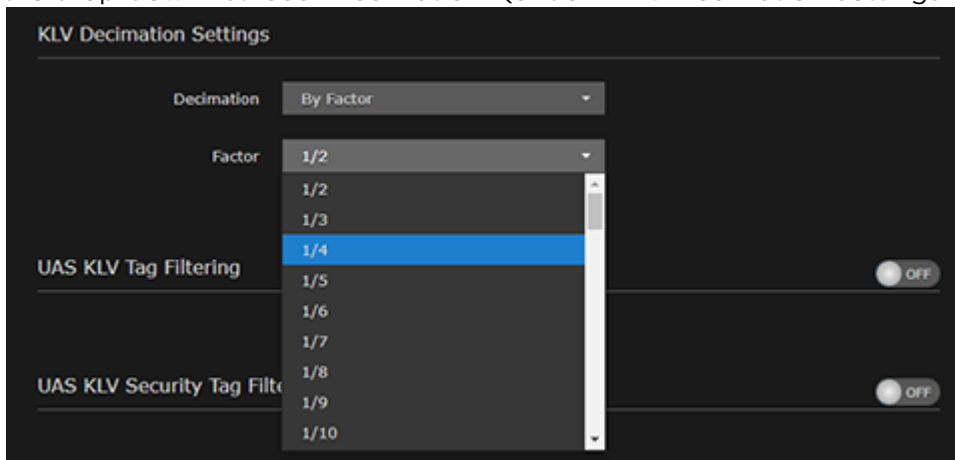
10. To configure UAS KLV Tag Filtering or UAS KLV Security Tag Filtering, see Filtering UAS KLV Metadata Tags.
11. To apply your changes, click **Apply**.

The new transcoder is added to the Transcoders List.

Related Topics

- Transcoder Settings
- Audio/Video Characteristics

Transcoder Parameters for RTSP

Transcoder settings should be taken into consideration when creating RTSP outputs (either PUSH or PULL). To ensure the compatibility of RTSP outputs with certain Video Management Systems (VMS) like those from Milestone or Genetec, we recommend using the following Transcoder parameters.

1. Video Parameters:
   - Use Hardware or Software encoder based on Kraken instance capabilities
   - **Format**: H.264 (AVC)
   - **Video Bitrates**: between 2000kbps and 6000kbps (depending on desired stream quality)
   - **Resolution Frame Rate**: as desired
   - **KLV Metadata**: optional
   - **Framing**: IP Framing (to minimize latency)
   - **GOP size**: 60-200 frames
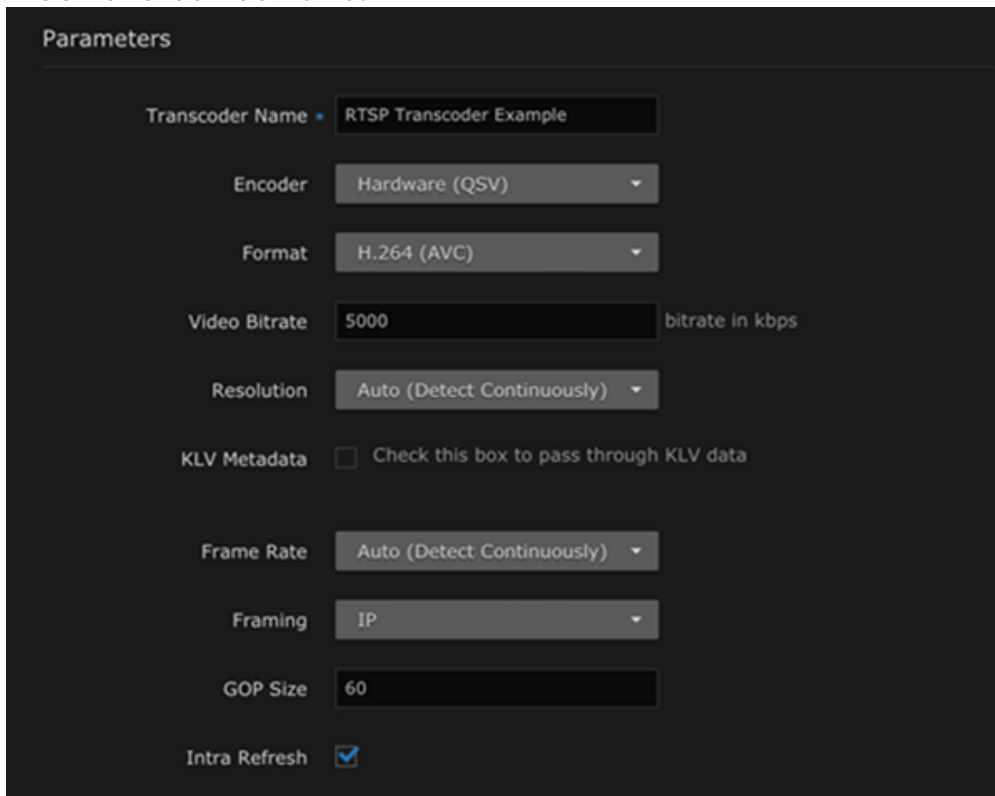
2. Audio Parameters:

   > ⓘ **Info**
   >
   > Including audio is optional.

   - **Audio Codec**: MPEG2 AAC ADTS
   - (If connecting to Milestone) Connect Milestone audio to the configured stream and specify AAC as the Audio Codec

Related Topics:

- **Configuring RTSP Outputs**
- **RTSP Server Service**

Filtering UAS KLV Metadata Tags

You can configure the transcoder to filter out data fields from MISB 0601 UAS KLV metadata in order to reduce the KLV data rate. Lowering the amount of bandwidth consumed by metadata allows higher video bitrates within bandwidth-constrained ISR workflows.

You can filter MISB 0601 metadata tags on a per tag basis, by specifying all or any subset of the MISB 0601 tags. If a tag is included, it is allowed to proceed to the metadata elementary stream (ES). Tags that are not included are filtered out of the metadata AU and not transmitted in the metadata ES. Non-MISB 0601 metadata (such as MISB 0605 or custom metadata adhering to SMPTE 336) is not affected by the MISB 0601 filtering.

When filtering MISB 0601 metadata tag 48 (security metadata), you can also filter the security metadata tags defined in MISB 0102.

This is useful to eliminate unwanted KLV information in order to minimize the metadata bandwidth required. You may choose to down-scale and frame-decimate the video and decimate the metadata as well.

> ✅ **Tip**
>
> Frame decimation on the video is accomplished by reducing or down-scaling the frame rate of the encoder on the Transcoders page.

To filter UAS KLV metadata tags:

1. From the Transcoders List view, click the link for the transcoder to filter.
2. On the Transcoders Detail View, check the KLV Metadata checkbox to pass through KLV data.
3. To filter MISB 0601 metadata tags, scroll down and toggle the UAS KLV Tag Filtering button to **On**.
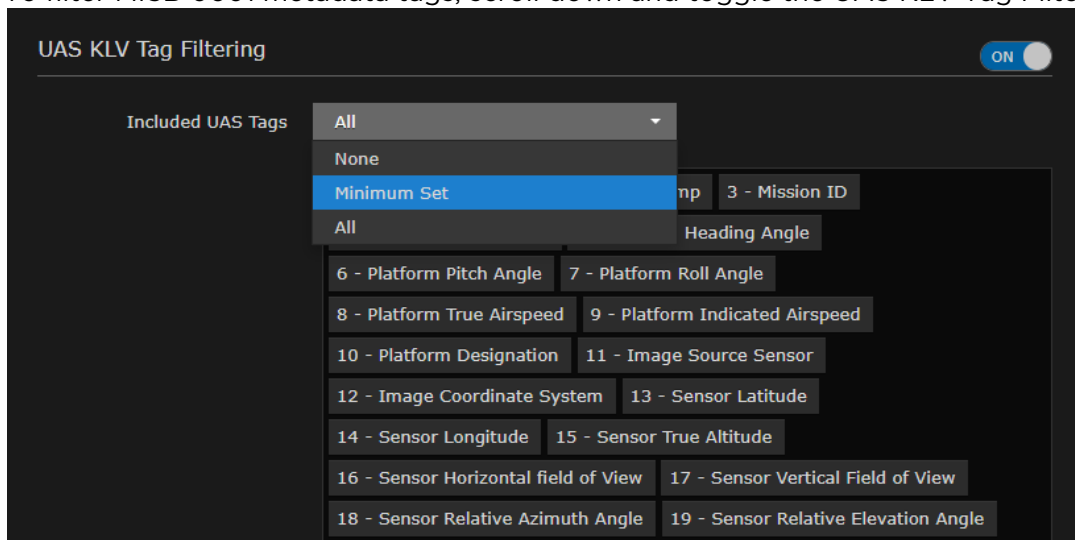
4. To configure the scope of filtering, select either Minimum Set or All from the Included UAS Tags drop-down list.
   • To remove tags for fields deemed not relevant to your operation, browse through the list and click **X** next to any tag labels to exclude, i.e., to filter out of the metadata. This creates a new option "Custom Set" on the Included UAS Tags drop-down list.

- To re-include a tag that has been excluded, click the down arrow at the bottom right of the list box and select the tag from the drop-down list of excluded tags.

5. To filter the security metadata tags defined in MISB 0102, toggle the UAS KLV Security Tag Filtering button to **On**, select Minimum Set or All, and fine-tune the Included Security Tags list as required to configure the scope of filtering.

> ✅ **Tip**
>
> Make sure #48 is included under UAS KLV Tag Filtering.

6. Fill in the remaining fields and click **Apply**.

Related Topics

- **Configuring Transcoder Parameters**

Transcoder Settings

The following table lists the Kraken Transcoder settings:

Basic Parameters   **Audio Parameters**   **Advanced Parameters**   **KLV Decimation**

UAS KLV Tag Filtering

Basic Parameters

Transcoder Setting	Description/Values
Transcoder Name	Enter a unique name for the transcoder. This name will be selectable from the list of Transcoders when you define a stream.
Encoder	(Optional, to enable hardware acceleration on qualified hardware, if detected) Select the encoding type, either: • Software (default, Kraken legacy): CPU-based encoding • Hardware (QSV): Video encoding will be hardware accelerated using the Intel Quick Sync Video capabilities of the processor. • Hardware (*name* #n>): Enables encode processing from the Kraken transcoder to be handled by NVIDIA GPUs. Assumes Kraken is running as a VM in an ESXi 6.5+ environment. Offloads the transcoding processing to the NVIDIA GPUs so that the server CPU remains free to be utilized by other applications. See **Kraken OVA Deployment Guide**. ✅ **Tip** Capabilities of the particular NVIDIA card dynamically affect available (basic) parameters, for example, NVIDIA does not support Intra-refresh or B-frames.
Format	Select the video compression standard for the outbound stream, either: • H.264 (AVC) (default) • H.265 (HEVC) • MPEG-4 (Part 2) • MPEG-2: The stream will be transcoded to MPEG-2 Video (ISO/IEC 13818-2) and MPEG-1 or MPEG-2 audio with closed captioning pass-through. This allows Kraken to inter-operate with legacy systems.
Codec Profile	(Format must be MPEG-2 or MPEG-4) Select the video profile for the encoder: • Auto: Defaults to Main profile. • Simple: Specifies that the output encoded video will adhere to the ISO/IEC 13818-2 / MPEG-2 Simple Profile. • Main: Specifies that the output encoded video will adhere to the ISO/IEC 13818-2 / MPEG-2 Main Profile.
Video Bitrate	Type in the Video Bitrate in kbps for the outbound stream, for example, 1024. Range = `1..100000`

Transcoder Setting	Description/Values
Resolution	Select the resolution for the outbound stream: • Auto (Detect Continuously) (default) • Auto (Detect on Stream Start) • Custom: Type in a horizontal and vertical (W x H) resolution, for example, 1280x720. ⚠ **Note** To maintain the resolution of the outbound stream that was detected at stream start (even if the input resolution changes), select "Auto (Detect on Stream Start)". 720x576 or lower is considered SD resolution. ✅ **Tip** With NVIDIA encoders, Kraken provides validation of custom resolutions and notification when a stream exceeds supported resolutions.
KLV Metadata	Check this checkbox to enable KLV metadata passthrough. ⚠ **Note** Disabled if KLV isn't licensed.
Frame Rate	Select the coded picture frame rate per second (fps): • Auto (Detect Continuously) (default) • Auto (Detect on Stream Start) • Select a frame rate from the list: 60..1 ⚠ **Note** In previous releases, selecting "Auto" caused the frame rate of the outbound stream to be what was detected at stream start. The legacy "Auto" setting has been renamed "Auto (Detect on Stream Start)" since it does an early detection of the input frame rate and uses that as the fixed output frame rate for the transcoder. The new default "Auto (Detect Continuously)" is an additional encoding/transcoding mode where the output Frame Rate follows the source frame rate. This mode monitors the incoming frame rate and if it can detect a steady frame rate that differs from the one it is currently using, it resets the video encoder and configures it accordingly.
Framing	Select the number of B-frames and B reference frames per P-Frames to allow in the output stream: • Auto (default): The Kraken software decides how many B-Frames and B reference frames to allow • IP: I and P frames only (lowest delay; lowest quality) • IBP: I, B and P frames • IBBP: I, BB (two B-frames and B reference frames in sequence) and P frames (higher delay; higher quality) • IBBBP: I, BBB (three B-frames and B reference frames in sequence) and P frames (highest delay; highest quality) ⚠ **Note** B-Frames improve the quality by increasing the efficiency of the encoding, thus allowing higher quality at the same bitrate. But B-Frames increase the encoder processing overhead, e.g., higher CPU utilization of the encoder.

Transcoder Setting	Description/Values
GOP Size	Type in the GOP (Group of Pictures) Size for the outbound stream, for example, 30. Range = `0..1000` ⚠️ **Note** You may choose to adjust the GOP to get different video quality on the outbound stream or to make the stream compatible with a different system than the original stream was intended for. ✅ **Tip** Increasing the GOP size can increase the time required for a player to tune into the stream. Reasonable GOP sizes tend to range from half the frame rate to up to 5 times the frame rate. A GOP size equal to the output frame rate is a good rule of thumb.
Intra Refresh	Check this checkbox to enable Intra Refresh for X.264 and X.265. This is an advanced feature that puts the encoder into a mode where it does not generate I-Frames. Instead the individual macro blocks are refreshed and over time all of the picture is refreshed. This eliminates I-Frame bitrate spikes and smooths the bitrate over the GOP interval. The GOP parameter is still used as a basis for the refresh interval. ⚠️ **Note** Not all decoders may support this feature so it can be enabled/disabled as desired.

Basic Parameters   Audio Parameters   Advanced Parameters   KLV Decimation

UAS KLV Tag Filtering

Audio Parameters

Transcoder Setting	Description/Values
Audio	Check this checkbox to enable audio on the outbound stream. ✅ **Tip** Kraken will automatically insert a silent audio stream into the output when the input source has no audio (see "Silent Audio Insertion" under **Recommended Start Settings for Advanced Shaping Settings**). ⚠️ **Note** When audio is removed on the outbound stream, the PID for the audio track is removed, as is the reference to it in the PMT.
Audio Codec	Select the audio compression algorithm: • Auto: Defaults to MPEG1 Layer II • MPEG1 Layer II: Encodes audio using the ISO/IEC 11172-3 / MPEG-1 Layer II algorithm. • MPEG2 AAC ADTS: Encodes audio using the ISO/IEC 13818-7 / MPEG-2 AAC-LC algorithm with an ADTS header.
Audio Bitrate	Type in the Audio Bitrate in kbps for the outbound stream, for example, 128. Range = 14..576 Kbps

Basic Parameters   Audio Parameters   Advanced Parameters   KLV Decimation

UAS KLV Tag Filtering

Advanced Parameters

Transcoder Setting	Description/Values
Performance Control System	(Video Format must be HEVC) Check this checkbox to enable the Performance Control System, an HEVC encoder feature that dynamically monitors the runtime performance of the encoder and adjusts the video encoder quality based on the instantaneous performance of the encoder. The goal is to provide optimal quality of the video encoder based on the performance of the system. It is particularly useful on small form factor (i.e., lower power) systems such as Kraken CR.

Transcoder Setting	Description/Values
Transport Stream Shaping	Check this checkbox to enable Shaping on the outbound stream. Checking this checkbox also displays advanced settings (see Advanced Shaping Settings). ⚠️ **Note** Traffic Shaping is used on some networks to smooth the traffic and respect the absolute upper limit configured. When Shaping is enabled, you can set the Maximum Bitrate for the Transcoder Stream (see Transport Stream Bitrate in Advanced Shaping Settings). ✅ **Tip** When Shaping is enabled, the Video Bitrate becomes the ceiling video bitrate target. When Shaping is disabled, this parameter represents the average video bitrate.
Output Pacing	(Kraken appliances only. Transport Stream Shaping must be disabled.) Check this checkbox to enable Output Pacing on the outbound stream. ⚠️ **Note** Output Pacing is used to make the traffic more or less smooth on the network, to allow the stream traffic to leave the Kraken in a more even manner. When pacing is enabled, you can set the Output Pacing Buffering Interval (see below).
Output Pacing Buffering Interval	(Output Pacing must be enabled) This Buffering Interval defines the depth of the Output Pacing in milliseconds (ranging from 0 to 1000ms). It is used to define the latency and smoothness added by the output pacing. You can either type in a value between 0 and 1000 ms. in the text box, or move the slider to the desired value. ⚠️ **Note** The higher the buffer is set, the more smooth the traffic is on the network. However, the optimal buffer setting will depend on the "spikiness" of the source stream.
Interleave Adjustment	(Optional) Type in the number of milliseconds to delay audio before multiplexing ("muxing"). Range = `-5000, 5000ms` • 0 (Default Value). No interleaving adjustment. • > 0 specifies the number of milliseconds to delay audio before muxing. • < -1 Number of milliseconds to delay video before muxing. ⚠️ **Note** Interleave adjustment is actually a muxer interleave adjustment of the packets without touching timestamps and does not affect AV sync. ✅ **Tip** The latency within the transcoder pipeline is higher for the video than the audio, so users typically want to delay the audio so that the video comes out of the muxer before the corresponding audio. By default, the transcoder attempts to adjust the interleaving to some appropriate value. This control allows you to override that when desired.

Transcoder Setting	Description/Values

PCR Delay	(Optional) Type in the number of milliseconds to delay the PCR (Program Clock Reference) behind the STC (System Time Clock). The PCR is the clock reference that is contained in the **MPEG transport stream**. It is used to signal to downstream decoders a consistent clock by which to time other media essences (such as audio, video, closed captioning, and metadata).
	
	✅ **Tip**
	This setting may be used to fine-tune stream timing for sensitive downstream decoder systems on streams with high relative delay between audio and video data within an MPEG2 Transport Stream.
	
	Range = `0, 10000ms`
	• 500 (Default Value)
	• Target Ranges:
	  • IPTV: 2,000 <=> 5,000
	  • ISR: 300 <=> 1,000
	• Increasing the value may incur additional latency at the player (i.e., larger buffers at the player):
	  • Greater than 5000 may cause unintended issues with remote players.
	  • Lower than 300 may introduce unstable audio playback issues.

Jitter Buffer	(Optional) Type in the Jitter Buffer for the inbound source/stream. A jitter buffer may be applied to video streams coming in at irregular intervals to help output the video in a steady stream (default = 250 ms). Range = `0, 5000ms` ⚠️ **Note** Transcoding latency will be affected proportionately.

Basic Parameters   **Audio Parameters**   **Advanced Parameters**   **KLV Decimation**

UAS KLV Tag Filtering

KLV Decimation

Transcoder Setting	Description/Values
Decimation	(KLV Metadata pass-through must be enabled) Select "By Factor" to frame-decimate ingested KLV messages to reduce the bandwidth used by the metadata service. • None • By Factor: `1/2..1/60` ⚠️ **Note** 1/2 means divide the amount by half, etc.
Factor	("By Factor" must be selected) Select the decimation factor.

Basic Parameters   **Audio Parameters**   **Advanced Parameters**   **KLV Decimation**

UAS KLV Tag Filtering

UAS KLV Tag Filtering (See Filtering UAS KLV Metadata Tags)

Transcoder Setting	Description/Values
UAS KLV Tag Filtering	(KLV Metadata pass-through must be enabled) Specifies a list of tag numbers/labels from the UAS Datalink Local Set that are allowed to be streamed. Tags not included in this list will be discarded. Select either: • None • Minimum Set: the set of metadata objects as define in MISB 0902. • All: the set of metadata objects as defined in MISB 0601.
UAS KLV Security Tag Filtering	Specifies a list of tag numbers/labels from the Security Local Data set inside the UAS that are allowed to be streamed. Tags not included will be discarded. Select either: • None • Minimum Set: the set of metadata objects as define in MISB 0902. • All: the set of metadata objects as defined in MISB 0102. ✅ **Tip** #48 must be included under UAS KLV Tag Filtering.

⚠️ **Note**

An asterisk (*) next to a field indicates that it is required.

Related Topics

- **Advanced Shaping Settings**
- **Filtering UAS KLV Metadata Tags**

Advanced Shaping Settings

> ⚠️ **Caution**
>
> Changing these settings can have a negative impact on the video performance and/or network performance.

> ✅ **Tip**
>
> See Recommended Start Settings for Advanced Shaping Settings.

Advanced Setting	Description/Values
Transport Stream Bitrate	(Transport Stream Shaping must be enabled) Type in the Maximum Transport Stream (TS) Bitrate in kbps for the outbound stream, for example, 3000. Kraken automatically generates a minimum value based on the Video Bitrate, Audio Bitrate and whether or not there is KLV metadata. This minimum value may be used by default, or you may set the Maximum TS Bitrate to a higher value (but not lower). ⚠️ **Note** If KLV metadata pass-through is enabled, 200 kbps will be added to the Maximum TS Bitrate value by default. If your site is utilizing KLV streams that are higher than 200 kbps, you should increase the Maximum TS Bitrate value to make room for the KLV stream. For example, to use a 1 Mbps KLV stream, you should increase the Maximum TS Bitrate by 800 kbps to allocate enough room in the Kraken output stream for the KLV, Audio and Video. ✅ **Tip** If the encoder is overrunning the ceiling bitrate and you have room in the channel to spare, you can increase this value, which allows more room in the channel for higher spikes in the encoder. By default, the Web Interface tries to set this to 20% above the expected aggregate bitrate of the elementary streams. For instance, it adds the Video Bitrate, Audio Bitrate, and expected KLV bitrate and adds 20%. This can be increased, but should probably not drop below 12%. You need at least 3% and sometimes more for the TS packetization and PSI tables, etc.
Shaping Video Max Bitrate	Type in the maximum video bitrate for shaping the outbound stream, as a percentage. Range = 50% - 150% ⚠️ **Note** Increasing this above 80% will increase the quality, but also increases the probability that the encoder will overrun the ceiling. At higher bitrates, it should be possible to increase this to 85%. ✅ **Tip** You can try setting this to 90% or higher to see where you start observing problems due to overrunning the network buffers. In most situations, you should not exceed 100%. The optimal setting is reached when this value is as close to 100% as possible without overrunning the buffers. This depends on a large number of factors, including Bitrate, Frame Rate, GOP size, Resolution, scene complexity, and VBV size.

Advanced Setting	Description/Values
Shaping Video Target Bitrate	Type in the target video bitrate for shaping the outbound stream, as a percentage. Range = 50% - 150% > ✅ **Tip** > > As a general rule, keep this at 70% for all operating points. It should be lower than the Shaping Video Max Bitrate and lower than 100%. 70% is fairly optimal for the Kraken's encoder.
Depth of VBV	Type in or adjust the slider to specify the value in milliseconds for the Video Buffering Verifier (VBV) depth. Range = 500 - 3000ms > ⚠ **Note** > > The VBV is a theoretical MPEG video buffer model used to ensure that an encoded video stream can be correctly buffered and played back at the decoder device. By definition, the VBV will not overflow nor underflow when its input is a compliant MPEG stream. > ✅ **Tip** > > This is the depth of the CBR buffer in the decoder VBV model in milliseconds. A value that you should strive for is 1000ms; lower values may decrease the rate at which the encoder overruns the network buffers at lower bitrates. Increasing this parameter increases latency and also increases quality. It should not be lowered below 1000ms. A good quality encoder will make intra frames 12- 15 times larger than non-intra frames. At 30fps, this means half of the stream bitrate is consumed for a single video frame. Since it must fit inside the VBV, the optimal point for our low delay application is 1000ms.
Depth of Network Shaping Buffer	Type in or adjust the slider to specify the value in milliseconds for the network shaping buffer depth. Range = 500 - 3000ms > ⚠ **Note** > > This is the depth in milliseconds of the network traffic shaper's buffers. Since a good quality encoder will generate an intra frame consuming approximately 50% of the available bitrate in one frame, this is the interval over which the bitrate spike of the intra frame is sent out over the network to keep it inside the channel bitrate. If the encoder overshoots this buffer, because the bitrate is too low for the resolution, frame rate, and/or scene complexity, the encoder will overrun this buffer. As a result, a decoder will receive a corrupt stream.

