Makito
X Series

Makito™ X
Decoder Family
User's Guide v2.1

HVS-ID-UG-MAKX-DEC-21
Issue 02

Haivision

Copyright

Document Number: HVS-ID-UG-MAKX-DEC-21
Version Number: v2.1-02

If you have comments or suggestions concerning this user's guide, please contact:

Technical Publications Department
Haivision
4445 Garand
Montréal, Québec, H4R 2H9 Canada

Telephone: 1-514-334-5445
Toll-free (North America) 1-877-224-5445
infodev@haivision.com

Trademarks

Third Party License Information

UDT4, 4.11, UDP-based Data Transfer, Permissive free software license.

- Neither the name of the University of Illinois nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

expat Custom License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

libuuid Modified Licensed (Modified BSD)

Safety Guidelines

Use the following guidelines when unsafe conditions exist or when potentially hazardous voltages are present:

- Always use caution and common sense.
- To reduce the risk of electrical shock, do not operate equipment with the cover removed.
- Repairs must be performed by qualified service personnel only.

Safety Information

WARNING This product is intended for installation in a restricted area. Limited access areas are protected by a specific mechanism, lock and key or other security device.

ATTENTION Ce produit est destiné à être installé dans une zone d'accès restreint. Les zones d'accès limité sont protégées par un mécanisme spécifique, une serrure et une clé ou tout autre dispositif de sécurité.

WARNING Since it is the main disconnect device, the plug-socket assembly must be accessible at all times.

ATTENTION Comme il constitue le principal dispositif de déconnexion, l'ensemble fiche-prise doit être accessible à tout moment.

WARNING The installation of the equipment must comply with local and national electrical regulations.

ATTENTION L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.

EMC Warnings

Notice with respect to Class A (FCC)

Changes to equipment without the permission of Haivision may result in its failure to comply with the FCC requirements for Class A digital devices. If applicable, your rights to use the equipment may be limited By the FCC rules and you may be able to remedy, at your own expense, any interference with radio or television equipment. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15

of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference that may occur when the equipment is used in a commercial environment. This equipment generates, uses and can radiate radio frequency energy. If not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Use of this equipment in residential areas may cause harmful interference. If necessary, users will have to resolve these issues at their own expense.

Avis relatif aux appareils de classe A (FCC)

Toute modification de l'équipement sans l'autorisation de Haivision peut entraîner sa non-conformité aux exigences de la FCC concernant les appareils numériques de classe A. Le cas échéant, vos droits d'utilisation de l'équipement seront susceptibles d'être limités par les règlements de la FCC et vous pourrez être amené à remédier, à vos frais, aux éventuelles interférences avec des dispositifs radiophoniques ou télévisuels. Cet équipement a été testé et jugé conforme aux limites d'un périphérique numérique de classe A en vertu de la partie 15 des règlements de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé ni utilisé conformément au manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. L'utilisation de cet équipement dans les zones résidentielles est susceptible de causer des interférences nuisibles. Le cas échéant, les utilisateurs devront résoudre ces problèmes à leurs frais.

Notification for Class A (Canada)

This Class A digital apparatus complies with Canadian ICES-003.

Notification pour les appareils de classe A (Canada)

Cet appareil numérique de Classe A est conforme à la norme NMB-003 du Canada.

Safety instructions for Class A for CISPR22

WARNING**:** This product is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to take appropriate measures.

Consigne de sécurité relative à la Classe A pour CISPR22

ATTENTION: Il s'agit d'un produit de Classe A. Dans un environnement domestique, ce produit peut entraîner des perturbations radioélectriques, auquel cas l'utilisateur devra éventuellement prendre des mesures adéquates.

Antistatic Precautions

Electrostatic discharge (ESD) results from the buildup of static electricity and can cause computer components to fail. Electrostatic discharge occurs when a person whose body contains a static buildup touches a computer component.

The equipment contains static-sensitive devices that may be easily damaged, and proper handling and grounding is essential. Use ESD precautionary measures when installing systems or cards, and keep the parts and cards in antistatic packaging when not in use. If possible, use antistatic floorpads and workbench pads.

Improper handling and/or installation practices may VOID the warranty.

CAUTION When handling components, or when setting switch options, always use an antistatic wrist strap connected to a grounded equipment frame or chassis. *If a wrist strap is not available, periodically touch an unpainted metal surface on the equipment.* Never use a conductive tool, such as a screwdriver or a paper clip, to set switches.