Recommended Start Settings for Advanced Shaping Settings

Following are the recommended start settings when using the Advanced Shaping settings:

Shaping Video Max Bitrate	100%
Shaping Target Bitrate	70%
VBV Size	1000ms
Network Shaping Buffer	1000ms

The goal should be to try and maximize the channel utilization (and thus the quality) while minimizing the shaping buffer overruns and minimizing the latency. Starting with the above values, you may try the following:

- Increase the bitrate percentages to improve quality.
- Increase the VBV and network shaping size to decrease bitstream drop based on shaping buffer overrun.

We do *not* recommend dropping the VBV and/or network shaping buffer much below 1000ms.

Silent Audio Insertion

Kraken provides a valid silent (blank) audio track, which may be inserted within streams that did not originally contain any audio, in order to achieve interoperability with receiving devices that need a valid audio track for clock recovery. Kraken will automatically:

- Insert a silent audio stream into the Kraken output when the input source has no audio.
- Utilize an audio stream from the source, should one become available after the transcoder session has started.
- Start silence injection should the audio stream become unavailable in the source after the transcoder session has started.
- Adapt to streams where the source audio stream becomes intermittently available and unavailable unexpectedly within the source (assuming the availability/non-availability of audio in the source stream does not change more rapidly than 30 second intervals).

> ⚠ **Note**
>
> There may be some transition artifacts. If you disable audio in the Transcoder session configuration, no silence injection will be performed.

Configuring Outputs

You must first define one or more Outputs before you can define a Stream. Each Output consists of a valid destination URL with an optional name and notes. The Output can also include settings such as the MTU (Maximum Transmission Unit), TTL (Time-to-Live), and ToS (Type of Service).

> ⚠️ **Note**
>
> In addition, you can select the network interface for the Output. Kraken may be configured to output streams to any of the available Network Interface Cards (NICs).

SAP

You can also enable Session Announcement Protocol (SAP) transmission for the stream to provide a playlist to viewers. SAP is a protocol for broadcasting multicast session information. An SAP announcer periodically multicasts an announcement packet to a well known multicast address and port. SAP listeners will listen on the well known SAP address and learn of all the sessions being announced.

When SAP is enabled, Kraken sends an SAP signal out to the player when it starts streaming. Any player that supports the SAP protocol will provide the end user an automatic playlist when Kraken is streaming.

Outputs List View

The Outputs List view displays a summary of defined outputs for Kraken, including the Output Name, Destination (output) URL, and Status for each output. It also provides an option for you to delete an output.

To open the Outputs List View:

1. On the Streaming page, click **Outputs** on the sidebar.
   The Outputs List View opens, as shown in the following example, displaying the defined outputs.
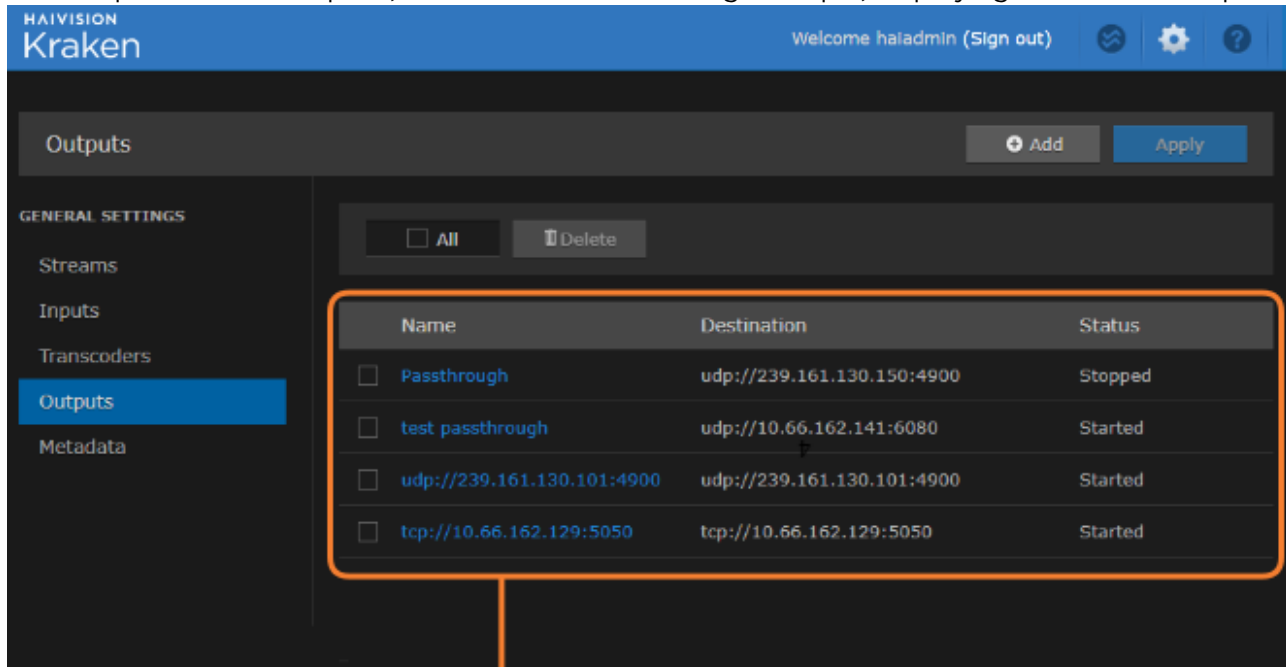
Click link to open Detail View

   - To add an output, click the ✚ **Add** button.
   - To view output details or add an output, click a line in the table to open the Outputs Detail View.
   - To delete an existing output, check the checkbox next to the item in the list and click the 🗑 **Delete** button.
2. To apply your changes, click the **Apply** button.

Related Topics

- **Configuring Output Parameters**
- **Transport Characteristics**

Configuring Output Parameters

To view and configure Output parameters:

1. From the Outputs List view, click the ⊕ **Add** button or click any line in the table.
2. On the Outputs Detail View, type in a unique name for the output and an output URL, for example, `udp://239.100.100.100:4900` .

3. Select or enter values in the fields to define the output. See **Output Settings**.
4. To configure TCP output, you simply need to enter the output port, as shown in the following example. (Decoders can receive this output by sending a request over TCP to the Kraken IP/Port. For example, to configure VLC to receive the stream from Kraken, enter the url tcp:// 10.70.5.23:55558 into the url field for a network stream.)
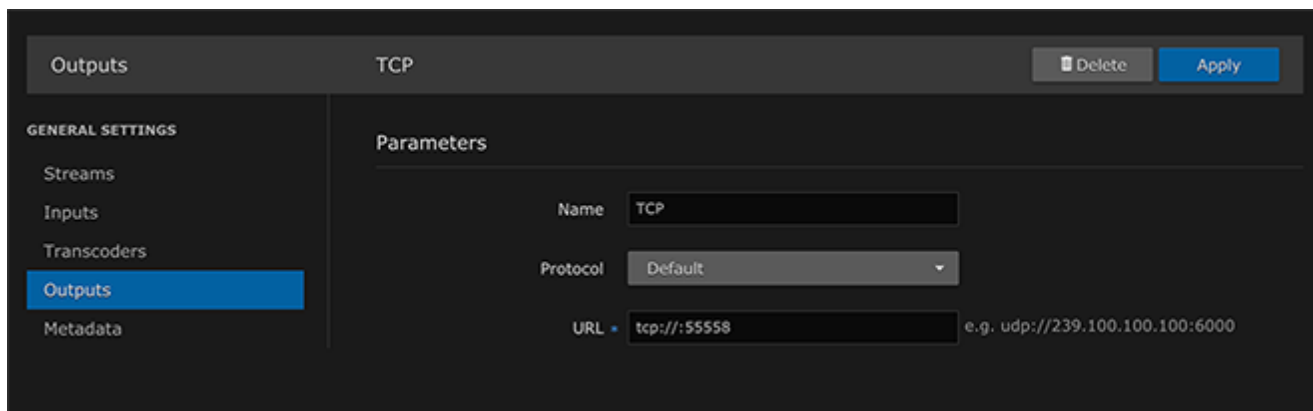
5. To modify link parameters, such as the MTU (Maximum Transmission Unit) size, TTL (Time-to Live for stream packets), or To (Type of Service) values, type these in.

6. To configure SRT output, select TS over SRT for the source and then complete the additional fields under SRT Settings. See **SRT Output Settings**.
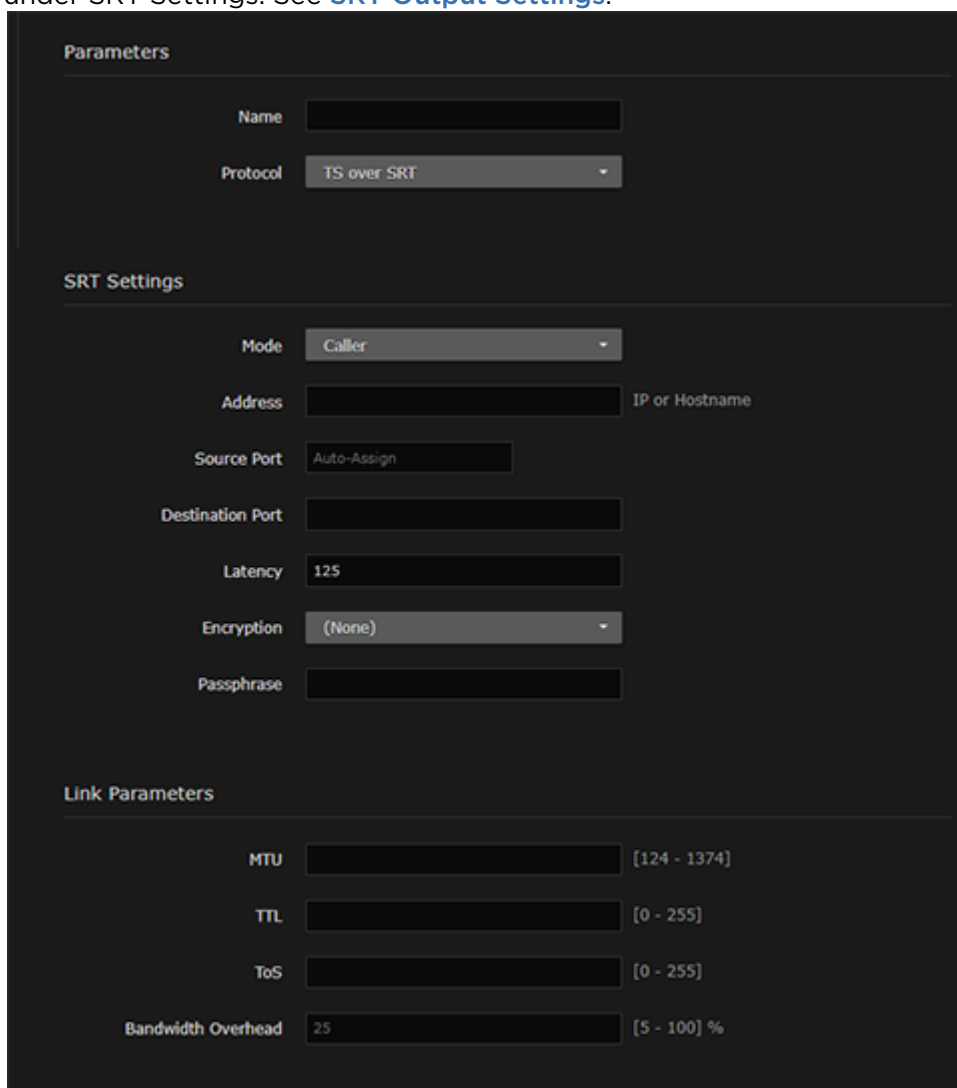
7. To configure HLS output, select **HLS** from the Protocol dropdown, and fill in the Max Number of Segments (default set to 10) and Segment Duration (default set to 2000ms).

For more information on using the HLS protocol, see 'Protocols' in **Output Settings**.

8. To apply your changes, click **Apply**.
   The new output is added to the Outputs List.

> ✅ **Tip**
>
> You can access Output statistics from the Streams Statistics page, including SRT Statistics graphs. For more information, see **Viewing Kraken Statistics**.

Related Topics

- **Output Settings**
- **Transport Characteristics**

HLS Live Preview

Once an HLS output has been configured, Administrators can view a live preview of any HLS media stream running through their Kraken device.

> ⚠ **Note**
>
> Kraken Video Preview via HLS is intended for operational confidence in media and not for wider distribution with user management in Kraken.

To view the HLS Preview:

1. Open the Stream List View and locate the panel of the HLS stream you would like to preview.
2. Ensure that the stream is started. If the stream is not currently running, select Start from the **Actions** drop-down list.
3. Once the stream is started, click the stream's output in the **Outputs** field.
4. The preview opens in a new player window, as in the example below:
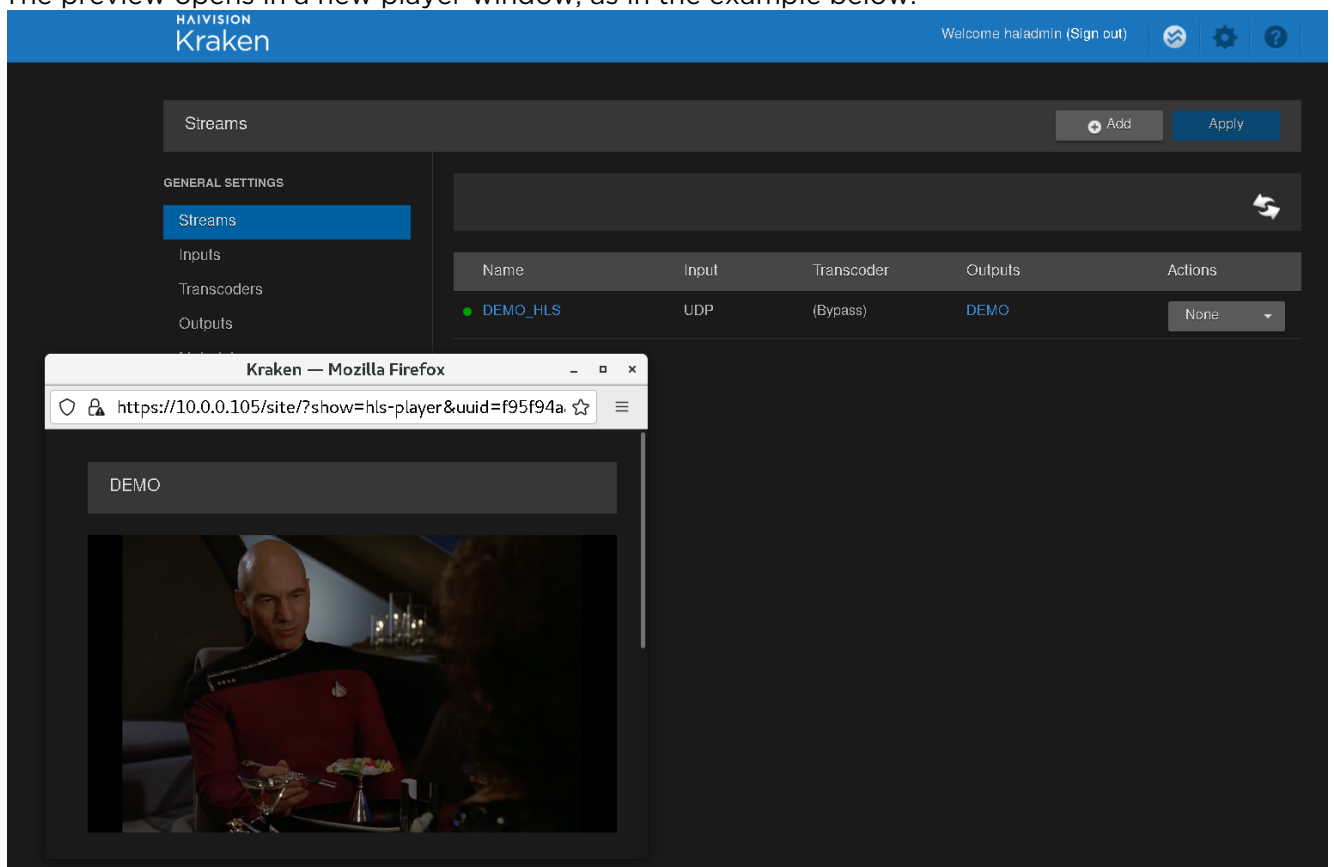
Related Topics

- **Streams List View**
- **Configuring Outputs**
- **Configuring Output Parameters**

- **Output Settings**

Configuring RTSP Outputs

Kraken supports RTSP PUSH and PULL operations for compatibility with Video Management Systems (VMS) such as Milestone and Genetec. You can use RTSP for video-only streams (typically for surveillance applications).

> ⓘ **Info**
>
> With the RTSP direction set to "PUSH", Kraken will actively seek out the specified client to send the Kraken Stream media directly to the remote device with the configured RTSP path. In this case Kraken will PUSH data to `rtsp://<rtsp_output_server>:<rtsp_output_port>/`
> `<rtsp_output_path>`
>
> With the RTSP direction set to "PULL", Kraken will make the Kraken Stream media available at the Kraken instance's configured IP address (or Hostname), the configured port (as defined in the **RTSP Server Service** configuration), and path. In this case, a remote client can connect to the Kraken output with `rtsp://<kraken_hostname>:<service_port>/<rtsp_output_path>`

To configure an RTSP Output from Kraken:

1. Enable RTSP from the Services page. For details, see **RTSP Server Service**.
2. Go to Streaming>Outputs, and click ⊕ **Add**.
3. Type in a name for your output and select RTSP as the Protocol.

4. Select either PUSH or PULL from the Direction dropdown menu.

5. For RTSP PUSH outputs:
   a. Type in the Server IP or Hostname.
   b. If applicable, configure the Port number.

> ⚠ **Note**
>
> The Port only needs to be specified if the RTSP server port is *not* set to the default 554. The Port number entered here must match the RTSP Port number configured from the Services page. See **RTSP Server Service**.

   c. Type in the Path (a string of 0-128 characters) for the remote RTSP receiver.
6. For RTSP PULL outputs:
   a. Type in the Path (a string of 0-128 characters) for the Kraken RTSP server.
7. Click **Apply**.

> ⓘ **Info**
>
> When using RTSP Outputs, be sure to use the appropriate Transcoder settings. See the recommended Transcoder Parameters for RTSP Outputs here: **Transcoder Parameters for RTSP**.

Related Topics:

- **Configuring Outputs**
- **Output Settings**
- **RTSP Server Service**
- **Services Settings**

Output Settings

The following table lists the Kraken Output settings:
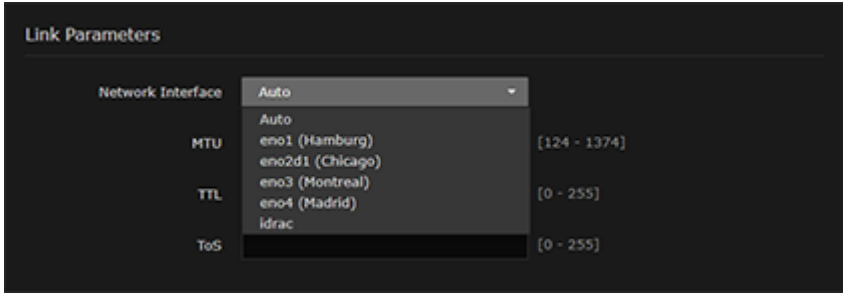
General   **Link Parameters**   **SAP**   **SRT Output Settings**   **RTSP Output Settings**

General Settings

Output Setting	Description/Values
Name	Enter a unique name for the output. This name will be selectable from the list of Outputs when you define a stream. ⚠ **Note** The Output name is not required. Kraken will use the Output URL as the name if none is provided.

Output Setting	Description/Values
Protocol	Select the Protocol type for the output streaming format: • **Default (TS over UDP)** • To use Haivision's Secure Reliable Transport (SRT) input and output streaming format, select **TS over SRT** for the protocol. For more information, please refer to the SRT Deployment Guide. • **RTMP**: Select to configure Kraken to output RTMP streams in Bypass mode. ⚠ **Note** RTMP input and output are *not* supported in "Transcoder" or "Transcoder + Passthru" modes. • **HLS**: Select to configure Kraken to output HLS streams in Bypass mode. Output source media for HLS streams ⚠ **Note** • HLS output is *not* supported in "Transcoder" or "Transcoder + Passthru" modes. • HLS outputs from Kraken require that the source media contain H.264 encoded video and AAC encoded audio. • **RTSP**: Select to configure Kraken to output RTSP streams. ⚠ **Note** RTSP output is *not* supported in "Transcoder + Passthru" mode.
URL	(Protocol must be "Default" or "RTMP") Type in the URL for the Output, for example, `udp://239.100.100.100:4900` Examples of supported output formats: • `udp://239.100.100.100:4900` = multicast UDP on 239.100.100.100 port 4900 • `udp://10.1.10.10:4900` will send unicast UDP to host 10.1.10.10 on port 4900 • `tcp://:4045` = unicast TCP delivered on port 4045 • `rtmp://10.5.6.7/somepath/endpoint` ⚠ **Note** Kraken output streams may be UDP unicast or multicast, TCP unicast, or RTMP. However, some limitations have been observed with TCP output to third-party media players.

General   **Link Parameters**   **SAP**   **SRT Output Settings**   **RTSP Output Settings**

Link Parameters

Output Setting	Description/Values
Network Interface	(Protocol must be "Default" or TS over SRT: Listener or Rendezvous Mode) Select the network (Ethernet) interface for the Output, either: • Auto (uses static route, if defined; otherwise uses the default) • <eth0> • <eth1> • ... ⚠ **Note** Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/..., pNp1/pNp2/..., or em1/em2/.... To configure customized names for the network interfaces, as shown in the following example, see "User Description" under **Network Settings**.
MTU	(Maximum Transmission Unit Size) Specifies the maximum allowed size of IP packets for the outgoing data stream. Range = `124..137` 4 ✅ **Tip** You may want to change the MTU on the outbound Kraken stream in order to be compatible with network segments or other systems/devices.
TTL	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `0..255`
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. Range = `0..255` (decimal) or `0x00..0xFF` (hex) ⓘ **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. ⚠ **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.

Output Setting	Description/Values
Bandwidth Overhead (%)	(Protocol must be TS over SRT) Specifies how much data SRT is allowed to add to the transmission over the actual bitrate of the stream being transcoded. This defines the extra bandwidth used to accommodate SRT controls as well as retransmission of lost packets. For example, with the overhead set to the default 25%, for a 10 MBit/s MPEG-TS stream, SRT is allowed to use 12.5 MBit/s of bandwidth on the network link. Range = 5-100% (default value is 25%). ⚠ **Note** SRT streams may temporarily overshoot the defined bandwidth overhead limit.

General   Link Parameters   SAP   SRT Output Settings   RTSP Output Settings

SAP (Protocol must be "Default")

Output Setting	Description/Values
Transmit SAP	Check this checkbox to enable SAP announcements.
Name	If SAP is enabled, enter a unique name for the Session. ⚠ **Note** Name is a required field for SAP entry.
Description	(Optional) Enter an expanded description of the Session.
Keywords	(Optional) Enter one or more keywords to associate with the Session. Keywords can serve as filters.
Author	(Optional) Enter the name of the program's author.
Address	Type in a valid multicast address for the SAP announcement. ⚠ **Note** Leave this blank to use the standard SAP address.
Port	Type in a valid port number for the SAP announcement. Range = 1025-65535 ⚠ **Note** Leave this blank to use the standard SAP port.

General   Link Parameters   SAP   SRT Output Settings   RTSP Output Settings

SRT Output Settings

Output Setting	Description/Values
Mode	Selects the Connection Mode for the SRT output: • Caller: Kraken acts like a client and connects to a server listening and waiting for an incoming call. • Listener: Kraken acts like a server and listens & waits for clients to connect to it. • Rendezvous: Allows calling and listening at the same time. To simplify firewall traversal, Rendezvous Mode allows Kraken and the other device to traverse a firewall without the need for IT to open a port. **✓ Tip** When using Listener or Rendezvous mode with multiple active interfaces, be sure to set the Default Interface on the Network page (see **Network Settings**). Listener and Rendezvous output modes require that an IP address be specified in the endpoint. However, since you cannot specify which interface to use with an SRT output, setting the Default Interface forces Kraken to use that specified interface for SRT. Otherwise the SRT endpoint may not receive the stream from Kraken.
Address	(Mode must be Caller or Rendezvous) The target IP address or hostname for the SRT stream (i.e., another device such as HMP or Media Gateway).
Source Port	(Mode must be Caller or Rendezvous) The UDP source port for the SRT stream, which is the unique port over which Kraken will be sending the SRT stream. You can (optionally) specify the UDP source port. If not filled in, an ephemeral source port will be assigned (between 32768 and 61000).
Destination Port	(Mode must be Caller or Rendezvous) The port over which the other device (i.e., HMP or Media Gateway) will be listening (between 1025 and 65535).
Latency	Specifies how long Kraken will buffer received packets. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20 - 8000ms Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.
Encryption	Select the AES (Advanced Encryption Standard) encryption key length and cipher: • None (default) • AES-128 • AES-256
Passphrase	(Only required and accepted if Encryption is enabled) Specifies a string used to generate the encryption keys to protect the stream (between 10 and 79 UTF8 characters).
Notes	(Optional) Type in any related information or comments.

General   Link Parameters   SAP   SRT Output Settings   **RTSP Output Settings**

RTSP Output Settings

Output Setting	Description/Values
Direction	The direction of the RTSP output. Options are: • PUSH (default) • PULL ⓘ **Info** PUSH operations send RTSP data to a specified remote receiver, while PULL operations make the Kraken RTSP server path available to remote clients via RTSP server queries.
Server	(Direction must be PUSH) A string (between 0 and 128 characters) that defines the destination remote server.
Port	(Direction must be PUSH) The port number (between 1 and 65535) of the remote RTSP receiver.

Path	A string (between 0 and 128 characters) that specifies path parameters for:
	• the remote RTSP receiver (if the direction is PUSH), for example,
	  • `rtsp://<rtsp_output_server>:<rtsp_output_port>/<rtsp_output_path>`
	• the Kraken RTSP server (if the direction is PULL), for example,
	  • `rtsp:// <kraken_hostname>:<service_port>/<rtsp_output_path>`

Configuring Metadata Capture

> ⚠ **Note**
>
> KLV Metadata Capture is an optional feature which may be installed at the factory or via a field upgrade by installing a license file.

From the Metadata pages, you can configure Kraken to capture either KLV (Key Length Value) or CoT (Cursor on Target) metadata and then incorporate data information within the metadata elementary stream of the standard MPEG Transport Stream. You can set up multiple metadata inputs to include in Transport Streams. Kraken supports up to three metadata input types: either from the COM1 serial port, the HD-SDI interface, or a user definable network port (up to eight UDP inputs).

- **Serial port:** The Kraken SDI extracts either KLV or CoT metadata packets from the serial port. From the Metadata Detail View, you must specify the Data Format, and for CoT metadata, the Max AirCraft-SPI Delta.
- **SDI:** The Kraken SDI extracts KLV metadata packets from the HD-SDI interface as per MISB RP 0605.2. Only progressive scan formats are supported (i.e., 1280x720p and 1920x1080p). Kraken can capture only 1024 bytes of KLV metadata per video frame.
- **Network:** Kraken can receive either (a) KLV payload encapsulated in UDP or (b) CoT inside UDP that is converted to KLV and then streamed. You must specify the UDP port on which Kraken will listen for incoming metadata. The Multicast Address is only required for reception of multicast metadata, or if you only want to accept messages coming from a specific sender.

You can define a small set of static KLV objects (i.e., mission IDs and security classification) for KLV and CoT metadata sources. For more information, see **Configuring KLV Metadata Insertion**.

CoT/UDP and CoT/Serial metadata sources can also be retransmitted to other IP destinations. For more information, see **Configuring CoT Retransmission**.

Metadata List View

The Metadata List View displays a summary of defined metadata sources for Kraken, including the Source Name, Type (Input Method), Data Format (KLV or CoT), and Parameters (Network Settings) for each source. It also provides an option for you to delete a source.

1. On the Streaming page, click **Metadata** on the sidebar.
   The Metadata List View opens, as shown in the following example.
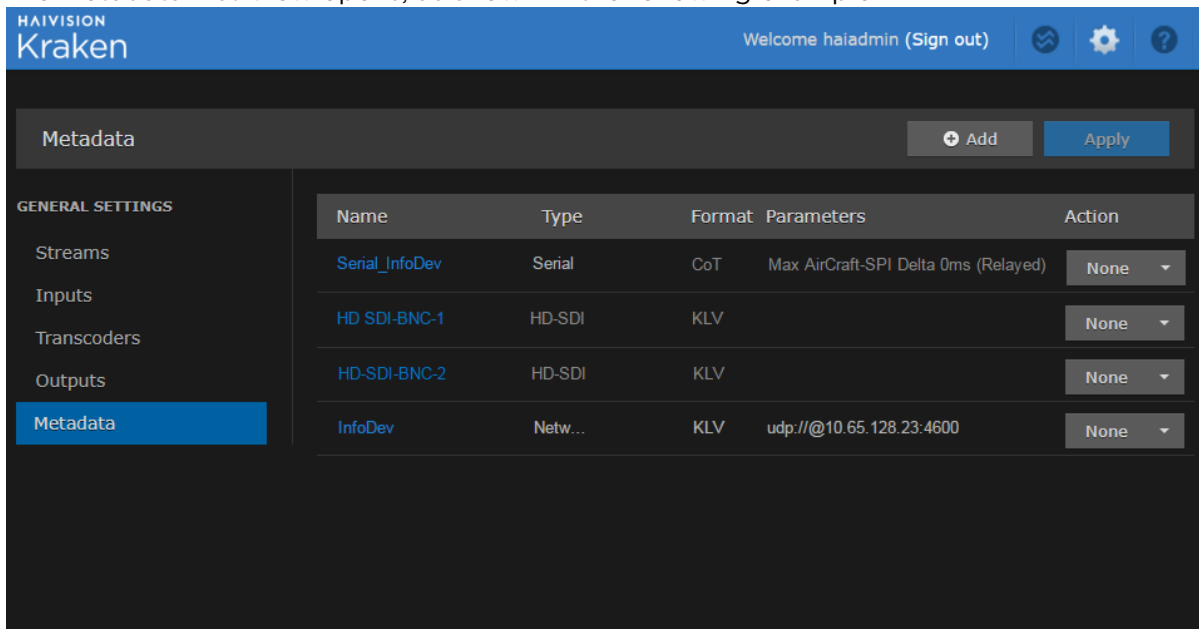
2. • To add a metadata source, click the ⊕ **Add** button.
   • To view details or modify the settings for a metadata source, click a line in the table to open the Metadata Detail View.
   • To delete a metadata source, click the drop-down list under Actions and select **Delete**.
3. To apply your changes, click **Apply**.

Related Topics

- **Configuring Metadata Parameters**

Configuring Metadata Parameters

To view and configure Metadata source parameters:

1. From the Metadata List view, click the ⊕ **Add** button or click any line in the table.
2. On the Metadata Detail View, type in the source Name and select the Input Method, either Serial, HD-SDI (Video Source), or Network (UDP).

The remaining parameters vary depending on the Input Method selected. For more information, see **Metadata Settings**.

HD-SDI Source   **Serial Source**   **Network Source**

HD-SDI Source

To configure HD-SDI (Video Source) input:

1. Select Video Source for the Input Method (as shown in the figure above).
2. (Optional) To define a set of static KLV objects to be used to replace erroneous or insert missing metadata within outbound TS streams, see **Configuring KLV Metadata Insertion**.
3. To apply your changes, click **Apply**.

The new source is added to the Metadata List.

HD-SDI Source   **Serial Source**   Network Source

Serial Source

To capture CoT or KLV metadata from the serial port:

1. Select Serial for the Input Method, as shown in the following example.

2. Select the serial port from the drop-down list or type in the text box.
3. If CoT has been installed, select CoT for the Data Format (under Input Settings) and fill in the **Max AirCraft-SPI Delta** and **SPI UID**.
4. If required, adjust the Serial settings.
5. (Optional) For CoT sources, you can configure CoT Relaying to retransmit CoT sources to other IP destinations for analysis and archiving. See **Configuring CoT Retransmission**.

6. (Optional) To define a set of static KLV objects (i.e., Mission IDs and Security Classification) to be used to replace erroneous or insert missing metadata within outbound TS steams, see **Configuring KLV Metadata Insertion**.

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

The new source is added to the Metadata List.

HD-SDI Source   **Serial Source**   **Network Source**

Network Source

To configure a network input:

1. Select Network (UDP) for the Input Method, as shown in the following example.

2. If CoT has been installed, select CoT for the Data Format (under Input Settings) and fill in the **Max AirCraft-SPI Delta** and **SPI UID**.

3. If required, under Network Settings, select Multicast for the type and fill in the multicast address and port.

4. (Optional) For CoT sources, you can configure CoT Relaying to retransmit CoT sources to other IP destinations for analysis and archiving. See **Configuring CoT Retransmission**.

5. (Optional) To define a set of static KLV objects (i.e., Mission IDs and Security Classification) to be used to replace erroneous or insert missing metadata within outbound TS steams, see **Configuring KLV Metadata Insertion**.

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

The new source is added to the Metadata List.

Related Topics

- **Metadata Settings**

Configuring CoT Retransmission

From the Metadata Detail View, you can configure CoT retransmission of COT metadata received over the Serial or UDP interface. The metadata will be retransmitted as a CoT/UDP unicast or multicast stream so that multiple CoT listeners can access the source CoT data. You can retransmit up to 8 CoT/UDP messages.

To configure CoT Retransmission:

1. From the Metadata List View, create of click the link for a serial or UDP CoT metadata source to retransmit. For details on setting up the metadata source, see **Configuring Metadata Parameters**.
2. On the Metadata Detail View, (if necessary) scroll down the page and toggle the CoT Relaying button to **On** (as shown in the following example).
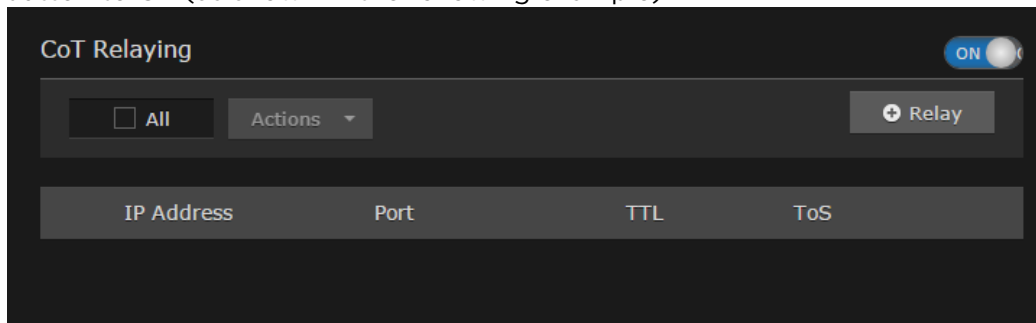
3. To add a CoT retransmission destination, click the ⊕ **Relay** button.
4. On the Add CoT Relay dialog, enter the IP Address and Port for the destination.
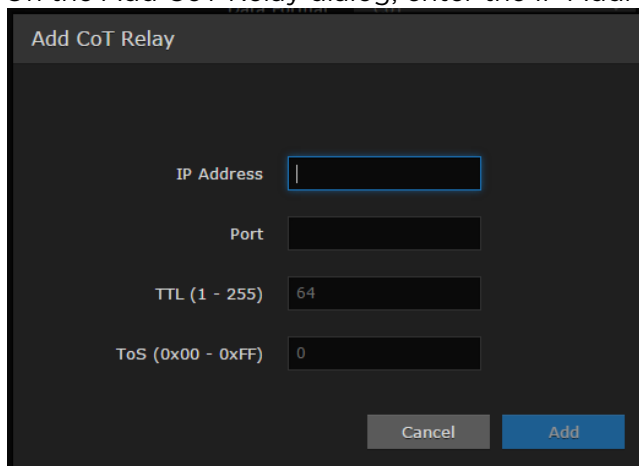
5. Click **Add**.
   The stream is added to the list:
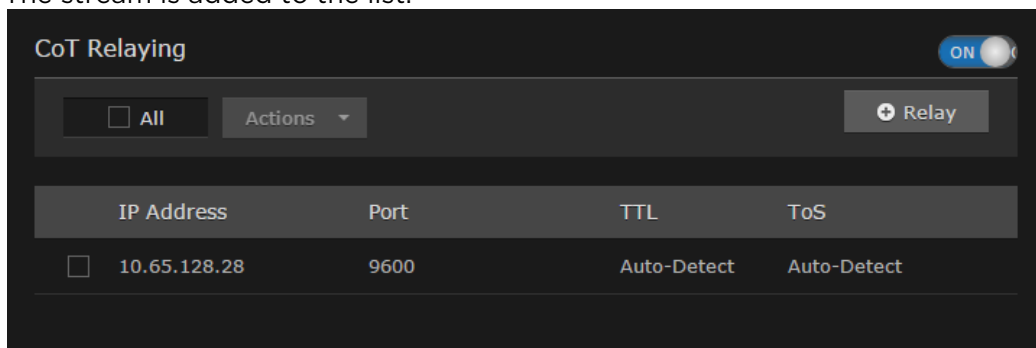
6. To edit or delete a CoT relay destination, select the relay from the list and select Edit or Delete from the Actions drop-down menu.

Related Topics

- **Metadata Settings**

Configuring KLV Metadata Insertion

From the Metadata Detail View, you can define a small set of static KLV objects (i.e., mission IDs and security classification) for KLV and CoT metadata sources. This allows customers to modify erroneous or insert missing metadata within outbound TS steams. These options are available:

- Configure a mission ID string of up to 127 characters: When the mission ID is configured, any received UAS KLV dataset will be processed in order to modify the existing mission ID or add a mission ID element if not there with the configured value.
- Enable or disable the update/generation of the security data set in UAS messages: When this feature is enabled, you then specify the classification (Unclassified, Restricted, Confidential, Secret, or Top Secret), the classifying country, and the object country/ies (up to 6) (using the proper ISO 3-letter country code).

In both cases, the mission ID or security data will get replaced or inserted with the ones created by Kraken based on the configuration.
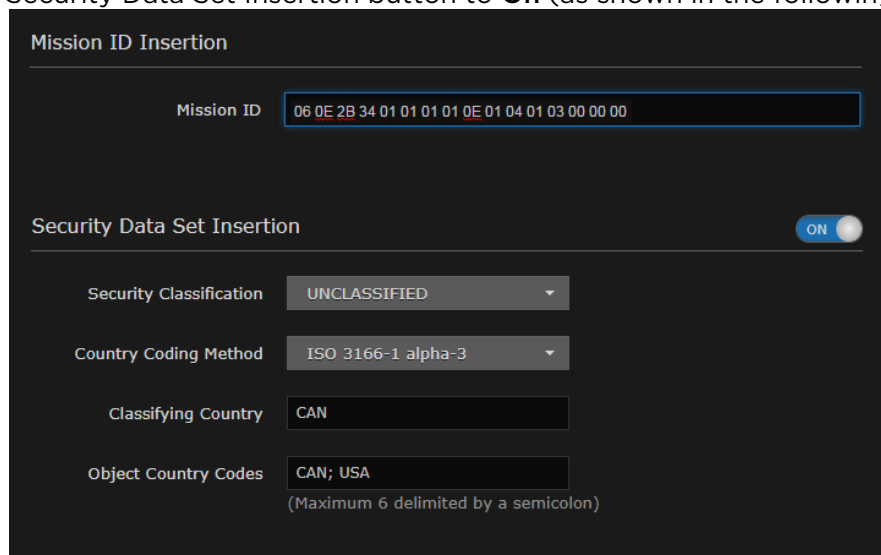
> ⚠ **Note**
>
> Metadata insertion and KLV decimation/filtering are mutually exclusive. If metadata insertion is specified, it will override KLV tag filtering.

To configure insertion of static KLV objects:

1. From the Metadata List View, click the link for the metadata source to define static KLV objects. For details on setting up the metadata source, see **Configuring Metadata Parameters**.
2. On the Metadata Detail View, if necessary, scroll down the page and (optional) type in a mission ID string of up to 127 characters in the Mission ID text box.
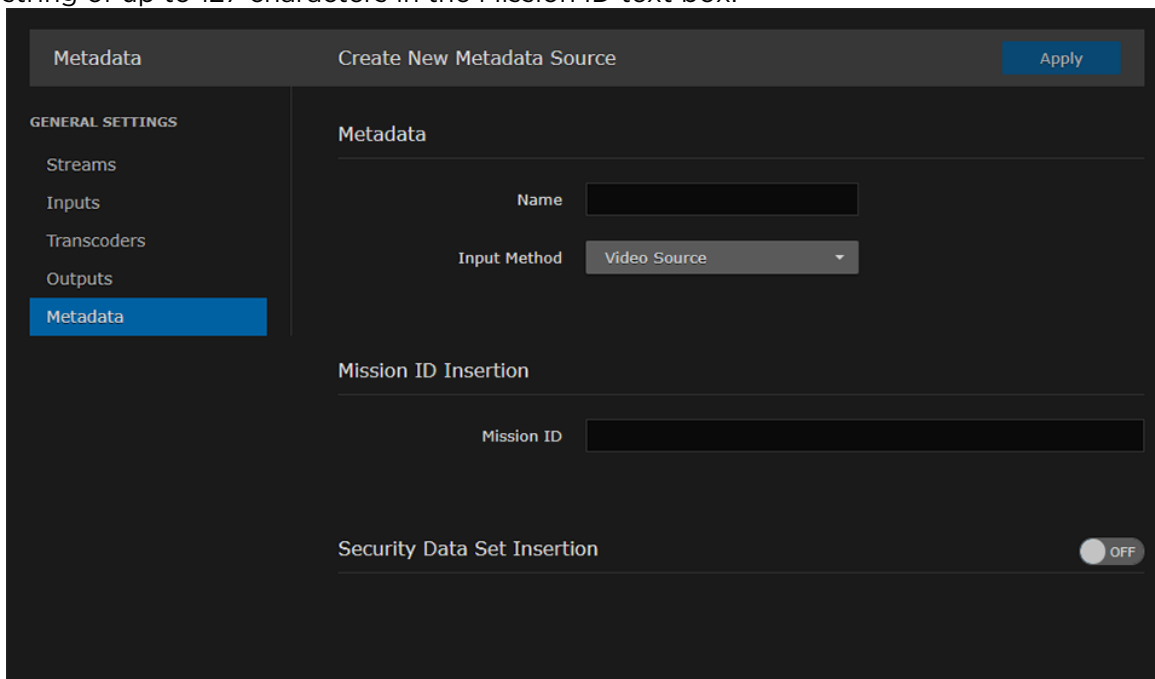
3. (Optional) To enable the update/generation of the security data set in UAS messages, toggle the Security Data Set Insertion button to **On** (as shown in the following example).

4. Fill in the remaining fields and click **Apply**.

Related Topics

- **Metadata Settings**

Metadata Settings

The following table lists the Kraken Metadata settings:

General   Input Settings   Network Settings   CoT Relaying   KLV Insertion

General

Metadata Setting	Default	Description/Values
Name	n/a	Enter a unique name for the metadata source.
Input Method	HD-SDI	Select the input interface for the source, either: • Serial • Video Source (HD-SDI) • Network (UDP)
Serial Port	n/a	(Serial input only) Enter the serial port name if not auto-detected. For example, `/dev/ttyS0` or `/dev/ttyUSB1` .

General   **Input Settings**   Network Settings   CoT Relaying   KLV Insertion

Input Settings

Metadata Setting	Default	Description/Values
Input Settings (Serial or Network input)		
Data Format	KLV	Select the data format for the metadata. • KLV (Key Length Value) or • CoT (Cursor on Target)
Max AirCraft-SPI Delta	0 ms	(CoT input only) Specifies the maximum delta between SPI and Aircraft message time-stamps for them to be considered a valid pair that can be converted to KLV. `0..1000` ms
SPI UID	n/a	(CoT input only) Double-click the text box to display the list of the SPI messages detected by Kraken and select a string for the UID filter.

General   Input Settings   **Network Settings**   CoT Relaying   KLV Insertion

Network Settings

Metadata Setting	Default	Description/Values
Network Settings (UDP Input)		
Type	Unicast	Select the stream type, either unicast or multicast.

Metadata Setting	Default	Description/Values
Network Settings (UDP Input)		
Multicast Address	n/a	(Optional) The address is only required for reception of multicast metadata. In this case, you need to provide the multicast IP address to which the data is being sent. You can also specify the address if you only want to accept KLV messages coming from a specific sender.
Port	n/a	(Required) Specifies the local UDP port on the Kraken that is receiving the packets.

General   Input Settings   Network Settings   **CoT Relaying**   KLV Insertion

CoT Relaying

Metadata Setting	Default	Description/Values
CoT Relaying (See Configuring CoT Retransmission)		
CoT Relaying	Off	When set to On, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP. `on,off`
+Relay	n/a	Use to specify the IP address and UDP port for each relayed packets. You can optionally specify the `ttl` and `tos`.
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `0..255`
ToS	0xB8	(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. Range = `0..255` (decimal) or `0x00..0xFF` (hex) ⓘ **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. ⚠ **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.

General   Input Settings   Network Settings   CoT Relaying   **KLV Insertion**

KLV Insertion

Metadata Setting	Default	Description/Values
KLV Insertion (See Configuring KLV Metadata Insertion**)**		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	Off	When set to On, enables reclassification of received UAS KLV messages. `on,off`
Security Classification	UNCLASSIFIED	Specifies the classification of the security data set: UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET
Country Coding Method	ISO 3166-1 alpha-3	The country coding method: ISO 3166-1 alpha-3 (only)
Classifying Country	n/a	The ISO 3166-1 3-letter code for the classifying country.
Object Country Codes	n/a	The ISO 3166-1 3-letter code(s) for up to six object countries separated by semicolons.

Recording a Stream

Recording in Kraken allows users to save Kraken outputs to a file on local or NFS storage. All Kraken instance types support recording including servers, small form factor appliances, virtual machines, and cloud instances.

A license is required to enable the Kraken recording functionality (for more information, please contact your Haivision account representative). With a valid Kraken license including Recording, the **Recording** feature is shown as enabled on the **Licensing** page. The license enables control of the Recording Service on the **Services** page:
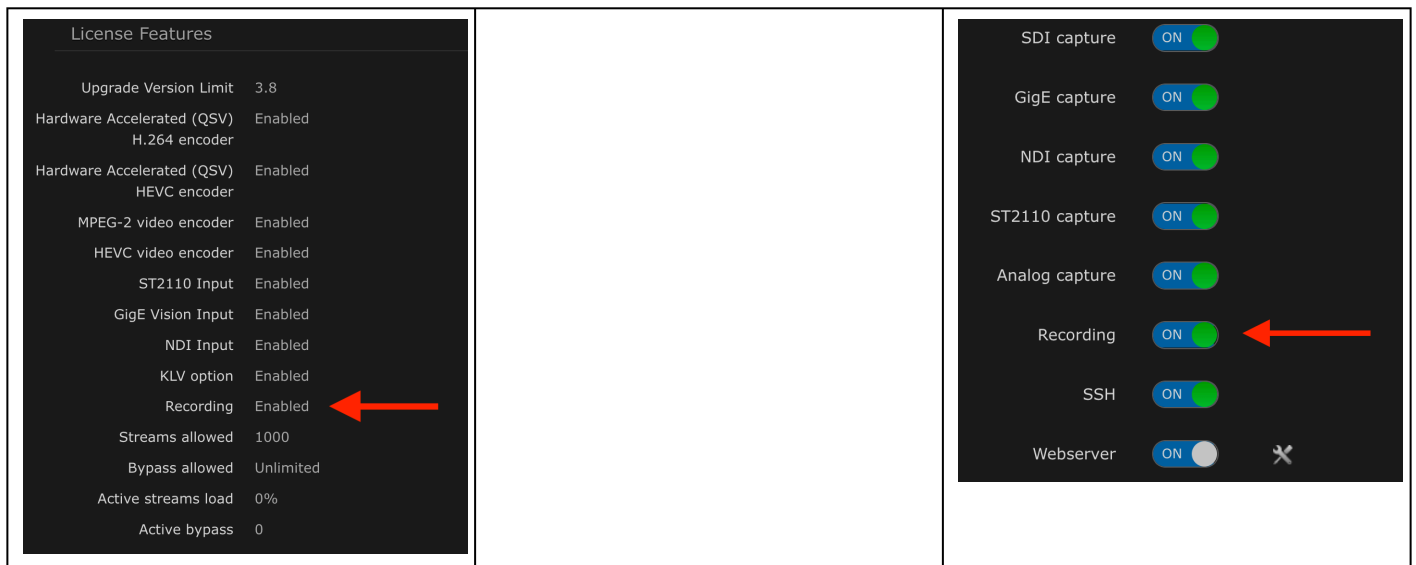
With the Recording service active and running, Kraken streams can leverage a new output type for recording media.

> ⚠ **Note**
>
> Recording outputs are available for Kraken Bypass streams ONLY at this time.

The new Kraken output type provides configuration parameters to define how media is written to storage. Storage is configured as an **Archive Location** in Kraken and is a required configuration parameter when creating a new Kraken output for recording media.

To use the Recording feature in Kraken, it is recommended to first configure an **Archive Locations** so that Kraken knows where it can write data.

Archive Locations

Kraken employs the concept of *archive locations* to isolate the management and lifecycle of storage from the act of processing and recording media. This separation of "write" operations from "storage" management provides flexibility in adapting to local or remote storage locations which impose requirements for authentication, active connection, throughput limits, etc. as Kraken evolves.

This allows users to separate recordings into distinct Archive Locations to keep recordings logically and physically separate from each other, as well as from other data.

To use the recording feature in Kraken, one or more Archive Locations must be configured.