Fan Blade

Do not touch or push the fan blade with fingers or other objects. Doing so may damage the fan and/or fan bearings, which can result in a noise problem as well as accelerated failure of the mechanical part.

Waste Electrical and Electronic Equipment (WEEE) Disposal

This symbol on Haivision products or packaging means that the product should not be disposed of with general waste. It is your responsibility to dispose of your waste equipment by handing it over to a designated recycling collection point. The correct disposal of your end-of-life equipment will help prevent potential negative consequences to the environment and human health.

In accordance with the European Union (EU) WEEE Directive, Haivision products that fall within the scope of the WEEE, are labeled with the above symbol, and customers are encouraged to responsibly recycle their equipment at the time of disposal. Haivision also offers its customers the option of returning Haivision equipment to facilitate its environmentally sound disposal.

For more information, please visit our website at: http://www.haivision.com/environment

Table of Contents

Chapter 5: System Administration and Security

Chapter 6: Configuring A/V Services Using SNMP

About This Guide

Welcome to the User's Guide for the Makito™ X Decoder Family, Version 2.1. This user's guide describes how to install, configure, and manage the Makito X decoder to receive audio, video, and data over an Ethernet-based IP network.

To access the online help, open the web interface and click Help from the menu bar.

Topics In This Section

About Haivision

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

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

Audience

This user's guide is directed towards qualified service personnel such as technicians and network system administrators who have a basic knowledge of telecommunications equipment, and IP and LAN networking concepts and terminology.

Reliability of Information

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

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

Haivision
4445 Garand
Montréal, Québec, H4R 2H9 Canada

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

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

Obtaining Documentation

You may download the latest software, Release Notes, Getting Started Guide, and other relevant documentation from our Download Center at: https://support.haivision.com

NOTE All customers may access the Download Center; however, a login is required. If you do not have a login, select the link to create an account.

Related Documents

In addition to this user's guide, the following documents are also available through Haivision's Download Center (see link above):

- Makito X Decoder Important Notice
- Makito X Decoder Getting Started Guide
- Makito X Harsh Decoder Important Notice
- Makito X Harsh Decoder Installation Guide
- Makito X Harsh Important Notice
- Makito X Harsh Installation Guide
- Makito XR (Ruggedized) Important Notice
- Makito XR (Ruggedized) Installation Guide
- Makito X User's Guide
- SRT Deployment Guide
- Makito X Hardening Guide

Service Support

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

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

Document Conventions

The following document conventions are used throughout this user's guide.

TIP The light bulb symbol highlights suggestions or helpful hints.

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

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

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

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

Safety Information

The CAUTION and WARNING notices shown above are not only preventative measures designed to uphold the safety of both the service engineer and operator, but also enhance equipment reliability.

The definitions and symbols for CAUTION and WARNING comply with ANSI Z535.2, American National Standard for Environmental and Facility Safety Signs, and ANSI Z535.4, Product Safety Signs and Labels, issued by the American National Standards Institute.

New Product Features

Version 2.1 of the Makito X introduces the following new features and enhancements:

Dual Channel HEVC Support

Dual Channel HEVC decoding is now supported. The Dual channel HEVC decoder (#S/B-292D-HD2-HEVC) is now supported with a total aggregate decoding capability of 2 x 1080p30 video when decoding dual input streams.

HEVC SD TV Resolution Support

The HEVC decoder now supports SD (480i and 576i) resolutions.

KLV Metadata and HEVC Support

KLV Metadata is now supported and inserted into the SDI VANC when an HEVC stream is decoded.

CC, TC and AFD Support for HEVC Streams

Closed Captions, SMPTE 12M ATC_VITC timecodes and AFD metadata are all supported and inserted into the SDI VANC when an HEVC stream is decoded.

Automatic Mode Improvements

Automatic mode now supports more stream types such as SRT, VF-FEC, MPEG-PRO FEC and shaped streams.

RTSP Stream Ingest

RTSP stream ingest support is now available as a preview feature improving interoperability with Makito Classic Encoders and Axis Cameras/Encoders.

CHAPTER 1: Introduction

This chapter provides a brief overview of Haivision's Makito X decoder, along with a description of the main hardware components and key features.