Archive Location Types

Kraken supports storage of media both locally within a Kraken instance, or remotely by access on an IP network.
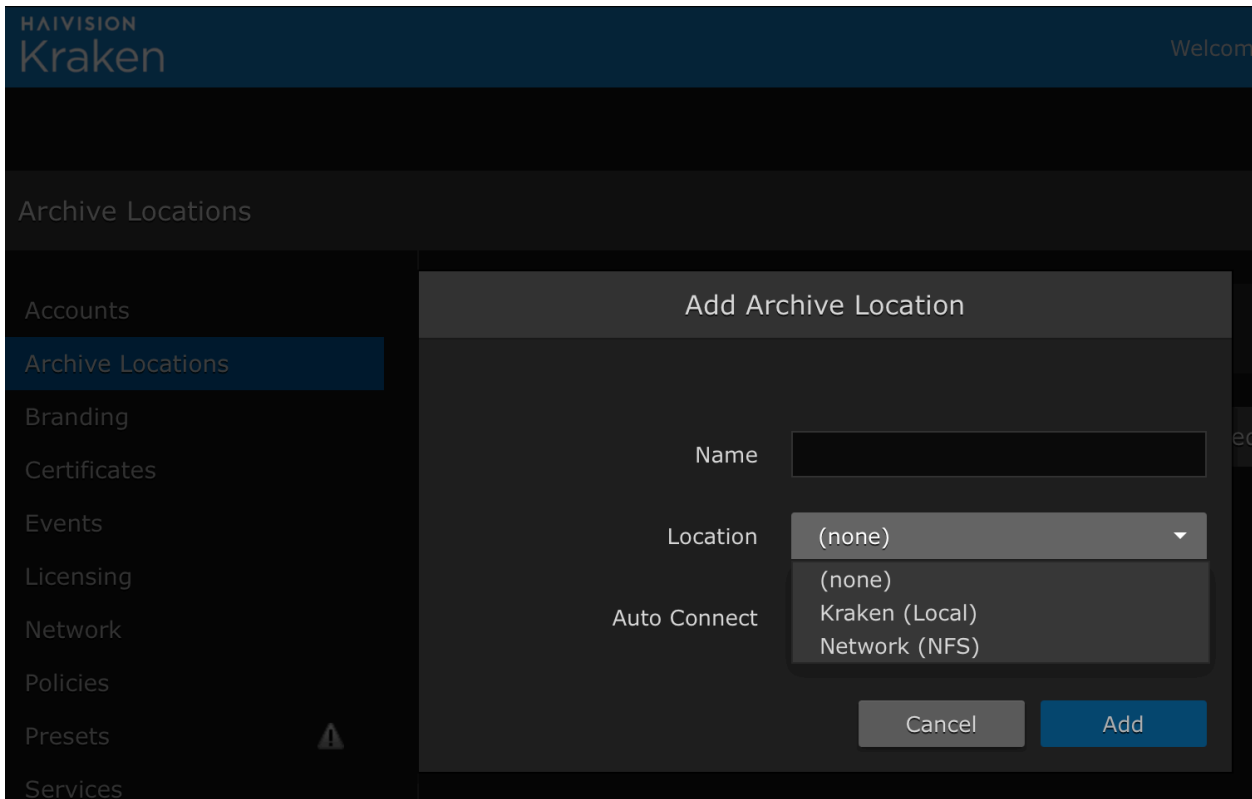
Kraken (Local) Recording

Local storage size in a Kraken instance varies by instance type and is configured as a "Local" Archive Location. This local location is in the `/assets` directory on the Kraken instance.

Kraken Instance Type	Storage
Kraken SFF	~180GB
Kraken Premium	~930GB
Kraken Ultra	~930GB
Kraken Virtual Machines	~10GB*

*Note: By default, Kraken Virtual machines have a 10GB disk created and mounted to the `/assets` path. This virtual disk can be right-sized by the Kraken administrator and re mounted to the `/assets` as the use-case demands.

Network (NFS) Recording

Use of Network storage as an Archive Location requires the network devices or capability to be accessible by the Kraken instance. The types of Network storage that Kraken can configure as an Archive Location include:

- Network File Share (NFS)

Additional Network storage locations are expected to be included in time.

Configuring Archive Locations

Available Fields for Archive Locations within the Administrative section:

Field Name	Applies To	Description
Name	All	The Name for the Kraken Archive Location. Used when configuring a Kraken Output for recording with an Archive Location.
Location	All	The type of Archive Location. Available locations include: • Kraken (Local) • Network (NFS)
Auto Connect	All	Selecting Auto-Connection will have Kraken automatically re-establish the connection between Kraken and the Archive Location after restart or service interruption.
Remote Host	NFS	The IP or hostname of the Network File System (NFS) host.
Remote Path	NFS	The configured path on the remote NFS server accessible by Kraken.

Creating a new Archive Location

1. On the **Archive Locations** page, click ➕ **Add**:
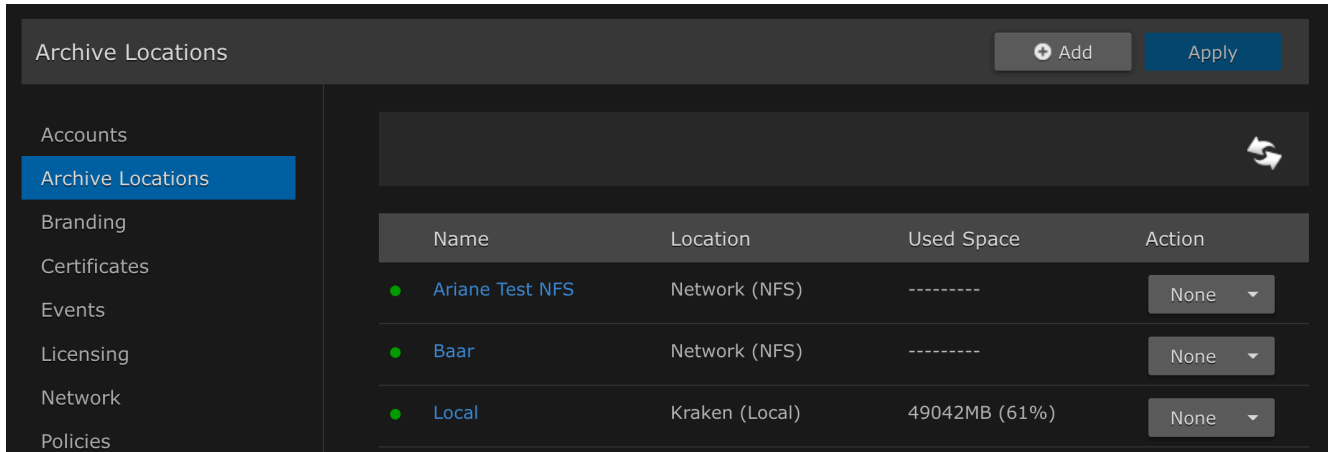
2. In the **Add Archive Location** panel, provide a **Name** for your new archive location.
3. Click the **Auto Connect** checkbox.
4. Choose the type of storage location from the **Location** menu.
   a. For NFS storage, you must also specify the IP address of the **Remote Host** and the **Remote Path** to the appropriate storage directory:

Local Archive Location

Network Archive Location
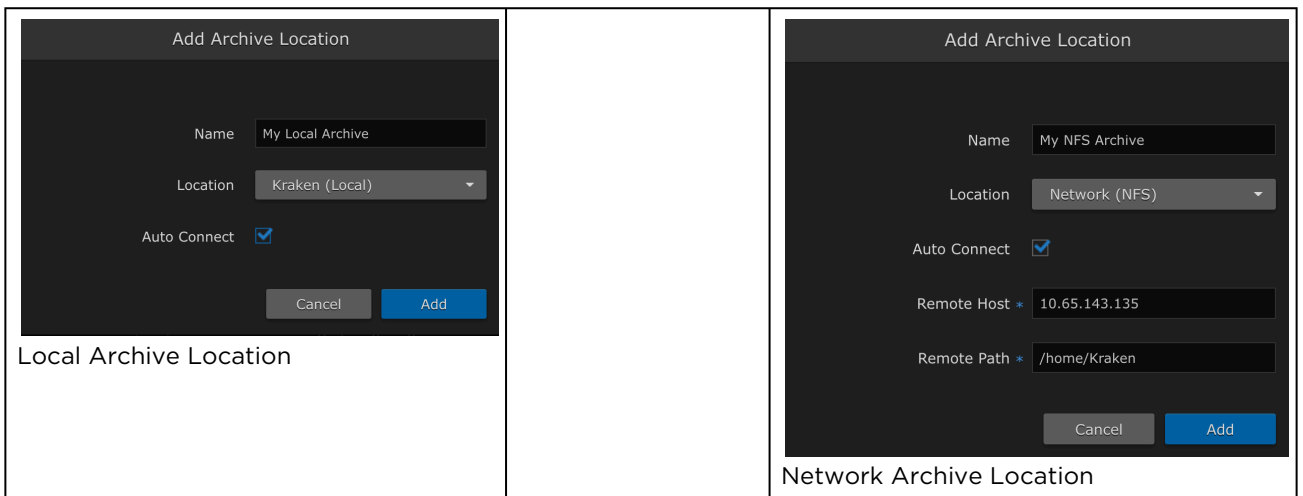
5. Click ➕ **Add**. The new entry will appear in the list of available **Archive Locations**:
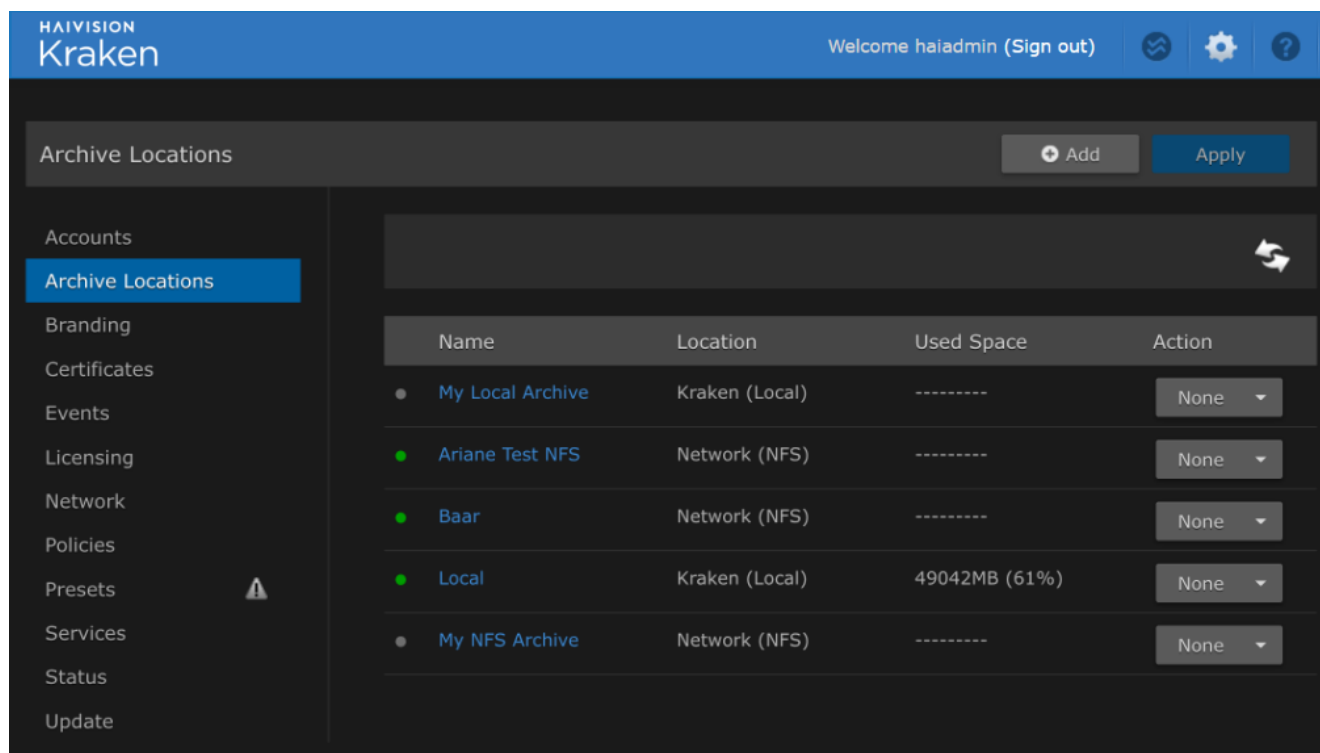
6. To connect the newly created **Archive Location**, click on its name to display its details:

When the **Archive Location** is added, Kraken will create a new folder with the UUID of the Archive Location used as the name. The **Mount Point** field contains the UUID of this **Archive Location** as part of the path where recordings are stored.

7. Click **Test Connection** to make sure the configured storage location is accessible.
8. Click **Connect** to connect the Kraken to the specified storage. Under **Status**, Kraken's state should show as CONNECTED, and the estimates of the used/available disk space should be displayed (you may need to refresh to update the display of this information):

Status

State	CONNECTED
Space Usage	
Location Used Space	49042MB (61%)
Filesystem Used Space	49074MB (61%)
Filesystem Free Space	31790MB (39%)

Test Connection

> **ℹ Note**
>
> The `etc/exports` file on your NFS storage must be configured to allow the Kraken to connect with proper permissions, and the `etc/fstab` file must be configured to allow remote clients (like Kraken) to auto-connect to your NFS server.

Configuring an Output for Recording

> **ℹ Note**
>
> An existing Archive Location is required in order to create a Kraken output capable of recording.

1. On the **Outputs** page, click ⊕ **Add**.
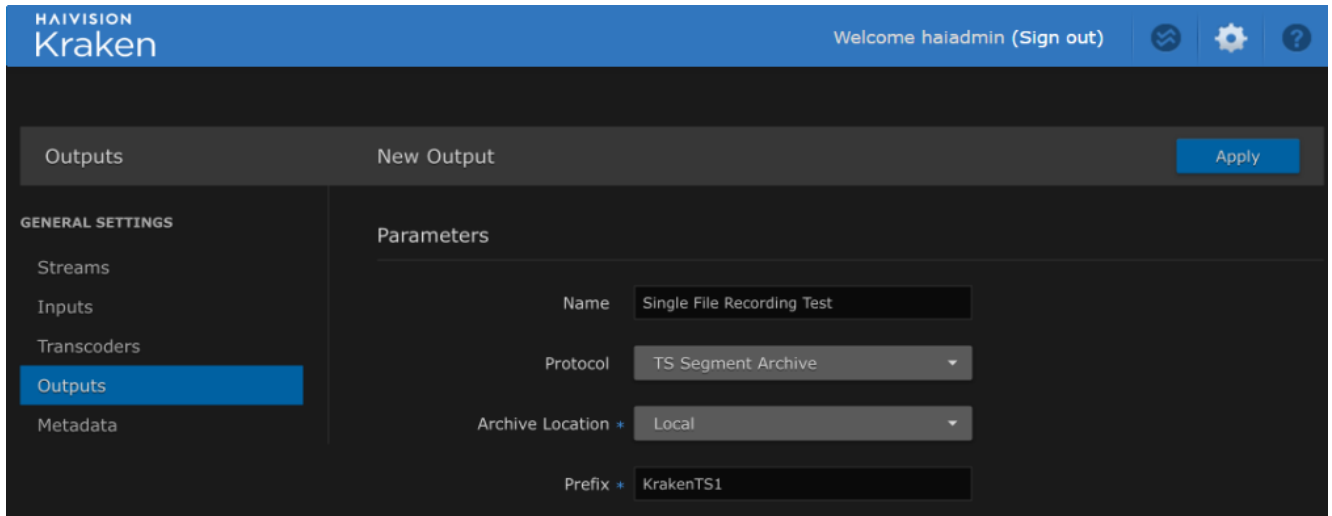
2. On the **New Output** page, provide a **Name** for your output (this will appear in the list on the main **Outputs** page).
3. From the **Protocol** menu, choose **TS Segment Archive**.
4. Specify an **Archive Location**.
5. Enter a **Prefix** (this will appear in the file name of any recordings produced using this output configuration).
6. If desired, add **Notes** to describe your settings.
7. Click **Apply**. The new output configuration now appears in the list on the **Outputs** page.

Recording a Stream

To make a recording of an output stream, do the following:

1. On the **Streams** page, click ⊕ **Add**.
2. On the **New Stream** page, configure a stream as follows:
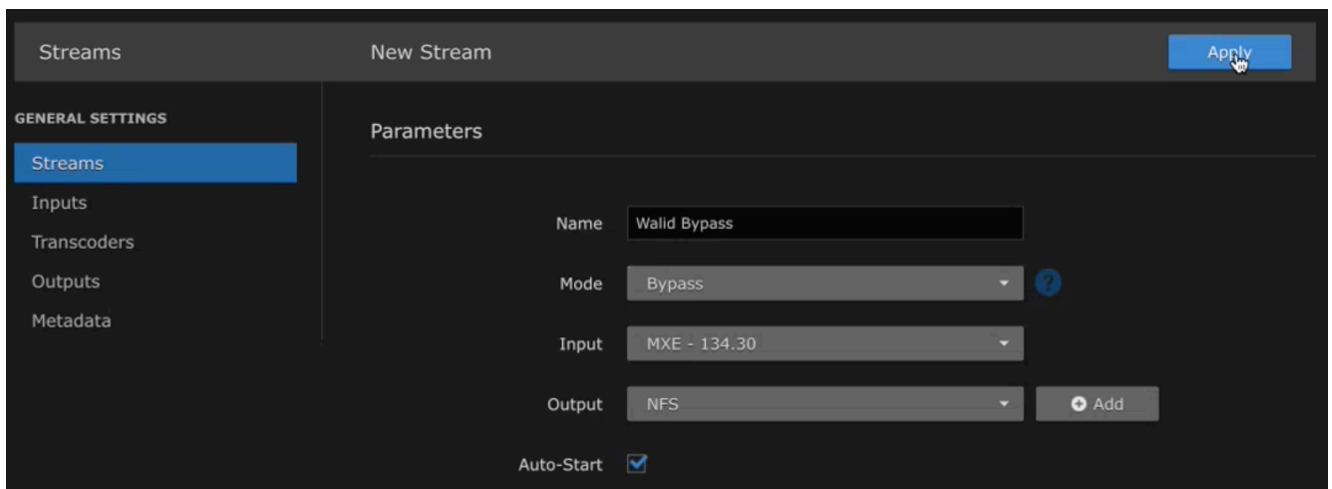
3. Provide a **Name** for the stream.
4. Choose **Bypass** from the **Mode** menu.
5. Choose a streaming source from the **Input** menu.
6. Choose an **Archive Location** from the **Output** menu. Note that you can add additional outputs, including additional recordings.

7. Enable **Auto Start** if you want the stream to resume after a restart or other service interruption.
8. Click **Apply**.
9. When ready to begin recording, click **Start**. To stop a recording, you must stop the stream.

> ℹ️ **Note**
>
> The recording feature only supports the creation of a single .ts file at a time. You must start and stop the stream manually to record the desired content. Duration is limited to the available free space at the archive location. A warning will appear in the list on the **Archive Locations** page under **Used Space** when you are running out of disk space.

Viewing a Recording

When Kraken records streaming output to an archive location, it creates a folder corresponding to the UUID of the output, and then writes the stream to a `.ts` (transport stream) file that has a filename composed of the Output prefix, the date, and a unique sequence number. To view a recording, do the following:

1. Find the UUID of your Output by viewing its details from the Outputs page. The UUID is displayed in the **Archive** parameter:
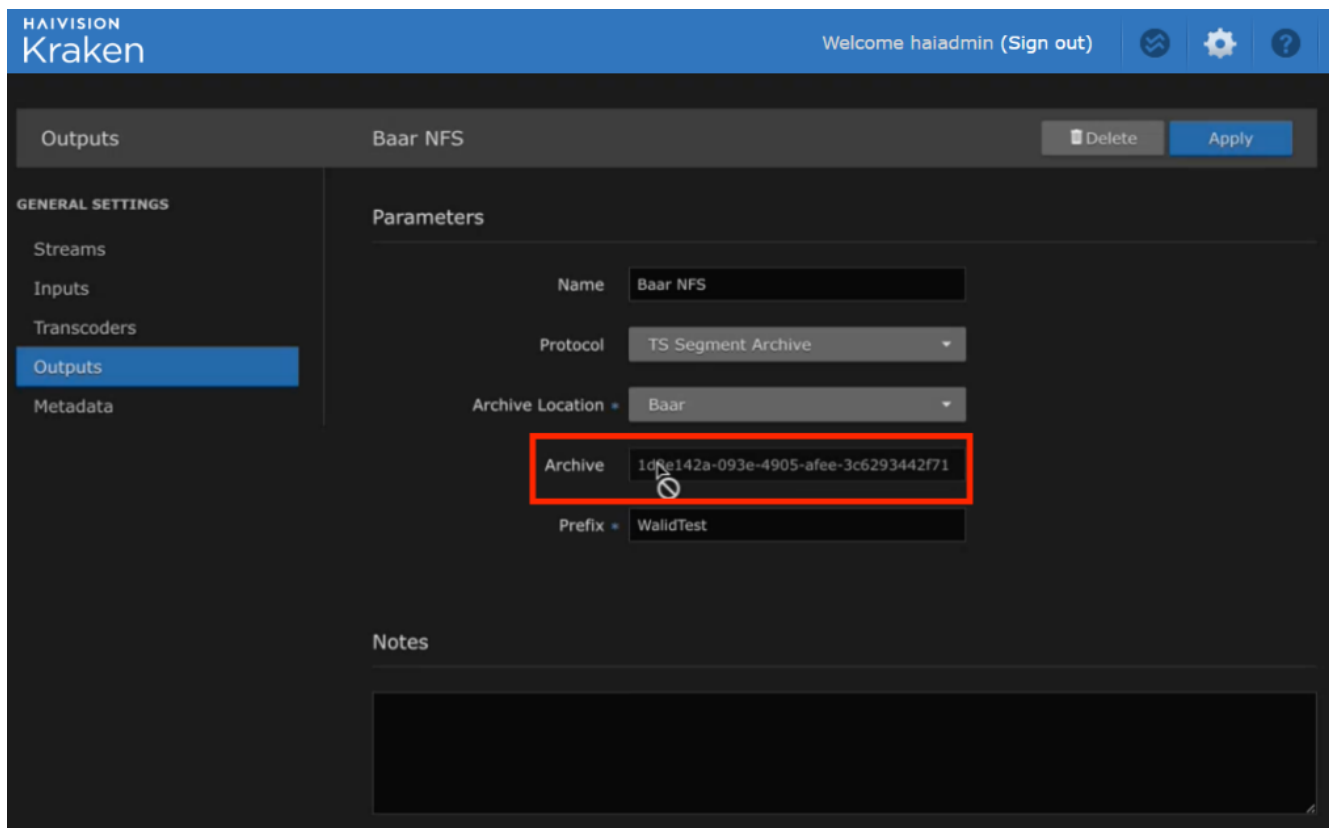
2. With an SFTP client, log into the Kraken using root credentials, or go to the `/home/kraken` directory on your NFS server.
3. Locate the folder corresponding to the Output UUID:
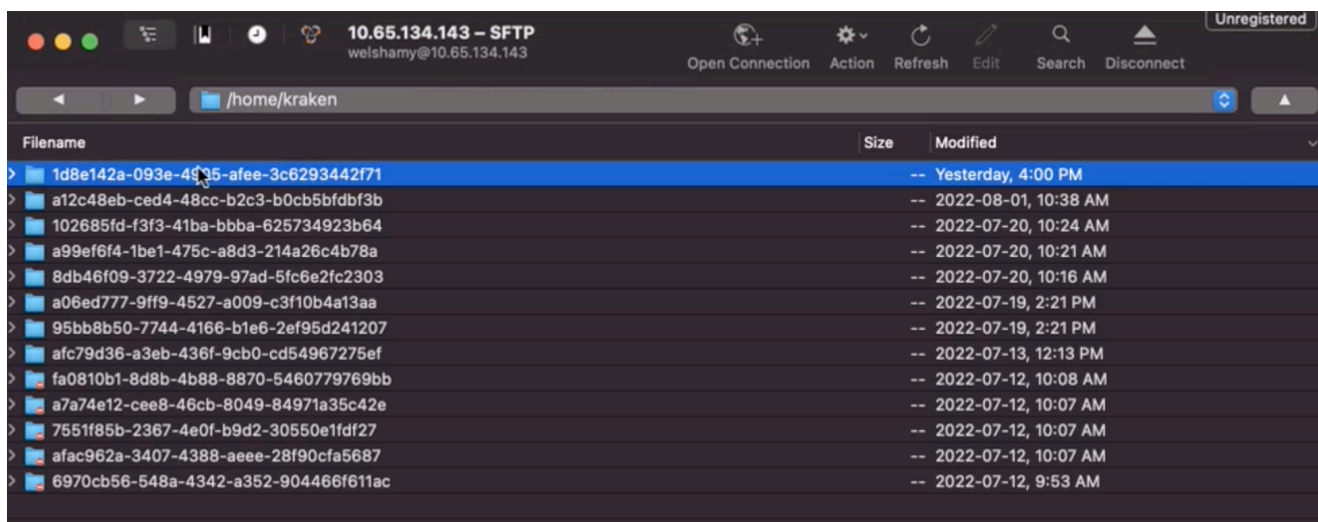
4. Open the folder, then download the `.ts` file corresponding to your recording:
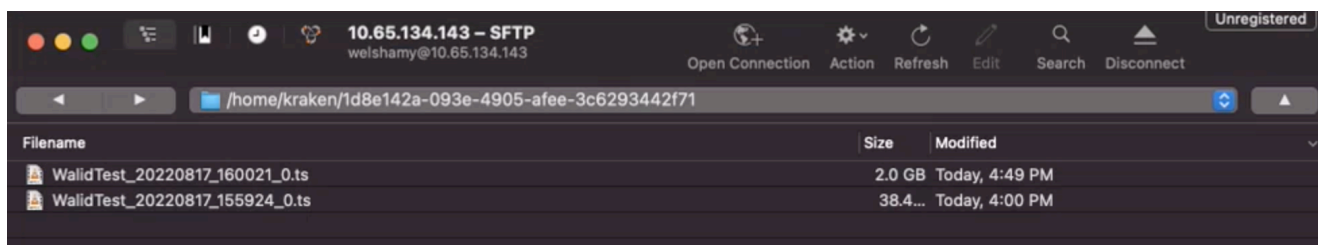
5. Use VLC or another media player to view the recording.

Related Topics:

- **Licensing Your Kraken**

System Administration

This section explains how to manage and maintain Kraken using the Web interface.

> ⚠ **Note**
>
> Before proceeding, make sure that the appliance is set up correctly and the network connection is established. For information on installing and connecting to your Kraken appliance or cloud platform, please refer to the **Quick Start Guides**.

Topics Discussed

- **Managing User Accounts**
  - **Account Management**
  - **Account Settings**
- **Re-Branding the User Interface**
  - **Branding Settings**
- **Managing Certificates**
  - **Generating a Certificate**
  - **Importing a Certificate**
  - **Viewing Certificate Details**
  - **Certificate Settings**
- **Monitoring Stream Health (Events)**
- **Licensing Your Kraken**
- **Configuring Network Settings**
  - **Network Settings**
- **Managing Security Policies**
  - **Policy Settings**
- **Saving and Loading Presets**
- **Enabling and Disabling Services**
  - **RTSP Server Service**
  - **Services Settings**
- **Monitoring the System Status**
  - **Status Settings**
  - **Rebooting Kraken**
  - **Taking a System Snapshot**
- **Installing System Updates**

Managing User Accounts

> ⚠ **Note**
>
> The Accounts pages are available to administrators only (i.e., users assigned `Administrator` role). From here, administrators can create and manage user accounts for Kraken (including their own accounts).
>
> The My Account page is available to users assigned either `Operator` or `Viewer` roles to change their own account password. For information, see **Changing Your Password**.

From the Accounts pages, administrators can create, delete and modify user accounts for the Web interface.

An account can be allocated to each user of the system so that the identity of the user can be uniquely determined. Kraken provides three predefined account roles to assign privileges to users: `Administrator` , `Operator` and `Viewer` . For details, see **Role-based Authorization**.

To view and configure user accounts:

1. On the Administration page, click **Accounts** on the sidebar.
   The Accounts List View opens, displaying the list of defined user accounts.
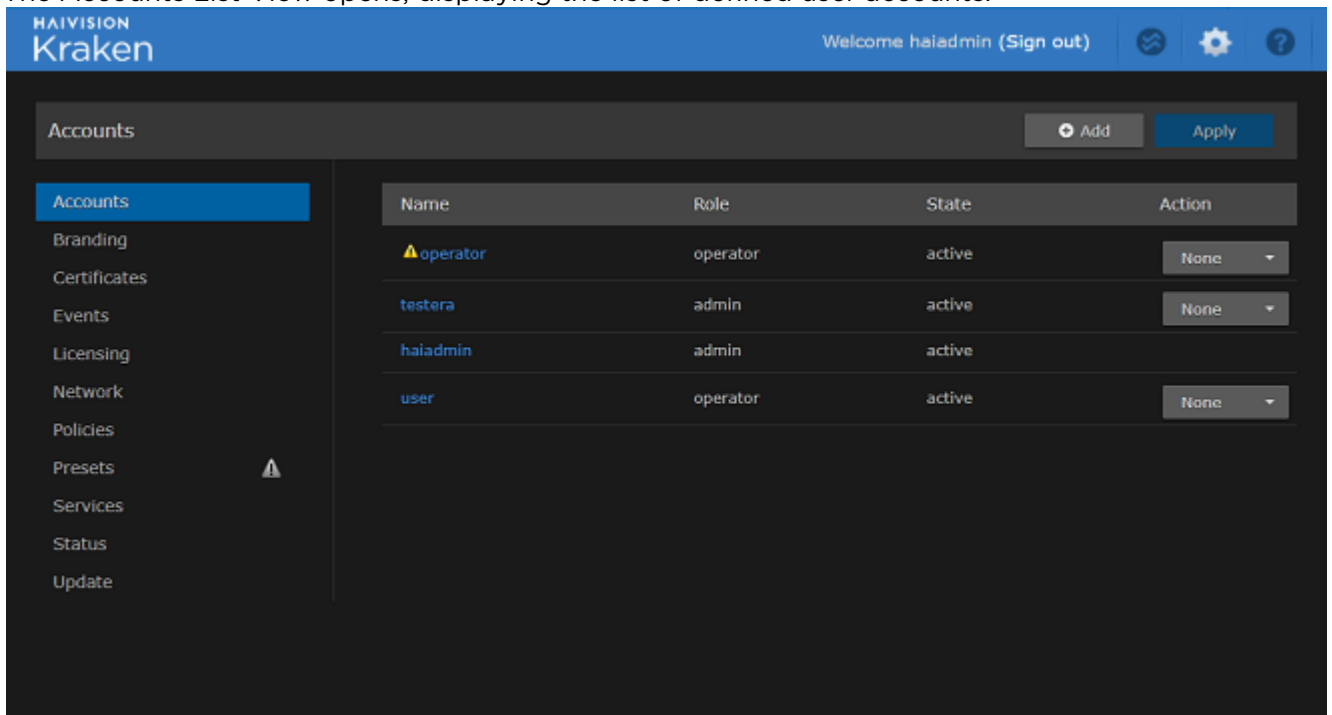
   The Accounts List View displays the Name, Role, and State for each account. In the current release, the State is either "Active", "Locked" or "Disabled".
2. To view or modify user account details, click the account link in the table to open the Account Settings page. For details, see **Account Management**.
3. To add a new account, click the ⊕ **Add** button. For details, see **Account Management**.

4. To disable or re-enable an account, click the drop-down list under **Action** and select either:
   a. Disable (if the account is Active or Locked) or
   b. Enable (if the account is Locked or has previously been disabled for inactivity)
5. To apply your changes, click **Apply**. The changes will take effect immediately.

> ✅ To delete an account, click the drop-down menu under **Action** and select Delete.
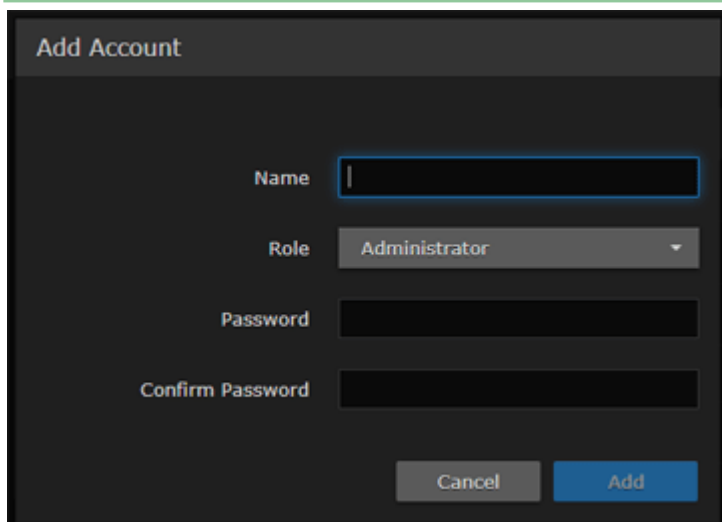
Account Management

To add a new account:

1. From the Accounts List View, click the ⊕ **Add** button.
2. On the Add Account dialog, type a unique user name in the Name text box.

> ✅ **Tip**
>
> The user name cannot include special characters `'/ \ [ ] : ; | = , + * ? < >'`.

3. Select the Role for the user. See "Role" in **Account Settings**.
4. Type the initial password in the Password field and again in the Confirm Password field. For the allowed characters, see "Password Requirements" in **Changing Your Password**.
5. Click **Add**.

> ⚠️ **Important**
>
> Accounts are initially disabled upon creation. An administrator must enable new accounts before those Kraken local users accounts can be used.

To manage existing accounts:

1. From the Accounts List View, click a link in the table for an existing account.
   The Account Settings page opens for the selected account (as shown in the following example).
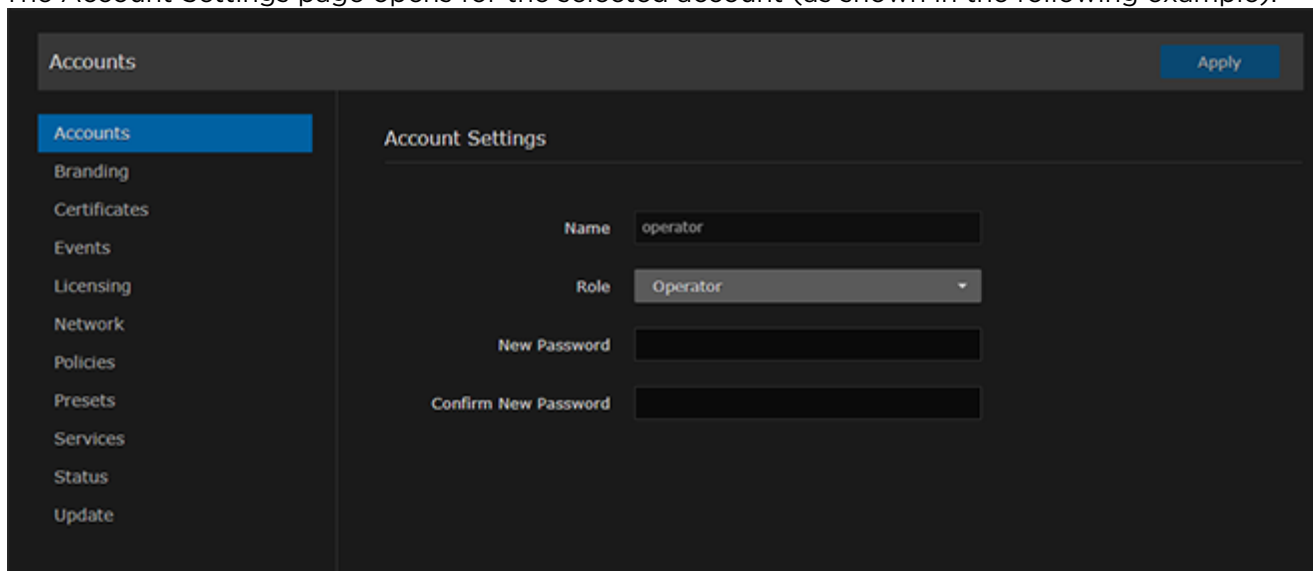
2. To reset the password of an existing account, type the password in the New Password field and again in the Confirm New Password field. For the allowed characters, see **Password Requirements**.
3. To change your own password (i.e., for the account to which you have logged in), type your old password in the Current Password field, type your new password in the New Password field and again in the Confirm New Password field.
4. To apply your changes, click **Apply**.

Account Settings

The following table lists the Accounts controls and settings:

Account Setting	Default	Description/Values
Name	n/a	(Read-only for existing accounts) The user name for the account. (New account) Type in a unique name for the account.
Role	n/a	(Read-only for existing accounts) The Role assigned to the account. (New account) Select the Role for the user account, either: • Administrator • Operator • Viewer

Account Setting	Default	Description/Values
Current Password	n/a	(Your own account only) Type in your current password. ⚠️ **Note** This is not required for other accounts since an administrator is frequently asked to change the password by users who have forgotten their passwords.
New Password	n/a	Type in the new password.
Confirm New Password	n/a	Re-type the new password.

Related Topics

- **Role-based Authorization**
- **Password Requirements**

Re-Branding the User Interface

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

You can customize the following user interface components:

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

Browser Favicon and Title

Sign-in Graphic

Banner Graphic (Logo)   Banner Color

Dark Color Theme

Light Color Theme
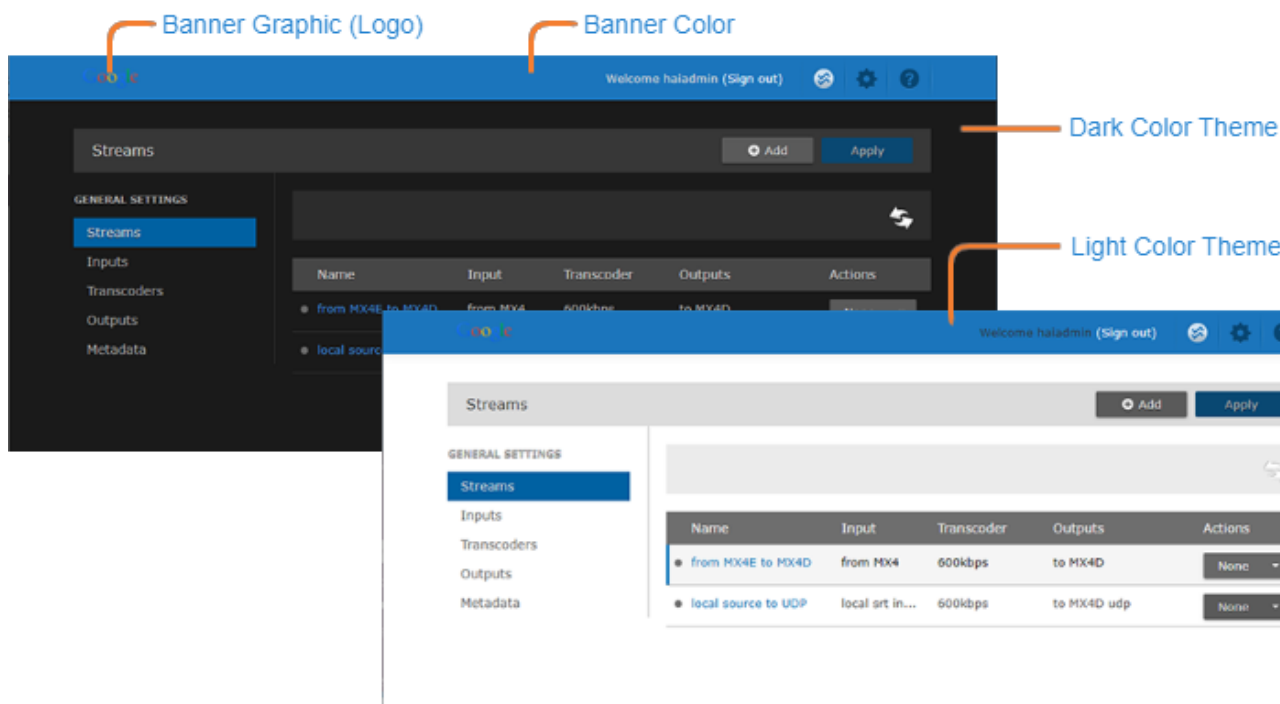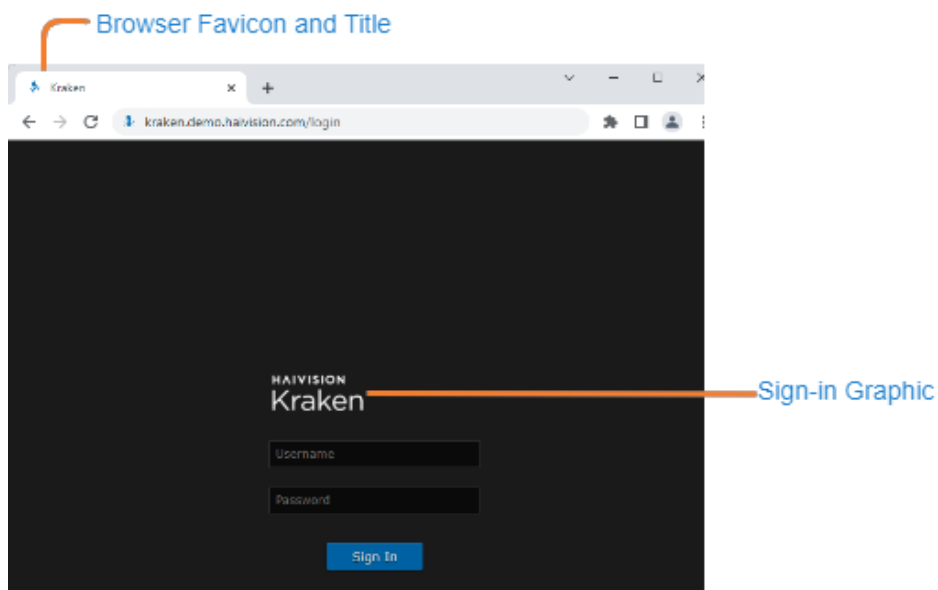
To customize the Kraken user interface:

1. On the Administration page, click **Branding** on the sidebar.
   The Branding page opens with options to change various aspects of the user interface.
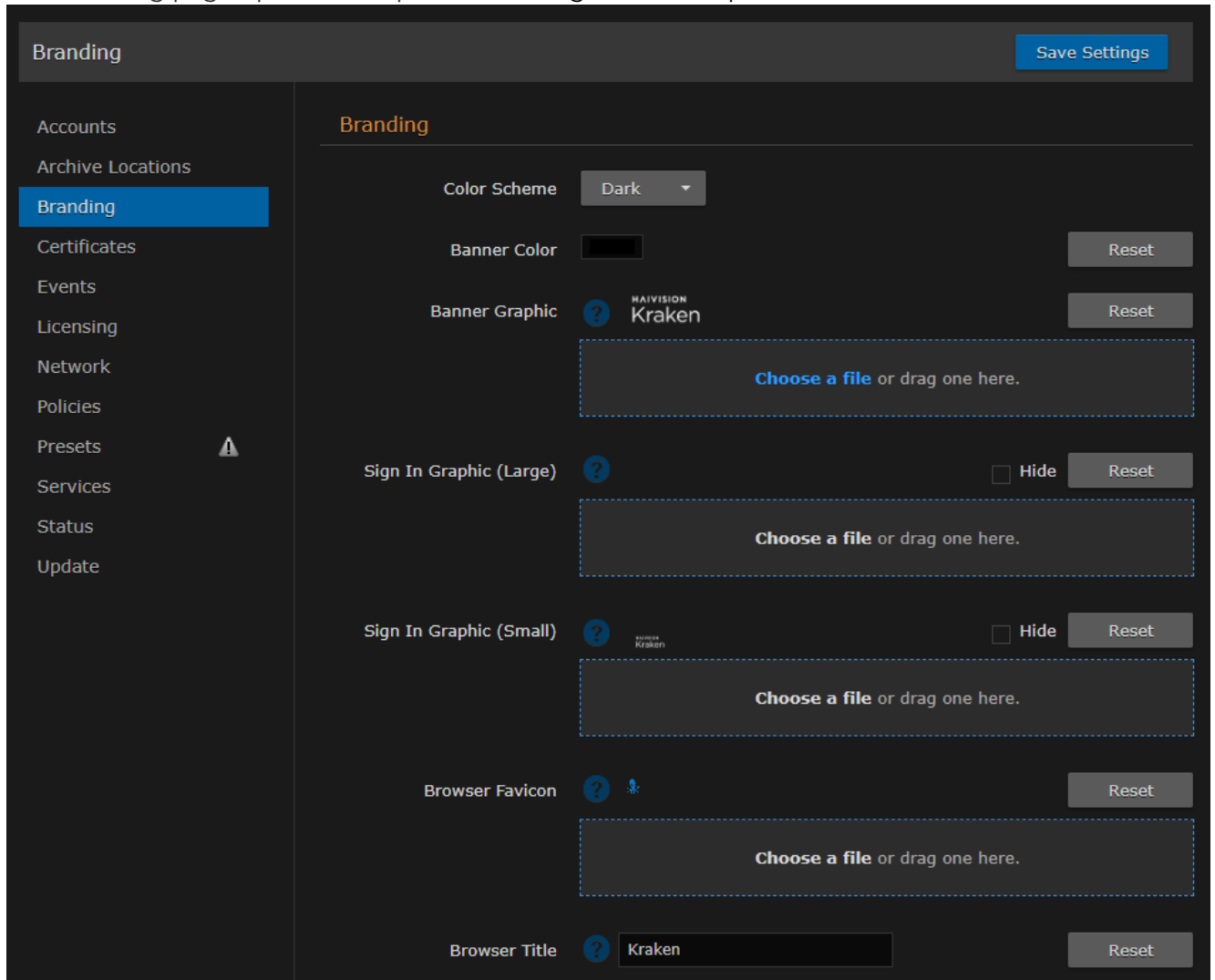
> ✅ **Tip**
>
> • To view additional help for a setting, hover the cursor over the ❓ icon.
> • To revert to the default image or banner color, click **Reset**.

2. To display your corporate branding, select or enter the new value(s) for the Color Scheme, Banner Color, and Browser Title. See **Branding Settings** for each option.
3. To import your corporate logo, choose an image file or drag one to the drop area to replace each logo.

> ⚠️ **Note**
>
> For the large and small Sign-in page Graphics, you can optionally check the checkbox to hide the graphic.

4. Click **Save Settings**.

Branding Settings

Setting	Default	Description/Values
Color Scheme	Dark	Switch interface between dark and light color schemes. • Dark: black background with white text (default) • Light: white background with black text.
Banner Color	Haivision blue (RGB: 27-117-188)	The color of the banner along the top of the page.
Banner Graphic	Haivision Kraken text logo (114x45px PNG)	The logo on the left side of the banner. The width of the image can be as long as needed up to a recommended maximum of 300 x 47 pixels. However, it should not run into the username (on the right side of the banner). Also, keep in mind that this is affected by factors such as window size, browser, etc.
Sign-in Graphic (small)	Haivision Kraken text logo (301x119px PNG)	The lower image on the Sign-in page. This graphic is white in the dark color scheme, and grey in the light color scheme. The width and height can be any dimension to fit the page. However, the image is resized to 220 pixels wide (while maintaining the aspect ratio). Also, a resized height greater than 400 pixels may require the user to scroll. The image is centered horizontally on the page.
Browser Favicon	Haivision favicon	The image to display in the browser's address bar. ✅ **Tip** The width and height can be 16, 32, 48, or 64 pixels (squared), 8-bit or 24-bit.
Browser Title	Kraken	The text to display in a browser tab/window.

Managing Certificates

The Certificates page shows the list of Identity and CA Certificates installed on Kraken devices.

- **Identity Certificates:** An Identity Certificate identifies the Kraken during the authentication process when trying to establish a TLS connection in Audit or HTTPS session startup. Its Common Name or Alternate Subject Names must match the device's IP address and/or its FQDN (Fully Qualified Domain Name) if DNS is used.
- **CA Certificates:** A CA Certificate is normally a root certificate from a certificate authority that is generally widely known and trusted. CA Certificates are stored on the Kraken so they can be used to authenticate CA-signed certificates from audit servers. You will need to import the root certificate from the CA that signed the certificate of the configured remote audit server. It is also recommended to import the root certificate of the CA that signed your Kraken identity certificate (if you have one).

From the Certificates page, you can generate self-signed certificates and certificate signing requests (CSRs), as well as import certificates or private keys.
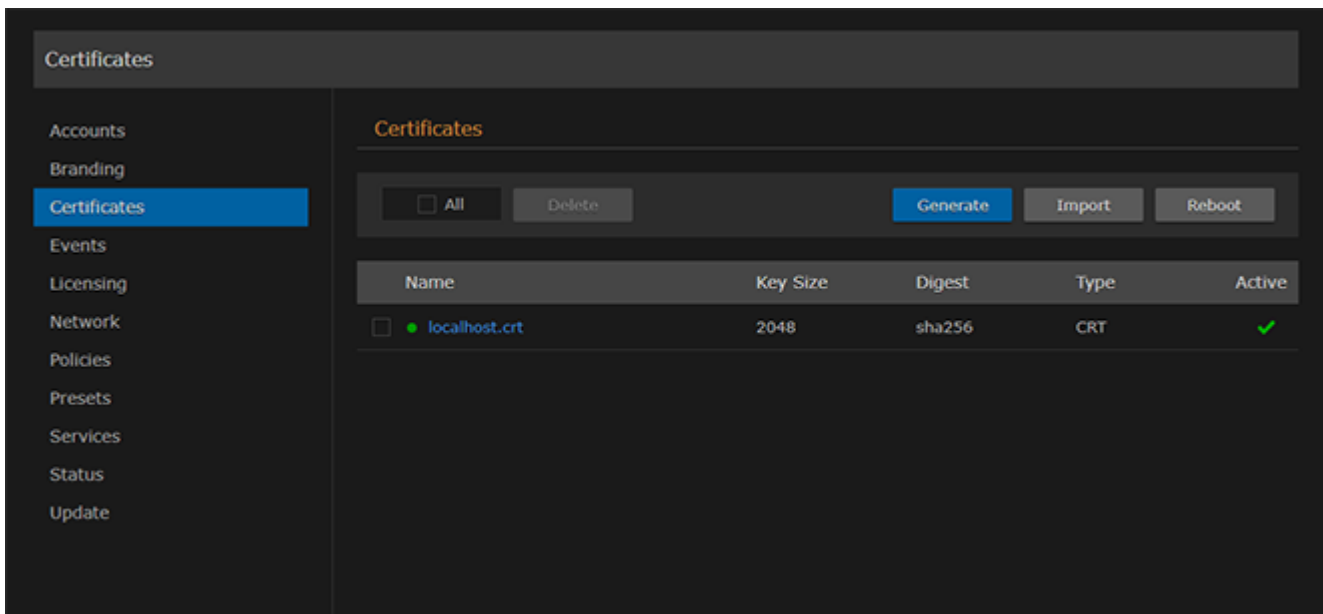
Generating a Certificate

To generate a Self-signed Certificate or a Certificate Signing Request (CSR):

1. On the Administration page, click **Certificates** on the sidebar.
   The Certificates page opens.
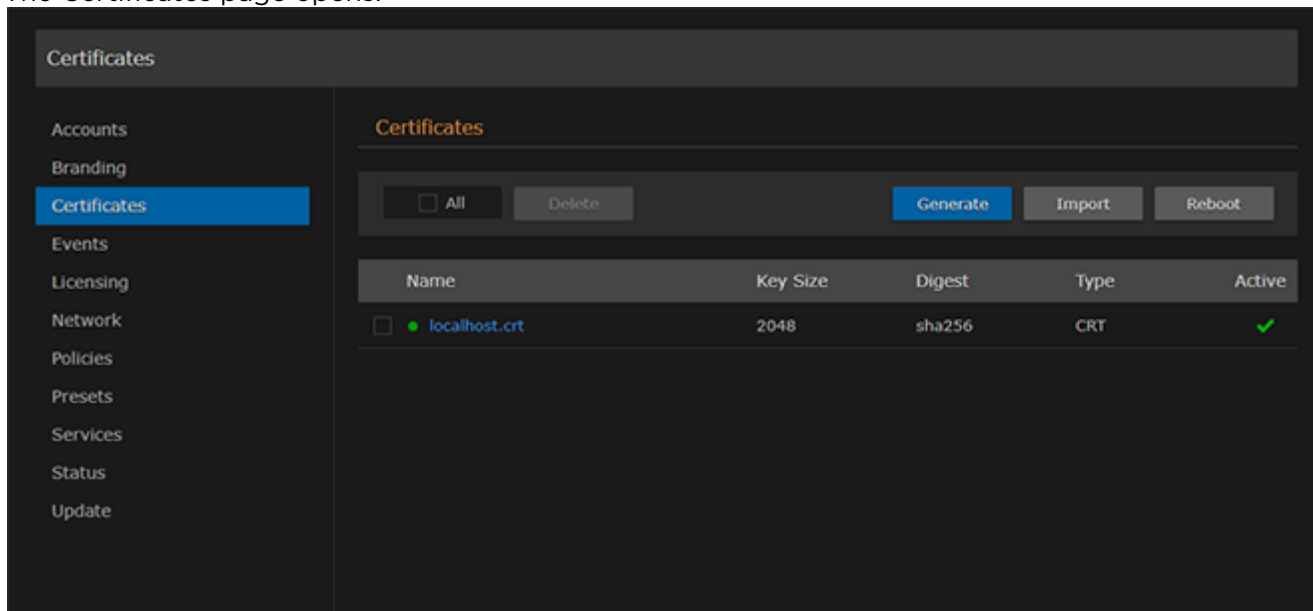
   The default Identity Certificate is indicated with a green check.
2. Click **Generate**.
3. (Optional) Type a name for the certificate in the Generate Certificate dialog.
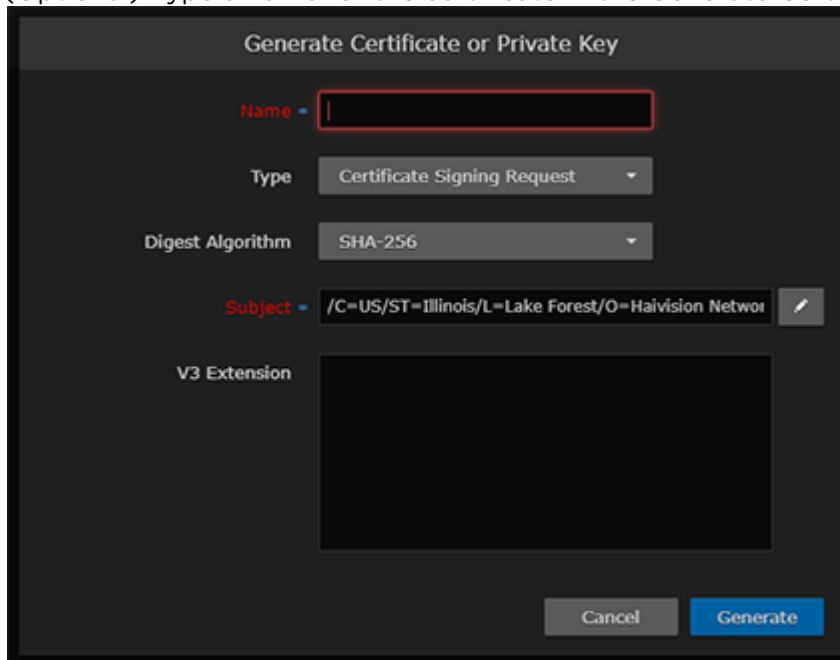
4. Select either Self-signed or Certificate Signing Request from the drop-down list. For more information, see "Type" in **Certificate Settings**.

5. For the Subject, type in information about the device that the Identity Certificate represents. For more information, see "Subject" in **Certificate Settings**.

6. Click **Generate**.
   If Certificate Signing Request (CSR) was selected, the generated CSR file needs to be sent to a Certificate 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).

> ✅ **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 Kraken and exported for signing. For details, see "Certificate Name" in **Certificate Settings**.
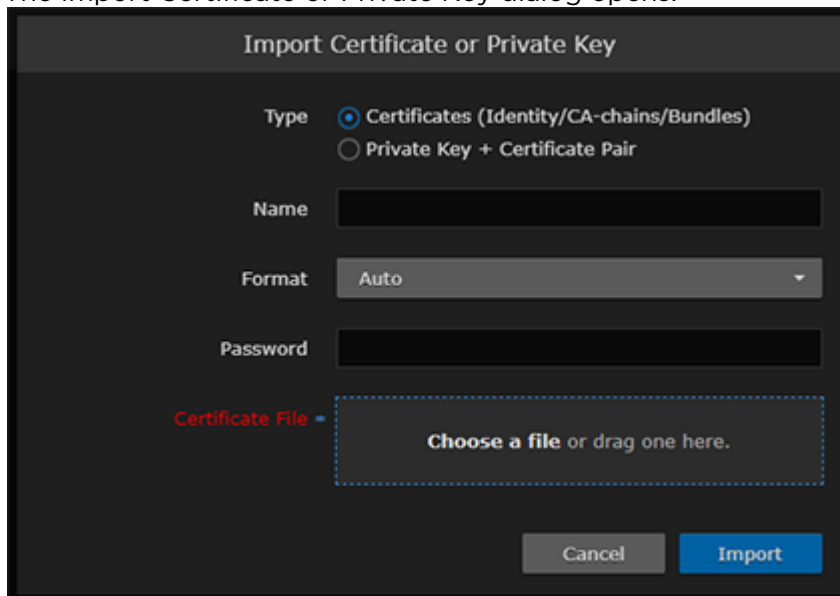
Related Topics:

- **Importing a Certificate**
- **Viewing Certificate Details**
- **Certificate Settings**

Importing a Certificate

To manage Certificates:

1. To import a Certificate, on the Certificates page, click **Import**.
   The Import Certificate or Private Key dialog opens.

2. In the Import Certificate or Private Key dialog:
   a. Select the Type: either Certificates (Identity/CA-chains/Bundles) or Private Key+Certificate Pair.

   b. (Certificates only) Type in the Certificate Name and select the Format.
   c. (If the imported certificate is password-protected) Type in the password.
   d. Drag a certificate file to the drop area or click **Choose a file** to select a cetificate file to import.
   e. Click **Import**.
3. To view the details of a certificate, on the Certificates page, click the certificate name from the Certificates list. (See **Viewing Certificate Details**.)
4. To set the default Identity Certificate (i.e., the Identity Certificate that will be used to represent the device during Audit and HTTPS authentication), hover over the certificate row and click the (grayed out) check mark under **Active**.
   The selected certificate will be set as the default certificate. It will be immediately applied to communications with the Audit server, but will not apply to HTTP communications until the next service restart or system reboot.

> ✅ **Tip**
>
> To delete a certificate file, select the name from the Certificates list and click **Delete**.

Related Topics:

- **Generating a Certificate**
- **Viewing Certificate Details**
- **Certificate Settings**

Viewing Certificate Details

To view the details of a certificate file:

1. On Certificates page, click the name from the list certificates.
   The certificate file opens in a new window (as shown in the following example).

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            db:66:31:56:f7:fc:17:cf
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Illinois, L=Lake Forest, O=Haivision Network Video, Inc., OU=PRODUCT DEVELOPMENT,
CN=localhost.localdomain/emailAddress=support@haivision.com
        Validity
            Not Before: Feb 18 20:44:11 2020 GMT
            Not After : Feb 17 20:44:11 2022 GMT
        Subject: C=US, ST=Illinois, L=Lake Forest, O=Haivision Network Video, Inc., OU=PRODUCT DEVELOPMENT,
CN=localhost.localdomain/emailAddress=support@haivision.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b2:69:4e:72:58:93:e8:96:22:6d:3a:75:93:c8:
                    53:74:1d:89:79:5e:5f:ec:ee:c8:d9:73:8a:d0:45:
                    bd:8e:bc:5e:4f:51:0f:34:dc:d0:34:4b:97:90:a4:
                    b0:26:0e:21:ad:92:8a:2d:26:c4:81:b2:5e:dd:b7:
                    9b:6e:d8:9f:c4:ee:7c:bd:6d:43:e3:38:a8:0c:44:
                    0e:4d:f8:21:21:d3:bc:5c:85:97:fe:6b:11:04:df:
                    4e:f8:b9:83:cc:dc:a6:80:35:e8:47:b0:bf:7f:d9:
                    0f:73:1d:17:fa:26:14:24:5f:67:db:64:aa:96:08:
                    b0:1f:b6:78:be:46:08:08:4d:5d:f8:b1:11:d3:94:
                    80:f9:94:a1:e6:33:43:59:8e:88:bf:bb:85:5b:01:
                    e9:70:6b:5b:43:17:9d:e8:ac:f4:99:df:27:b2:b8:
                    f7:a7:98:dd:c5:59:9a:2c:6b:f4:0a:c8:77:b7:57:
                    2c:8d:bb:57:eb:ac:2f:a5:46:2f:76:4a:d4:9f:8d:
                    f0:23:62:5a:1a:73:8c:c9:d7:c2:58:0a:2c:b4:2d:
                    0c:8d:c0:d3:dc:b2:c9:4a:e5:a1:26:a9:97:99:9c:
                    5c:43:ca:52:98:a0:21:a5:4d:b3:bf:51:b8:33:b9:
                    00:d0:d1:c1:1a:52:db:44:bd:f7:66:0b:7c:22:16:
                    f4:5f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:localhost.localdomain
    Signature Algorithm: sha256WithRSAEncryption
        5f:d6:0b:e5:fc:8f:e5:98:53:ac:82:bd:a4:1a:86:63:fa:d2:
        73:5d:ce:64:2a:b6:2a:61:e6:64:b8:b9:fe:62:31:42:27:2d:
        b2:df:81:1f:99:66:ef:ea:71:a2:59:63:8c:e0:45:6f:23:bd:
        df:25:b4:62:0d:cd:2a:59:c8:42:20:ef:c2:26:f4:06:82:aa:
        05:7b:20:b9:11:93:a1:7a:49:9e:8f:69:74:b6:3e:51:52:58:
```

2. (Optional) Save the file.

Certificate Settings

Generate Certificate or Private Key   Import Certificate or Private Key

Generate Certificate or Private Key

Setting	Default	Description/Values
Certificate Name	n/a	Type in a unique name under which the certificate will be stored on Kraken as well as listed on the Certificate page.
Type	Certificate Signing Request	Select the Signature Type: • Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates. • Certificate Signing Request (CSR): A request will be generated, and its name will be added to the list of Identity Certificates. A copy of the request is saved in the current administrator's home directory, or it can be copied and pasted into a new file in a text editor from the CSR view. 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.
Create New Private Key	Disabled	(Type must be Self-Signed) Check this checkbox to create a new private key. ✅ **Tip** Generating a new private key will overwrite the current private key.
Digest Algorithm	SHA-256	Select the digest algorithm (Secure Hash Algorithm): • SHA-256 • SHA-384 • SHA-512
Subject		The Subject identifies the device being secured, in this case, Kraken. Entering the special value "auto" (or leaving the field blank) sets the Common Name to the device's FQDN if DNS is set, or the IP address otherwise. The Subject Alternative Name extension is also set to the FQDN, hostname, and IP Address of the device (there is no other method to enter Subject Alternative Name values). Type in the subject in the form: `"/C=US/ST=Maine..."` where the most common attributes are: • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name Note that parameters with spaces should be enclosed in quotation marks.

Setting	Default	Description/Values

V3 Extension		(Type must be CSR) V3 extensions allow more configuration options to be inserted in the Code Signing Request, such as alternative subject names and usage restrictions to certificates.
		To add one or more Subject Alternative Names, enter the same information that would go in the extensions section of an OpenSSL configuration file. For example:
		
		``[req]
		req_extensions = v3_req
		[v3_req]
		# Extensions to add to a certificate request
		subjectAltName = @alt_names
		[alt_names]
		DNS.1 = server1.example.com
		DNS.2 = mail.example.com
		DNS.3 = www.example.com
		DNS.4 = www.sub.example.com
		DNS.5 = mx.example.com
		DNS.6 = support.example.com```

Generate Certificate or Private Key   **Import Certificate or Private Key**

Import Certificate or Private Key

Setting	Default	Description/Values
Type	• Certificates (Identity /CA-chains/Bundles)	Select the type of the imported certificate: • Certificates (Identity/CA-chains/Bundles): If you are importing an identity certificate. • Private Key + Certificate Pair
Name	n/a	The Certificate Name is the name under which the certificate will be stored on the device. • If the certificate is a new certificate generated outside of the Kraken, the file should also contain the certificate Private Key, and its chosen name should be one that isn't already installed on the device. • If the certificate is a newly signed one that was sent as a certificate signing request and is returned by the CA, the certificate name should be the same as its CSR (Certificate Signing Request) counterpart in the list.
Format	Auto	Select the file format for the Certificate (the formats differ in the way the file is encrypted): • Auto: detected from the file extension • DER: Distinguish Encoding Rules • PKCS #7 • PKCS #12
Password	n/a	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.

Setting	Default	Description/Values
Certificate File	n/a	Drag a certificate file to the drop area or click **Choose a file** to select a certificate file to import.

Related Topics

- **Generating a Certificate**
- **Importing a Certificate**
- **Viewing Certificate Details**

Monitoring Stream Health (Events)

Kraken offers stream event reporting with the option to download the stream event log. This feature is designed to aid in diagnostics and debugging sessions, in particular, providing feedback related to problematic streams that have been restarted by Kraken error handling or the watchdog process.

The Events page displays a list of events in reverse chronological order (newest to oldest). The list shows the stream name and UUID, followed by the date and a description of the event. Hovering your mouse over a message displays the full message, which is useful for longer messages.

You can download the log and open it in a text editor.

> ⚠️ **Note**
>
> The event log rolls over every two days; i.e., events are removed from the list after two days.

To view event information:

1. On the Administration page, click **Events** on the sidebar.
   The Events page opens, as shown in the following example.
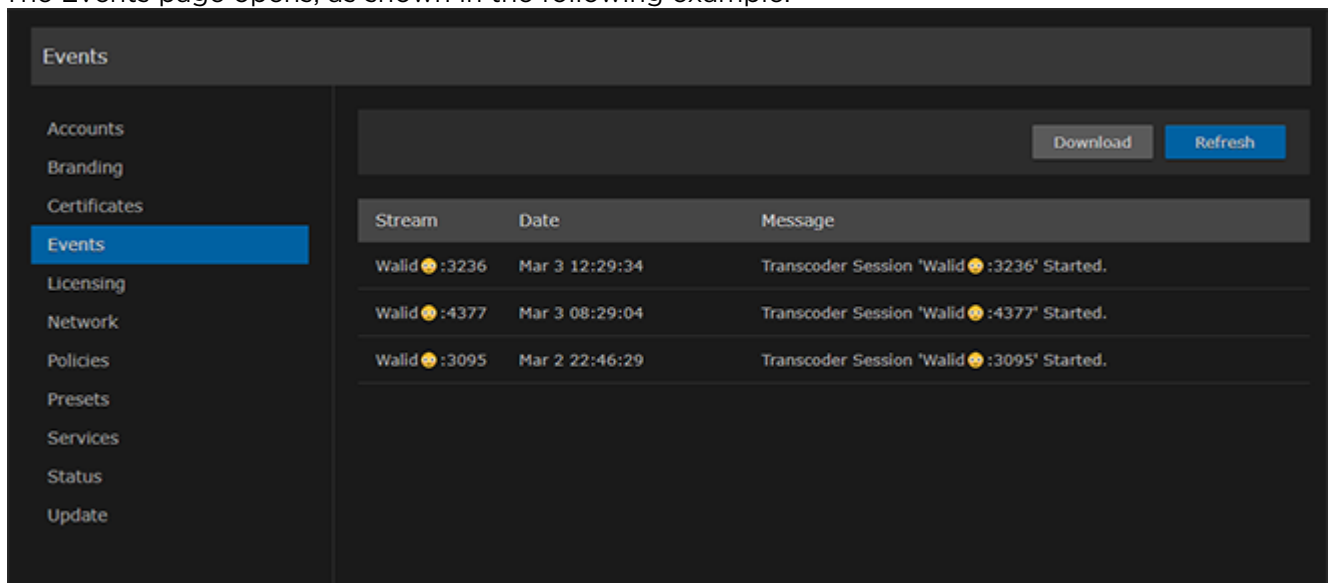
2. To refresh the list, click **Refresh**.
3. To download the list, click **Download** and save the log file. You can then open the log in a text editor.

Licensing Your Kraken

You can update your Kraken license directly from the Web Interface. Updating a license is typically required to expand the feature set or capabilities of the system, for example, to upgrade from SD to HD, enable KLV data, or obtain more input streams or unique transcodes.

Your first step is to obtain the new license file from Haivision Technical Support (**https:// support.haivision.com**). Next you need to copy and paste the new license string into the License page and submit it. Only a valid license will be accepted; if an invalid license is entered, it will be rejected and not replace the current license being used.

> ⚠ **Note**
>
> Kraken offers licensable options (perpetual licenses) for KLV pass-through, HEVC Encoding, as well as the number of H.264 encoding channels. HEVC Decoding does not require a license.

> ✅ **Tip**
>
> The Upgrade Version Limit indicates the highest version that the current license supports. For example, if the upgrade version limit is 2.8, you would need to re-license your system for 2.9 (or higher) prior to upgrading to 2.9.

To update your system license:

1. On the Administration page, click **Licensing** from the sidebar.
   The Licensing page opens displaying the installed license, including its expiration date and license

features, as shown in the following example.

> ⚠ **Note**
>
> If you are running a VM Kraken version, the Licensing page also shows the Instance UUID and CPU ID.

2. To update your license, copy and paste the new license string into the text box.
3. Click **Save Settings** to load the license.

Configuring Network Settings

From the Network Configuration page, you can modify Kraken's network interface settings, including configuring the unit with a valid IP address and gateway to work in your environment. You can configure the network to use either IPv4 or IPv6 addressing, or both. The default is IPv4.

> ⚠ **Note**
>
> Network settings are not configurable through the Web Interface on the software-only Kraken. The Network Settings page is only available for Kraken appliances.

From the Network Configuration page, you can modify the Kraken network interface settings. This includes general settings, such as specifying the server hostname and DNS servers, as well as advanced settings, such as setting up multiple network interfaces, link negotiation settings, and static routes.

The Network Configuration page shows the number of the available Network Interface Cards (NICs) depending on whether you have the High Density or Standard Density Kraken appliance. If available, you can configure additional NICs. Kraken can be configured to input streams from and/or send streams out on any of the available NICs.

> ⬣ **Caution**
>
> When you make changes to the Network Settings, be sure to write down the new IP Address or label the chassis. After you save your changes and reboot, you will have to redirect the browser to the new IP address and log in again in order to access the appliance.
>
> If you are connecting to the encoder through an IPv4 connection, disabling the IPv4 interface will drop your connection after a reboot. You will need to reconnect using IPv6 or the serial interface (if available).

To view and configure the Network Settings:

1. On the Administration page, click **Network** on the sidebar.
   The Network Configuration page opens, as shown in the following example.
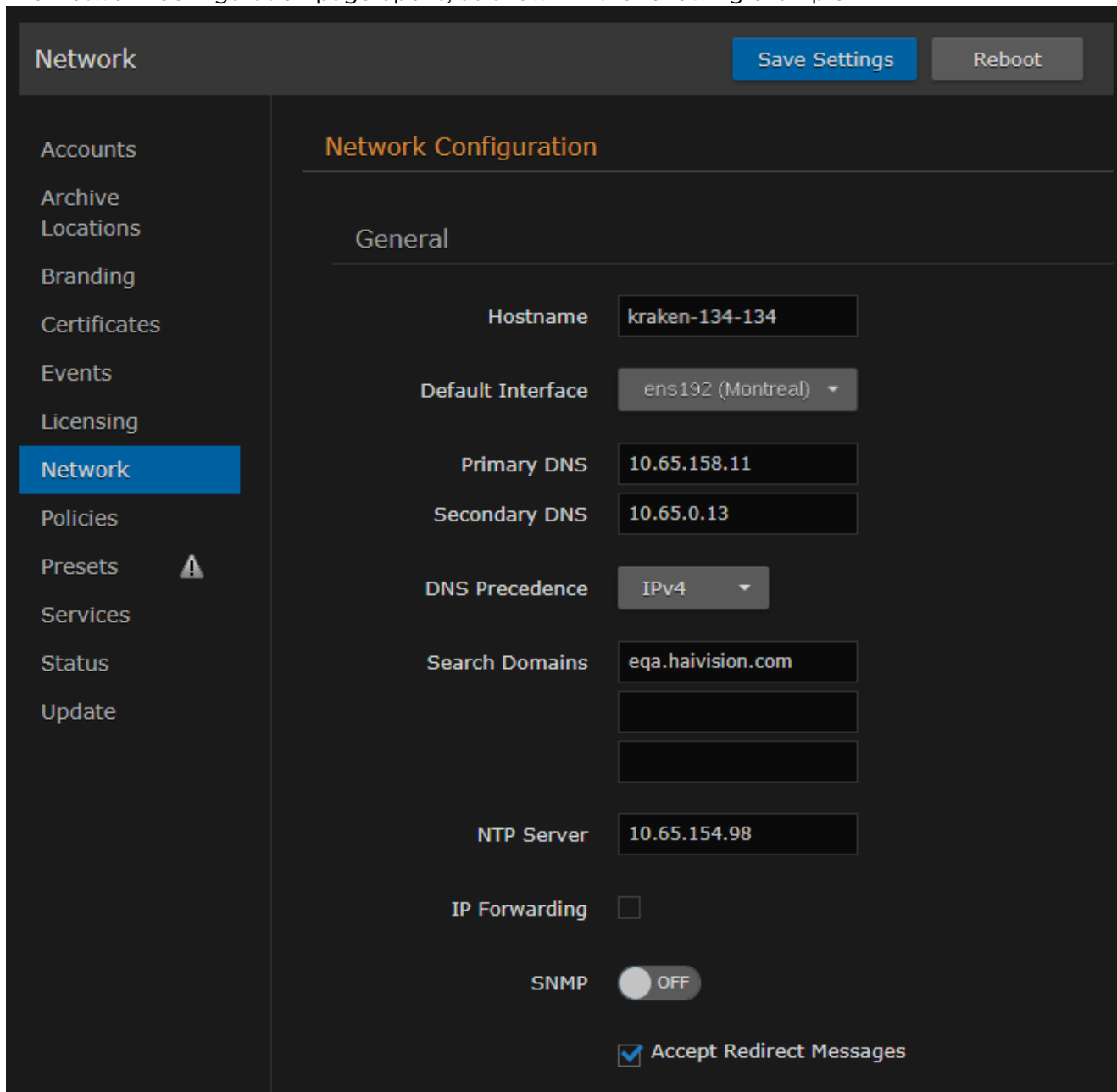
2. Fill in the General section. For details, see Network Settings.
3. Select the DNS Precedence (IPv4 or IPv6) to specify the priority DNS resolution.
4. To enable SNMP alerts, toggle the SNMP button to **On** and specify the read-only community string and trap server(s).

5. To configure additional NICs (Network Interface Cards) for the server, scroll down to the Interfaces section and click the next available interface tab (if available) and configure the required settings.

Interfaces

ens192   ens224

Interface General

User Description   Montreal

IPv4   ON

Addressing   Static

IP Address *   10.65.134.134

Subnet Mask *   255.255.255.0

Gateway   10.65.134.1

MTU   1500

MAC Address   00:50:56:95:65:87

Link   ⦿ Auto   ◯ Manual

IPv6   OFF

Static Routes

☐ All   Actions   ⊕

Destination	Mask/Prefix Len	Gateway	Interface

6. To configure IPv6 addressing, toggle IPv6 to **On**, and select the appropriate Addressing option. Enter the new value(s) as required. For details see 'IPv6' in **Network Settings**.

7. To add a static route, click the ⊕ **Add** button. Fill in the Destination, Subnet Mask, Gateway, and Interface in the Add Static Route dialog.

> ✅ **Tip**
>
> All entries in the routing table must be in dotted-decimal format.

8. Click **Save Settings**.
   You must reboot the system for the changes to take effect.
9. To apply your saved changes, click **Reboot**.

Kraken will reboot. You need to refresh the page after approximately five minutes to see the Sign-In page again.

Network Settings

The following table lists the Kraken Network settings:

General   **Interfaces**   **IPv4**   **IPv6**   **Static Routes**

General

Network Setting	Description/Values
Hostname	The hostname to be assigned to the Kraken. This is a FQDN (Fully Qualified Domain Name), for example, **myserver.mycompany.com**.
IPv4	When set to On, configures the network to use IPv4 addressing. See the 'IPv4' tab.
IPv6	When set to On, configures the network to use IPv6 addressing. See the 'IPv6' tab.
Default Interface	The default Ethernet interface: Select an available interface from the drop-down list. ⚠ **Note** Network Interface names for Ethernet interfaces vary, such as eth0/eth1/… or eno1/eno2/…. "None" or Blank indicates that the default interface is not set. To add customized interface names, as shown in the following example, see **User Description** under "Interfaces".
Primary DNS	(Optional) Enter the primary DNS server address for your network.
Secondary DNS	(Optional) Enter an alternate DNS server address for your network. The alternate DNS server is used only if the primary server is not responding.
DNS Precedence	Select either IPv4 or IPv6 to specify the priority for DNS resolution. On systems with both IPv6 and IPv4 enabled, if users use HOSTNAMES instead of specifying IP addresses when creating connections, the default behavior is to resolve to IPv6 first if it is available.
Search Domains	(Optional) The search strings to use when attempting to resolve domain names.
NTP Server	If the Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server.
IP Forwarding	Check this checkbox to enable IP forwarding when setting up streams using non-primary interfaces for their input.
SNMP	To enable SNMP (Simple Network Management Protocol) alerts for out-of-band monitoring, toggle this button to **On**. This tells Kraken to start the SNMP server, in order to query for OS information, such as CPU usage. SNMP alerts are typically used by IT administrators to monitor system health.
Read-Only Community	(SNMP must be enabled) Type in the SNMP community string associated with the SNMP Trap Server. This is the string to use when sending a trap to an SMTP Trap server. For example: "Kraken"
SNMP Trap Servers	(SNMP must be enabled) The SNMP server to send SNMP Traps to. This is an IPv4 or FQDN of an SMTP Trap server listening for traps via SNMP. For example: **SNMP1.mycompany.com**

General   **Interfaces**   IPv4   IPv6   Static Routes

Interfaces

Network Setting	Description/Values
User Description	(Optional) Enter a customized name for the network interfaces. This description appears beside the interface names on the Default Interface drop-down list (see above), as well as the Network Interface drop-down lists on the Input and Output creation pages.
eth0 | eth1 | eth2 | ...	Allows for multiple interfaces. Select the appropriate tab to view and configure. ⚠ **Note** Depending upon your device, the network interface prefixes may differ.

General   Interfaces   **IPv4**   IPv6   Static Routes

IPv4

Network Setting	Description/Values
Addressing	Select DHCP or Static to enable or disable the Dynamic Host Configuration Protocol (i.e. to use a static or dynamic IP address). Options are: • None: Select to disable the interface. • Static: Select to disable DHCP (Dynamic Host Configuration Protocol). When DHCP is disabled, you must manually enter the IP address and subnet mask. • DHCP: Select to enable DHCP. When DNCP is enabled, Kraken will get an IP address from a DHCP server on the network.
IP Address	Displays the IP Address for the Kraken appliance. This is a unique address that identifies the unit in the IP network. If DHCP is disabled, you may enter an IP address in dotted-decimal format.
Subnet Mask	This is a 32-bit subnet mask used to divide an IP address into subnets and specify the network's available hosts. If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.0.0).
Gateway	Displays the gateway address of the network (typically the address of the network router).This is the gateway that is used when no other route matches. This address must be reachable on your local subnet. If DHCP is disabled, you may enter a gateway address in dotted-decimal format.
MTU	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing data stream.
MAC Address	(Read-only) The Media Access Control address assigned to the interface. This is the physical address of the network interface and cannot be changed.

Network Setting	Description/Values
Link	Determines whether the Ethernet parameters are set automatically or manually (i.e., enables or disables autonegotiation): • Auto: The system will match the Ethernet Speed and Duplex Mode to the Ethernet hub to which it is connecting: • Manual: These values must be set manually. See following settings. ⚠ **Note** Always use Auto with Gigabit Ethernet (GigE) speed (1000 Mbps).

General   Interfaces   IPv4   **IPv6**   Static Routes

IPv6

Network Setting	Description/Values
Addressing	Select one of the following options to obtain an IPv6 address for the unit: • Automatic: Uses SLAAC (Stateless Address Autoconfiguration) to obtain IP addresses automatically without the need for a DHCP server • Automatic (DHCP): Enables the Dynamic Host Configuration Protocol to get an IP address from a DHCP server on the network • Static: Use to manually configure the device's IP and gateway addresses
Global IPv6 Address	If Automatic addressing is used, displays the IPv6 address (with a `/128` suffix). This is a unique address that identifies the unit in the IP network. If Static addressing is used, enter an IPv6 address in hexadecimal notation.
Global Temporary IPv6 Address	If privacy extensions (SLAAC) are being used with Automatic addressing, this field displays the temporary IPv6 address. The temporary address will change in accordance with network changes.
SLAAC Management Address	If Automatic addressing is used, displays the address assigned by SLAAC for management of the unit using the Subnet Prefix and the interfaces MAC address. This is a unique address that identifies the interface/device in the IP network.
Subnet Prefix Length	(**Static** Addressing only) The Prefix Length in IPv6 is the equivalent of the Subnet Mask in IPv4. However, instead of being expressed in four octets as it is in IPv4, it is expressed as an integer between 1 through 128.
Gateway	If Automatic addressing is used, displays the gateway address of the network (typically the address of the network router). If Static addressing is used, enter a gateway address in hexadecimal notation.
Privacy Extensions	(**Automatic** Addressing only) Check this checkbox to enable SLAAC Privacy Extensions. As documented in RFC 4941 "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", this entails using randomly generated, temporary, global scope IPv6 addresses that are regularly discarded and replaced with different addresses.
Duplicate Address Detection	Check this checkbox to automatically detect if your Link-Local IPv6 address is a duplicate of one already in use. If so, the Link-Local IPv6 Address changes to a unique address. See RFC 4862 "IPv6 Stateless Address Autoconfiguration" for more details.
Link-Local IPv6 Address	(Read-only) A link-local address is an Internet Protocol (IP) unicast address intended to be used only to connect to the hosts on the same network. A link-local address starts with fe80: and is always automatically assigned.

Network Setting	Description/Values
Accept Redirect Messages	(Disabled by default) Check this checkbox to accept ICMP redirect messages from remote routers. This enables Kraken to use a more direct route for a particular location. ⚠ **Note** Because these remote unauthenticated messages modify Kraken's route table, this capability should only be enabled within trusted environments.

For further IPv6 support details, see **IPv4 and IPv6 Support**.

General　　Interfaces　　IPv4　　IPv6　　**Static Routes**

Static Routes

Network Setting	Description/Values
Destination	Each static route requires a destination.
Subnet Mask/ Prefix Length	This is a 24-bit subnet mask used to divide an IP address into subnets and specify the network's available hosts. ⚠ **Note** If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.255.0).
Gateway	This is the gateway that is used when no other gateway matches. This address must be reachable on your local subnet. If DHCP is disabled, you may enter the gateway address in dotted-decimal format.
Interface	The interface associated with the static route. Use the drop-down menu to make your selection.

Managing Security Policies

From the Policies page, administrators can set Transport Layer Security (TLS) policies such as the accepted TLS versions and the reverse-path filter.

> ⚠ **Important**
>
> The TLS Version and RP Filter settings are *not* preserved across software updates and need to be re-applied when running a new version.

To view and manage the Security policies for the encoder:

1. On the Administration page, click **Policies** on the sidebar.
   The Policies page opens.
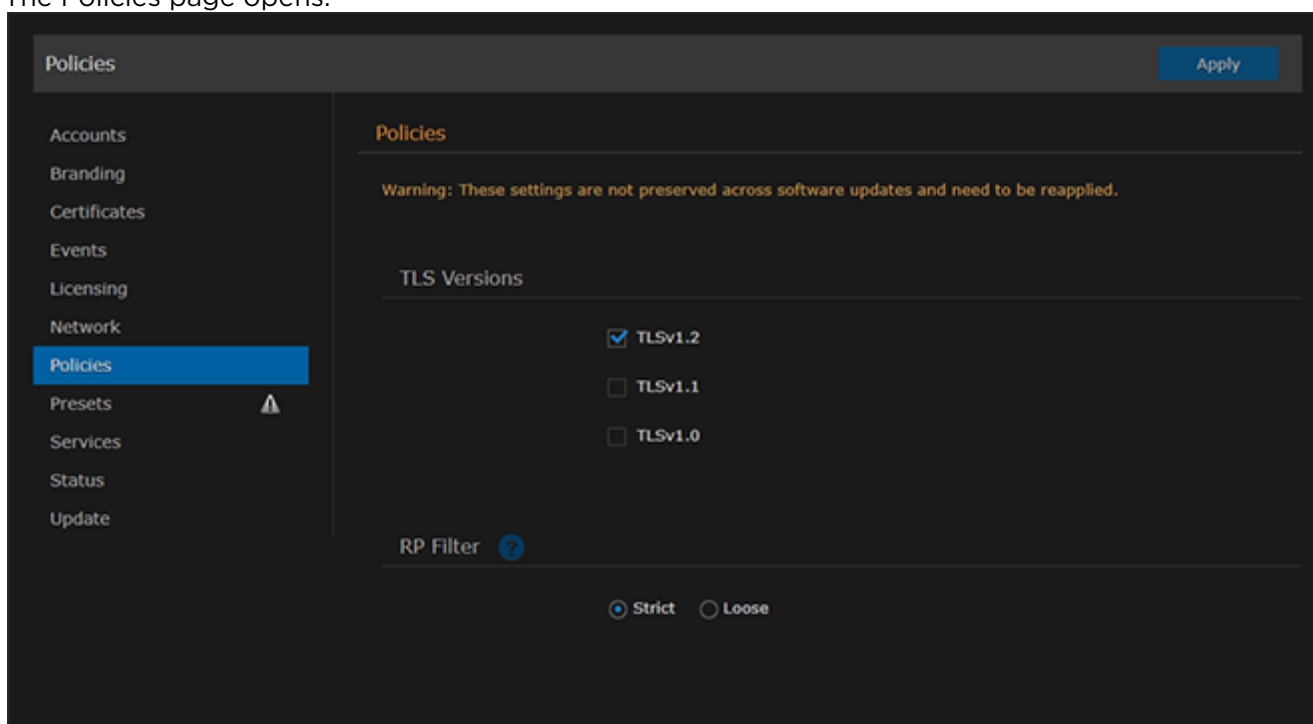
2. Select one or more TLS versions. For details, see **Policy Settings**.
3. (Optional) Select the RP (Reverse Path) filter. For details, see **Policy Settings**.
4. To apply your changes, click **Apply**.

Policy Settings

The following table lists the Policy settings for Kraken:

Policy Setting	Default	Description/Values
TLS Versions	TLSv1.2, TLSv1.1, TLSv1.0	Specifies which TLS (Transport Layer Security) versions are accepted from the HTTPS client. • TLSv1.2 • TLSv1.1 • TLSv1.0
RP Filter	Strict	Specifies the Reverse Path filtering method. Reverse-path filtering is a Linux Kernel feature (defined in RFC 3704) designed to ensure that packets that are not routable are dropped. Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface they were received on. It should not be used on systems that are routers for complicated networks, but is helpful for end hosts and routers serving small networks. Select either: • Strict: Each incoming packet to a router is tested against the routing table and if the interface that the packet is received on is not the best return path for the packet, then the packet is dropped. • Loose: Each incoming packet is tested against the route table and the packet is dropped if the source address is not routable through any interface. The allows for asymmetric routing where the return path may not be the same as the source path **✓ Tip** Set to Loose only if using asymmetric or other complicated routing.

Saving and Loading Presets

Each Kraken is configured by users' selecting and setting values of applicable system settings, such as transcoder and stream settings and the stream destination. Although these configuration settings are not automatically saved, presets provide a way for you to save groups of settings and recall these configurations settings to apply to other streams.

Configuration settings saved as the "startup" preset will continue to be used after a reboot, or when the unit is turned off and on. You can also direct the system to apply a preset to restore settings when the system startup process performs the configuration autoload.

From the Presets page, you can view the list of saved presets, load a saved preset, and save the current settings as a preset. You can also view the contents of a preset file, delete a preset, and select the preset to load at startup.

> ⚠ **Note**
>
> A warning indication ⚠ appears in the title bar on systems where changes to Streams, Inputs, Transcoders, Outputs, or Metadata have been applied but not saved to a preset. The indication is displayed when a user signs out or in to Kraken. The warning indication disappears when you reload or save the present.
>
>
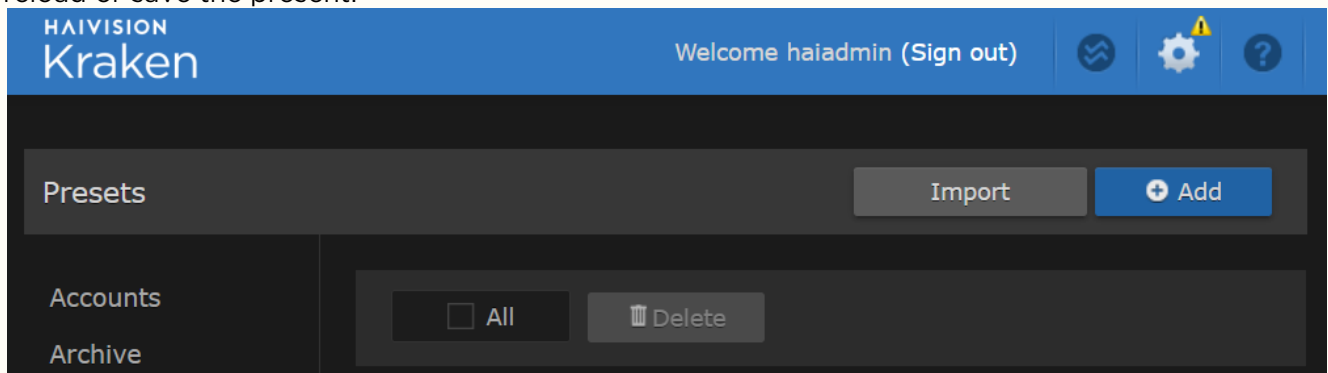
> ✓ **Tip**
>
> The stream state (started/stopped) is not saved in presets, and therefore, manually starting or stopping the stream does not trigger the warning indication. When Kraken reboots or loads or saves a preset, the stream uses the Auto-Start value and not the actual stream state (i.e., if it was started or stopped manually with the Start or Stop button).

To view and manage presets:

1. On the Administration page, click **Presets** on the sidebar.
2. The Presets List View opens displaying the list of saved presets for the transcoder, as shown in the following example.
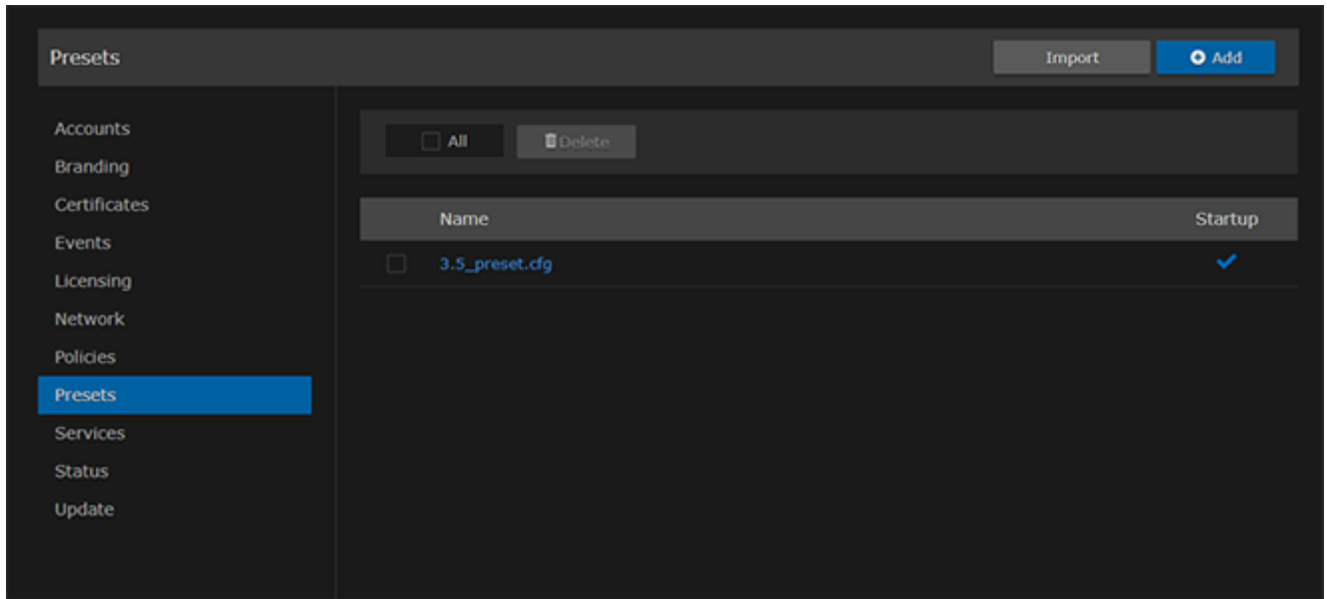
The Presets List View opens displaying the list of saved presets for the transcoder, as shown in the following example.

3. To load an existing preset into the current session, hover over the preset name or anywhere in the row and click ⬆ **Load**.
4. To select an existing preset to load at startup, hover over the preset row and click the (grayed out) check mark under **Startup**.
5. To save the current settings as a new preset, click ⊕ **Add** button.
   a. In the New Preset dialog, type a new filename in the Name text box.
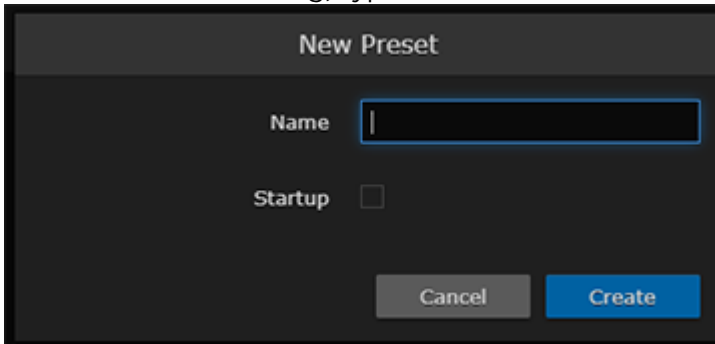
   b. To select this preset to load at startup, check the **Startup** checkbox.
   c. Click **Create**.
6. To save the current settings as an existing preset, hover over the preset row and click **Save**. You can (optionally) check the **Startup** check mark.
7. To save the preset as a text file to view or export to other Kraken encoders, click the preset name and save it in the Save As dialog. Note that the file is in Unix format.
8. To import a preset, for example, from another Kraken encoder, click **Import** and select the file in the Open File dialog box.

9. When you see the filename in the text box, click **Upload**.
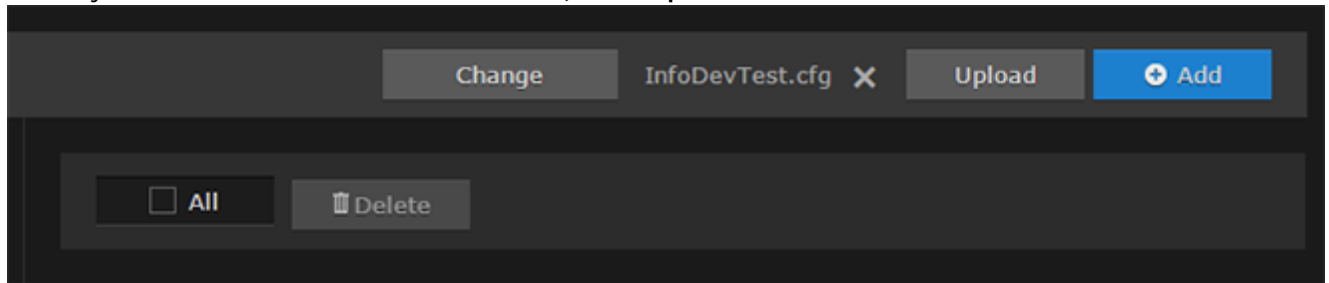
> ✅ **Tip**
>
> To select a different preset file, click **Change**. To remove the selection, click the ✖ icon. To delete one or more presets, check the checkbox next to one or more preset names (or check **All**) and click 🗑 **Delete** on the Content toolbar.

Enabling and Disabling Services

For security purposes, an administrator may need to stop one or more services from accessing Kraken. From the Services page, you can enable and disable network or input capture services, including SDI (DeckLink) Capture, GigE Capture, NDI Capture, ST2110 Capture, Analog (V4L2) Capture, RTSP and SSH.

You can also select which network interfaces allow access to the Kraken Web and API interface in a multi-NIC system. This enables separation of streaming and management interfaces on Kraken.

> ⚠ **Note**
>
> Some services require a valid Kraken license to enable control of the desired Kraken service.

To enable or disable services:

1. On the Administration page, click **Settings** on the navigation bar and **Services** on the sidebar. The Services page opens displaying the current status of network services (as shown in the following example).
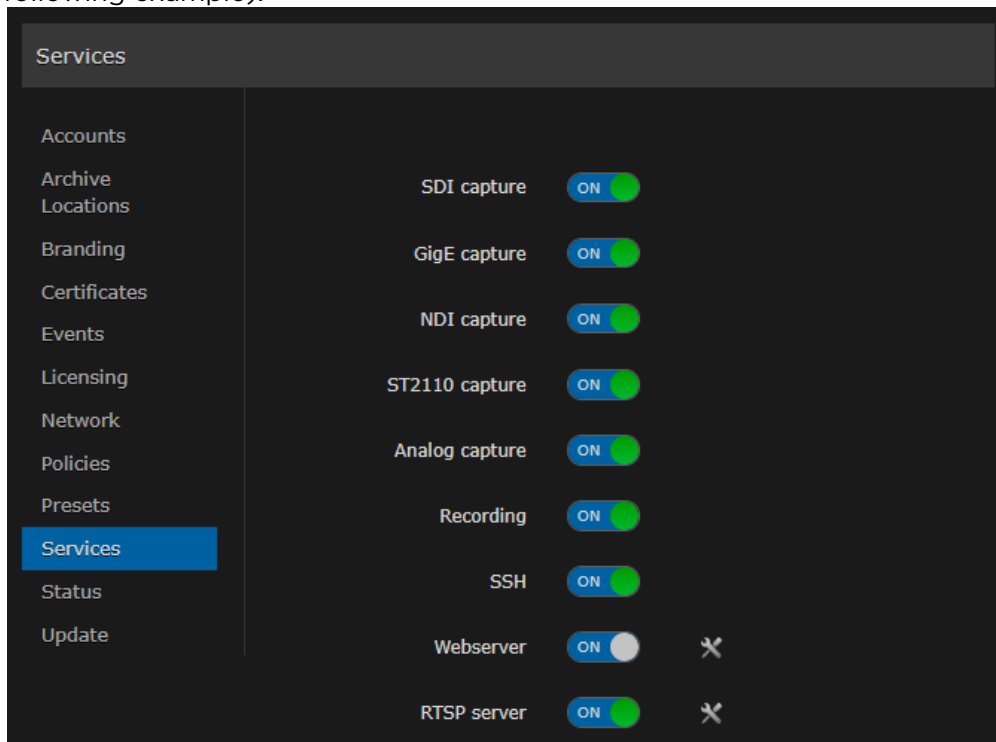
⚠ **Note**

The On-Off button color indicates the service status:

Color	Indication
Green	Service is started and operating as expected.
Red	Services is not operating correctly, or failed to start.
Orange	Service is started and operating, but requires attention or configuration to operate as expected.
Grey	Service is stopped.
White	Service cannot be disabled.

2. To enable or disable a service, toggle the associated Service button to **On** or **Off**. For details, see **Services Settings**.
3. To select which network interfaces allow access to the Kraken Web and API interface, hover over the Webserver row and click ✖ **Configure**. See **Services Settings** for configuration details.

The service(s) will be stopped or started immediately. (You do not need to click **Apply**).

RTSP Server Service

The RTSP server in Kraken enables the Kraken transcoder to interoperate with Real-Time Streaming Protocol (RTSP)-based clients which pull media from Kraken. These clients include desktop players like QuickTime and VideoLan VLC, as well as Video Management Servers (VMS) like those from Milestone and Genetec.

The RTSP Server Service can be configured to operate from the Services page:

1. On the Services page, toggle the RTSP button to **On**.
2. Click ✕ **Configure** next to the RTSP toggle.
3. If applicable, type in the desired RTSP Port number in the dialogue box.

> ⚠ **Note**
>
>   The default RTSP server port is 554.
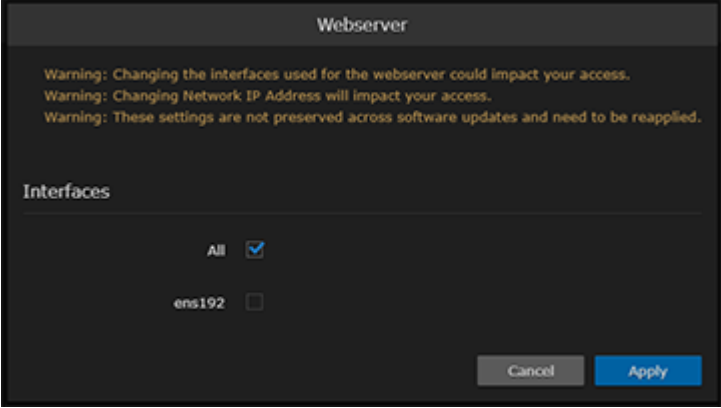
4. Click **Apply**.
5. If you have active streams using RTSP pull outputs, you must manually restart the Kraken to apply the RTSP port change.

Related Topics:

- **Configuring RTSP Outputs**
- **Services Settings**

Services Settings

The configurable Services are as follows:

Service	Description/Values
SDI capture	Enables video capture and encoding of SDI input from a DeckLink Micro Recorder device.
GigE capture	Enables video capture and encoding of input from a GigE Vision camera.
NDI capture	Enables video capture and encoding of input from a **Network Device Interface (NDI)** device.
ST2110 capture	Enables video capture and encoding of ST2110 input from an SFP SDI to IP gateway device.
Analog capture	Enables video capture and encoding of Analog input from a V4L2 device.
SSH	Secure Shell, a network protocol that allows data to be exchanged using a secure channel between two networked devices.
Webserver	(Multi-NIC systems) Selects which network interfaces allow access to the Kraken Web and API interface. 1. Hover over the Webserver row and click ✕ **Configure**. 2. On the Webserver dialog, select "All" or one or more of the available interfaces. **⚠ Note** At least one network interface must always be enabled.
RTSP Server	Enables RTSP streaming to remote clients. For information on how to configure the RTSP Server, see **RTSP Server Service** and **Configuring RTSP Outputs**.

Monitoring the System Status

The Status page displays Kraken system status information such as the version, system load, system uptime, and licensed capacity.

You can also reboot or shut down Kraken, as well as take a system snapshot from the Status page.

To view status information:

1. Click the ⚙ **Administration** icon on the toolbar to navigate to the Administration page.
2. Click **Status** on the sidebar.
   The Status page opens, as shown in the following example.
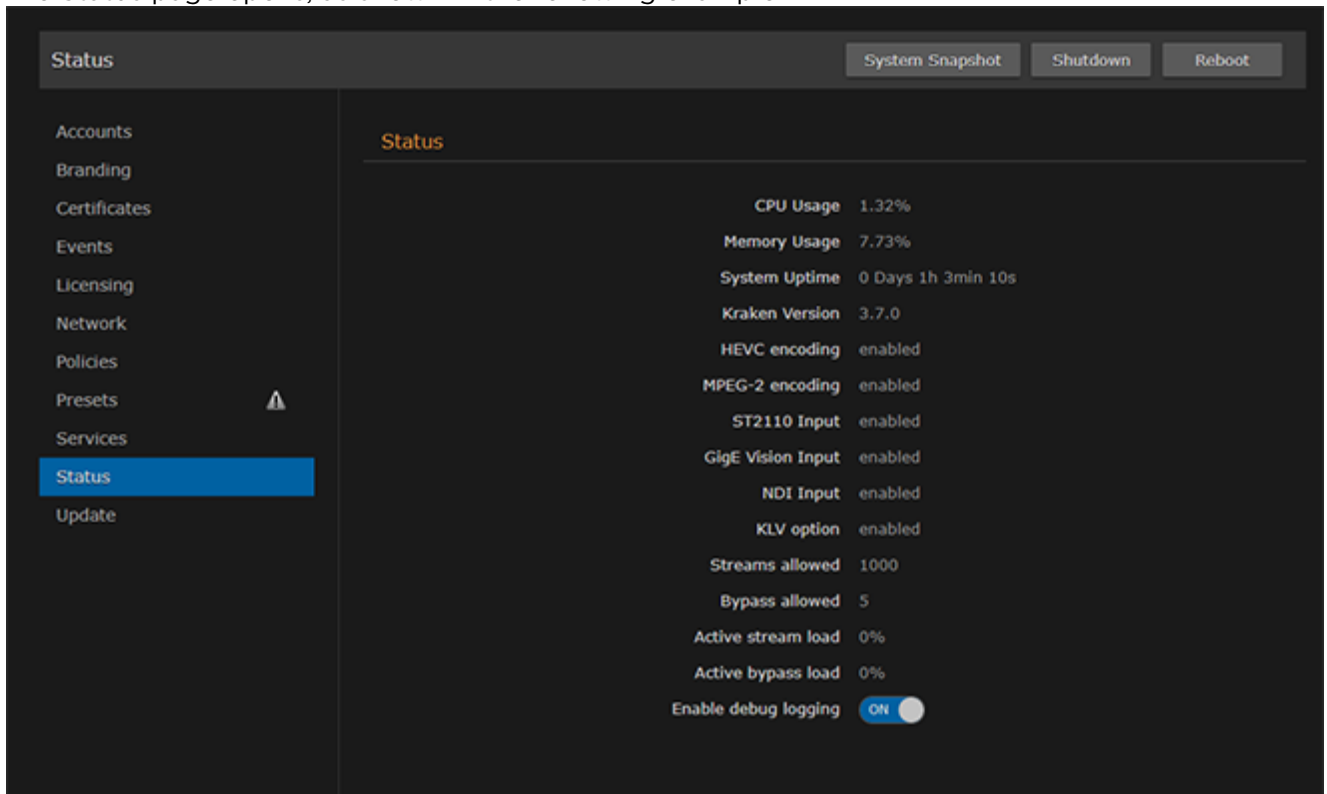
The Status settings are read-only. For details, see Status Settings.
3. To reboot the transcoder, see Rebooting Kraken.
4. To display a snapshot of system information, see Taking a System Snapshot.

HAIVISION

Status Settings

The following table lists the Status settings. Status information can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

Status Setting	Description/Values
CPU Usage	The combined CPU usage (across all cores). [100% minus the percentage of time the CPU remains idle.]
Memory Usage	The total RAM usage in percentage% (does not include swap space = 0).
System Uptime	The length of time (dd:hh:mm:ss) the appliance has been "up" and running.
Kraken Version	The Kraken firmware version, e.g., v2.6- XXXXX
HEVC Encoding	Whether the HEVC Encoding license is enabled or disabled.
MPEG-2 Encoding	Whether the MPEG-2 Encoding license is enabled or disabled.
ST2110 Input	Whether the ST2110 Input license is enabled or disabled.
GigE Vision Input	Whether the GigE Vision Input license is enabled or disabled.
NDI Input	Whether the Network Device Interface Input license is enabled or disabled.
KLV option	Whether the KLV pass-through license is enabled or disabled.
Streams allowed	The number of HD/SD H.264 channels licensed.
Bypass allowed	The number of bypass streams licensed.
Active stream load	The system load based on the Stream license. Each active Transcode Stream counts against the Active Stream Load. When Bypass Streams is unlicensed, each active Bypass Stream also counts against the Active Stream Load.
Active bypass load	The system load based on the Bypass license. When Bypass Streams is licensed, each active Bypass Stream counts against the Active Bypass Load. This status value is available when Bypass Streams is licensed.
Load calculated based on	The rules that describe the load calculation.
Enable debug logging	Set to On or Off to enable or disable transcoder debug logging. ⚠ **Note** Enabling transcoder logs may affect system performance and should *not* be used in production. We recommend that transcoder logs be used for debugging purposes only, under the guidance of Haivision Technical Support. Transcoder logs are Off by default and can be turned On/Off individually for each stream with a button in the Stream Statistics page. If you disable debug logging, streams with logs previously enabled will be restarted.

Status Setting	Description/Values
System Snapshot	Displays a snapshot of system information in a new window. See Taking a System Snapshot.
Reboot	Reboots the transcoder. See Rebooting Kraken.

Rebooting Kraken

To reboot Kraken:

1. Click the ⚙ **Administration** icon on the toolbar and click **Status** on the sidebar.
2. On the Status page, click **Reboot**.
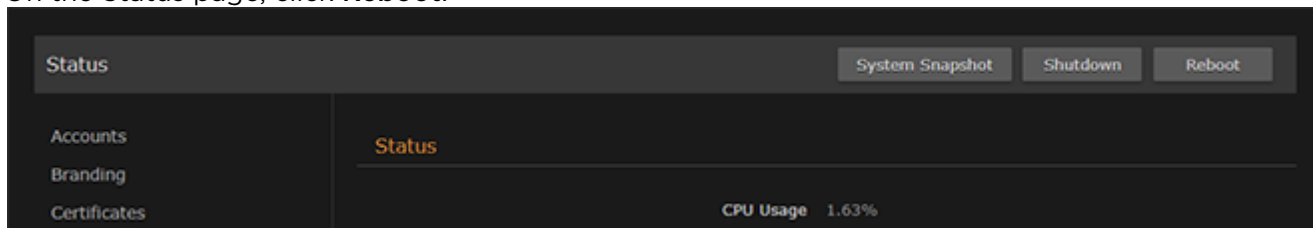
Kraken will reboot and you will be returned to the Login page. If you did not save your configuration/presets, you will end up with the default configuration with no streams at all.

Taking a System Snapshot

Taking a system snapshot can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

The system snapshot lists information such as component versions, network settings, loaded modules, running processes, system traces, configured streams and stream status checks, configured video encoders and status checks, configured audio encoders and status checks, startup configuration file contents, global settings file contents, debug logging settings file contents, downloaded software packages, last software update log, and OS statistics.

> ✓ **Tip**
>
> The system snapshot includes device probe information, to show any hardware encoder/decoder acceleration capabilities available on your Kraken system (VM or appliance). These include:
> - NVIDIA hardware capabilities and current State
> - Intel hardware capabilities and current State
> - Capture device capabilities and current State

To take a system snapshot:

1. From the Status page, click **System Snapshot**.
   The system will display a timestamped snapshot of system information in a new window, as shown

in the following example:

```
================================================================================
START OF SYSTEM SNAPSHOT
================================================================================


--------------------------------------------------------------------------------
Credentials:
--------------------------------------------------------------------------------
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0

--------------------------------------------------------------------------------
Local Time:
--------------------------------------------------------------------------------
Tue Apr 16 13:44:06 EDT 2019

--------------------------------------------------------------------------------
Universal Time:
--------------------------------------------------------------------------------
Tue Apr 16 17:44:06 UTC 2019

--------------------------------------------------------------------------------
System UP Time:
--------------------------------------------------------------------------------
 13:44:06 up 3 days, 23:38,  1 user,  load average: 0.23, 0.18, 0.12

--------------------------------------------------------------------------------
System Information:
--------------------------------------------------------------------------------
Created VFLOG to HVMAF Logger adapter.
Haivision Transcoder Application -- Version 2.9.0-52-RELEASE
{
    "release-info": {
        "product": "Kraken",
        "version": "2.9.0",
        "build_id": "52",
        "build_type": "RELEASE",
        "commit_id": "885b30455a372a47e6c9077cc3b4bfa20e564c52",
        "pretty_version": "2.9.0-52",
        "pretty_name": "Haivision Kraken release 2.9.0-52"
    }
}

================================================
IGNORE Protobuf SPAM
================================================


HVMAF DeckLink Capture Client -- hvmaf-0.9.0 (20190327 12:34:27)

ffmpeg version 885b30455a372a47e6c9077cc3b4bfa20e564c52-VF Copyright (c) 2000-2018 the FFmpeg developers
built with gcc 4.4.7 (GCC) 20120313 (Red Hat 4.4.7-23)
configuration: --extra-version=VF --prefix=/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/ffmpeg --cc=/usr/bin/gcc --objcc=/usr/bin/gcc --cxx=/usr/bin/g++ --ar=/usr/bin/ar --nm=/usr/bin/nm --target-os=linux --
arch=x86_64 --cpu=x86_64 --enable-pic --enable-static --enable-shared --enable-rpath --disable-appkit --enable-avfilter --enable-zlib --enable-
bzlib --enable-runtime-cpudetect --enable-hardcoded-tables --disable-doc --disable-audiotoolbox --disable-videotoolbox --disable-amf --disable-
cuda --disable-cuvid --disable-d3d11va --disable-dxva2 --disable-nvdec --disable-nvenc --disable-vdpau --
x86asmexe=/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/tools/nasm/bin/nasm --sdl2-
config=/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/sdl2/lib/../bin/sdl2-config --
enable-vaapi --disable-vaapi-x11 --extra-cflags='-I/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/zlib/include -I/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/bzip2/include -I/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/lzma/include -I/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/sdl2/include -I/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/vaapi/include -DVFBUILD_DISABLE_INTMATH_OPTIMIZATIONS=1' --extra-ldflags='-L/var/tmp/tinderbox_build/vfcore-
kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/zlib/lib -L/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-
2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/bzip2/lib -L/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-
ortbuild/ort/stage/lzma/lib -L/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/sdl2/lib -
L/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/vaapi/lib -Wl,-
rpath,/var/tmp/tinderbox_build/vfcore-kraken/2.9/release_Kraken-2.9.0/vf.git/vfcore/kraken-ortbuild/ort/stage/vaapi/lib' --disable-stripping --
enable-optimizations
libavutil      56. 21.100 / 56. 21.100
libavcodec     58. 34.202 / 58. 34.202
libavformat    58. 19.202 / 58. 19.202
libavdevice    58.  4.106 / 58.  4.106
libavfilter     7. 39.200 /  7. 39.200
libswscale      5.  2.100 /  5.  2.100
libswresample   3.  2.100 /  3.  2.100


================================================
IGNORE Protobuf SPAM
================================================


HVMAF Shared Memory IPC EnCoder -- hvmaf-0.9.0 (20190327 12:34:27)
```

2. Save the file.

Installing System Updates

> ✅ **Tip**
>
> On systems licensed for MPEG-2 output, when upgrading from v2.5.0 or earlier, you will need to apply the license *before* the upgrade and a second time after the upgrade to license the new features.

When you first receive a Kraken appliance, the necessary software is pre-installed on it. System updates are available for download through the **Haivision Support Portal**. When a system update becomes available, you can easily install it from the Web interface after downloading the file to your local computer or network. The firmware update comes in the form of a file with the extension .hai, which when loaded will replace the application on your Kraken. Please refer to the Product Bulletin for release-specific details regarding upgrading from current vs. previous platforms.

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

To install a firmware update:

1. On the Administration page, click **Update** on the sidebar.
   The Update page opens displaying the currently installed firmware version, as shown in the following example.
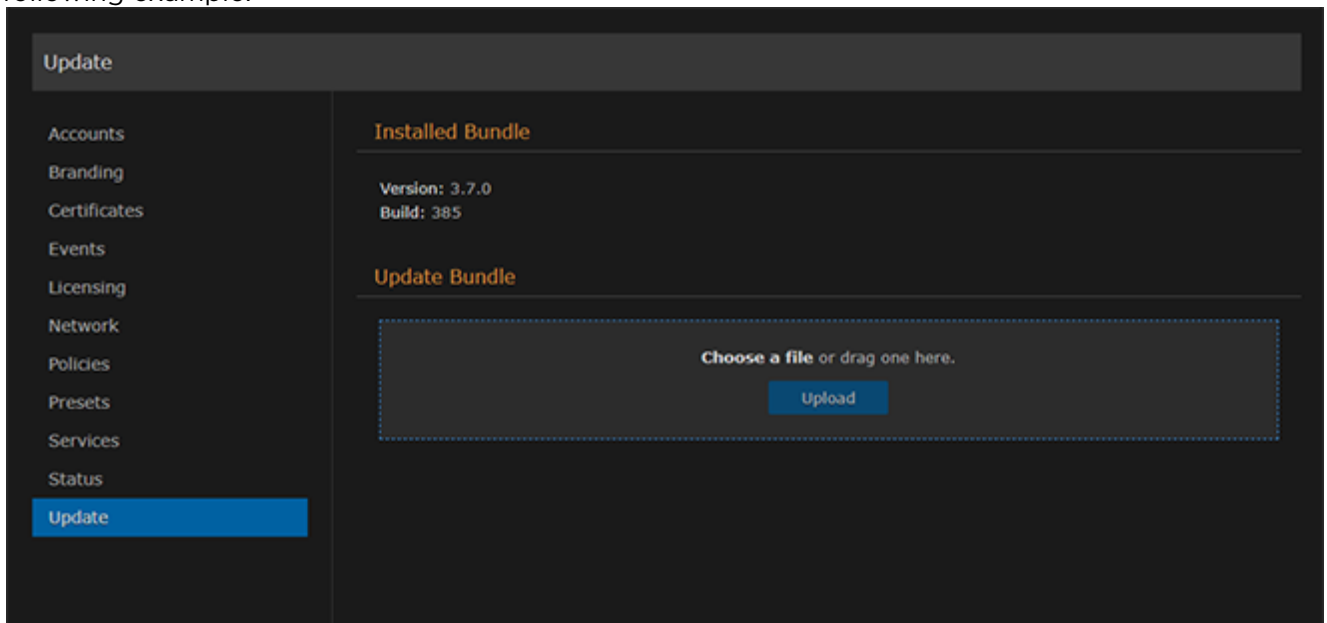
2. Drag an update bundle (titled `Kraken-x.x.x_rxxxx_RELEASE.hai`) to the drop area or click **Choose a file** to select a bundle to load.
3. A confirmation appears showing the filename. Click **Upload** to continue.
   The progress bar shows the progress of the upload.

> ⚠ **Important**
>
> Wait for the file to be uploaded. Remain on this page and do *not* click anything else in the Kraken Web interface during the upload.

4. After the bundle is uploaded and verified, click **Update** and then click **Confirm**.
5. Wait until the update is complete and your Kraken system reboots.

> ⚠ **Caution**
>
> You must remain on this page until the system completes the process of unpacking the firmware. Failure to do so could result in damage to your system.

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

> ✓ **Tip**
>
> After upgrading, clear your browser's cache to ensure that all new screens display correctly.

Technical Specifications

This section lists the technical specifications for Kraken.

Topics Discussed

- Transcoding
- Video Processing
- Networking
- Management
- Kraken Transcoding System
- Physical
  - Kraken Server Premium System (S-KR-PREMIUM-KLV)
  - Kraken Server Ultra System (S-KR-ULTRA)
  - Kraken CR (S-KR-CR-KLV)
  - Kraken Edge (S-KR-SFF / S-KR-SFF-XC)

Transcoding

Sources	Metadata Pass-through (Supported Standards)
• Makito, Piranha Encoders • 3rd Party Encoders • MJPEG from L-3 Vortex • Digital Video Broadcast	• Closed Captioning (EIA-608 & EIA-708) • KLV with support of both Asynchronous and Synchronous KLV • Support of MISB Standard 0601 • Support of MISB Standard 0604 • SMPTE 336M-2007 Data Encoding Protocol

Input H.265/HEVC	Output H.265/HEVC
• Main Profile • Up to Level 4 (1080p30) • Transport Stream • Up to 10 Mbps • CBR, VBR	• Main Profile • Up to Level 4 (1080p30) • Transport Stream • Up to 10 Mbps • Transport Stream Shaping, VBR
Input H.264/AVC	**Output H.264/AVC**
• Baseline, Main, High Profile • Up to Level 4.2 (1080p60) • Transport Stream • 0 kbps - 20 Mbps • CBR, VBR	• Baseline, Main, High Profile • Up to Level 4.2 (1080p60) • Transport Stream • Up to 20 Mbps • Transport Stream Shaping, VBR
Input MPEG-2	**Output MPEG-2 Video**
• MainProfile@MainLevel (SD) • MainProfile@HighLevel (HD) • Transport Stream • Up to 20 Mbps • CBR, VBR	• Simple and Main Profile@MainLevel • Up to 10 Mbps • Transport Stream Shaping, VBR
Input MJPEG	**Output AAC Audio**
• HTTP MJPEG sources • Validated against L3 Vortex	• AAC 2 channel • Audio Sync Preserved
Input Audio	**Output MPEG-1 Audio**
• MPEG1 layer 2 • AAC 2 channel and 5.1	• 2 Channel MPEG-1 Layer II • Audio Sync Preserved
	Output MPEG-4 Part 2
	• Transport Stream Shaping, VBR

Video Processing

Video Processing
De-interlacing
Down Scaling
Aspect Ratio Preserved
Configurable Frame Rate

Networking

Networking
Single Program Transport Stream (SPTS)
⚠ **Note** Multi Program Transport Stream (MPTS) inputs are *not* supported.
Unicast/Multicast
TS over UDP
SRT
RTSP (input only)
Session Announcement (SAP)

Management

Management
Web User Interface (HTTPS only)
REST API v1.0 and v2.0
Console UI

Kraken Transcoding System

Kraken Transcoding System	
Operating System:	Embedded Linux (CentOS7)
Standard IP Interfaces:	2 x RJ-45 Ethernet

Physical

Topics Discussed

- Kraken Server Premium System (S-KR-PREMIUM-KLV)
- Kraken Server Ultra System (S-KR-ULTRA)
- Kraken CR (S-KR-CR-KLV)
- Kraken Edge (S-KR-SFF / S-KR-SFF-XC)

Kraken Server Premium System (S-KR-PREMIUM-KLV)

Physical Specifications - Kraken Server Premium System (S-KR-PREMIUM-KLV)	
Capacity:	• Up to 8x HD H.264/AVC encoding channels • Up to 2x HD H.265/HEVC encoding channels
Dimensions (H x W x D):	Dimensions without faceplate (1RU): • 1.68" x 17.09" x 23.9" • 42.8 mm x 434.0 mm x 607 mm
Weight:	43.87 lbs. (19.9 kg)
Power:	2x Redundant 100-240 VAC 550 W Power Supplies

Kraken Server Ultra System (S-KR-ULTRA)

Physical Specifications - Kraken Server Ultra System (S-KR-ULTRA)	
Capacity:	• Up to 16x HD H.264/AVC encoding channels • Up to 4x HD H.265/HEVC encoding channels
Dimensions (H x W x D):	Dimensions without faceplate (1RU): • 1.68″ x 18.98″ x 27.6″ • 42.8 mm x 482.3 mm x 700.5 mm
Weight:	59 lbs. (26.76 kg)
Power:	2x Redundant 100-240 VAC 750 W Power Supplies

Kraken CR (S-KR-CR-KLV)

Physical Specifications - Kraken CR (S-KR-CR-KLV)	
Dimensions (H x W x D):	44.45mm H x 124.968mm W x 213.868mm D (1.75″ H x 4.92″ W x 8.42″ D)
Weight:	2.6 lbs (1.18 Kg)
Power Requirements:	12-28VDC, 45W 100-240VAC External locking power supply
Temperature:	Operating: 0ºC to 50ºC (32ºF to 122ºF) Non-Operating: -40ºC to 50ºC (-40ºF to 122ºF)

Kraken Edge (S-KR-SFF / S-KR-SFF-XC)

Physical Specifications - Kraken Edge Base Transcoding System (S-KR-SFF-XC) and Base Media System (S-KR-SFF)	
Dimensions (H x W x D)	182.00 mm H x 36.00 mm W x 178.56 mm D (7.16 in. H x 1.42 in. W x 7.03 in. D)
Weight	3.04 lbs (1.38 kg) ⚠ **Note** The weight depends on the configuration ordered and the manufacturing variability.
Power Supply	130 W, 4.5 mm (for 35 W CPU)
Temperature	Operating: 10°C–35°C (50°F–95°F) Non-Operating: -40ºC to 65ºC (-40ºF to 149ºF)
Relative humidity (maximum)	Operating: 20% to 80% (non-condensing) Non-Operating: 5% to 95% (non-condensing)
Vibration (maximum)	Operating: 0.26 GRMS random at 5 Hz to 350 Hz Non-Operating: 1.37 GRMS random at 5 Hz to 350 Hz
Shock (maximum)	Operating: Bottom half-sine pulse with a change in velocity of 50.8 cm/sec (20 in./sec) Non-Operating: 105G half-sine pulse with a change in velocity of 133 cm/sec (52.5 in./sec)
Altitude (maximum)	Operating: 3048 m (10,000 ft) Non-Operating: 10,668 m (35,000 ft)

Warranties

1-Year Limited Hardware Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

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

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

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

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

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

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

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

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

OBTAINING WARRANTY SERVICE

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

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

APPLICABLE LAW

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

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

EULA - End User License Agreement

READ BEFORE USING

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

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

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

SLA - Service Level Agreement

1. Introduction

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

2. Definitions

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

3. Service Levels for the Video Content Management System

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

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

4. Exceptions to Availability for the VCMS

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

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

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

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

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

5. Credits for Downtime for the VCMS

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

6. Support Services for the VCMS

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

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

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

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

7. Service Levels for Haivision Streaming Media Service

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

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

Agents and Polling Frequency

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

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

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

8. Credits for Outages of Haivision Streaming Media Service

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

9. No Secondary End User Support

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

Getting Help

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