Topics In This Chapter

Product Overview

The Makito X Decoder Family is a series of IP video appliances designed to be paired with the Makito X Encoder Family. The Makito X decoder can be configured to decode video from a Haivision encoder (Makito X, Makito "Classic", or Hai1000/Piranha) or a third party compatible encoder. The Makito X decoder delivers single or dual-channel HD digital video to 3G-SDI and HDMI interfaces.

The Makito X decoder supports H.264 High Profile video sources and delivers HD digital video with embedded digital and separate (balanced and unbalanced) analog audio output. The HEVC-capable variant supports decoding of a single or dual stream containing High Efficiency Video Coding (HEVC/H.265) compressed video content. When paired with the Makito X HEVC encoder, the Makito X HEVC decoder yields up to 1080p60 video from a HEVC or H.264 stream with extremely low end-to-end latency.

The Makito X decoder is available as a compact standalone appliance or as mini-blades within rack mountable chassis. It can be configured to decode up to 12 channels within a single rack unit.

Figure 1-1 Front View (Single Height Chassis)

Both SDI and HDMI output interfaces support many common SD, HD and 3G-SDI TV resolutions. The HDMI output interface also supports the decoding and display of computer graphics resolutions.

NOTE In this guide, "SDI" refers to any of the SD, HD and 3G variants. The actual standard used by the decoder is determined by the resolution and frame rate of the received video stream.

The Makito X decoder is a general purpose decoder capable of decoding many stream formats generated by Haivision and third party encoders. It accepts streams that are remotely generated and de-encapsulates them depending on the stream format.

- MPEG-2 TS/UDP (with optional Furnace-compatible FEC)
- MPEG-2 TS/RTP (as described in RFC 2250) with optional Pro-MPEG compatible FEC
- SRT (Haivision's Secure Reliable Transport) technology. SRT optimizes video streaming performance across unpredictable Internet networks, recovering from packet loss, jitter, network congestion and bandwidth fluctuations that can severely affect the viewing experience.

The Makito X decoder supports decoding Baseline, Main and High Profile H.264 4:2:0 coded elementary stream NALs which use B frames (I, IP, IBP and IBBP GOP structures), Intra-Refresh, VBR or CBR rate control, intra-partitioning, CABAC or CAVLC entropy coding, and GOP sizes ranging from 1 to 1000.

The Makito X decoder's implementation of the Advanced Encryption Standard (AES) protocol delivers video content securely and ensures high quality even on congested or unreliable networks. The Makito X decoder provides recovery from packet loss with forward error correction (FEC) and an adjustable receive buffer to tune its performance in varying networks.

Makito X Decoder Features

Makito X decoder features and benefits include the following:

- General decoder features:
  - Unicast/Multicast Stream support
  - Still image insertion on loss of video stream
  - Output interface frame rate or resolution control for display matching for HDMI
  - A/V Sync Modes for clock recovery
  - Output Delay Buffer (0-1000 ms) Selection
  - KLV / SDI insertion (Licensable) (H.264 and HEVC)
  - CEA-708-B Closed Caption / SDI insertion with line control
  - AFD / SDI insertion with line control
  - SMPTE 12M ATC_VITC timecode / SDI insertion with insertion line control
  - Intra-Partitioning (supporting 8x8 and 4x4 MB partitioning tools)
  - Intra-Refresh support
- High Efficiency Video Coding (HEVC/H.265) decoding of a single or dual stream:
  - Only available on HEVC-capable dual-height Makito X decoder
  - Supports interlaced or progressive streams and resolutions up to one channel of 1080p60 or two channels of 1080p30
  - Stream type is automatically determined on decoder startup
- Multi-Track audio support (to inter-work with Makito X encoder v1.1 and later)
  - Up to eight audio decoders supported
  - MPEG-2 AAC-LC (ADTS) support
- Support for two video decoders feeding two different SDI interfaces up to 1080p60
- Ability to select which video stream is displayed on the HDMI interface up to 1920x1200p60 resolution

- Visual notifications displayed on systems with unsaved configurations at login, logout, or reboot to warn users to save their current configuration as a preset
- Supports the administrative features required to comply with the Common Criteria NDPP v1.1
- Secure Reliable Transport (SRT) Streaming support
- Field licensing of the video decoder instances, SRT and KLV

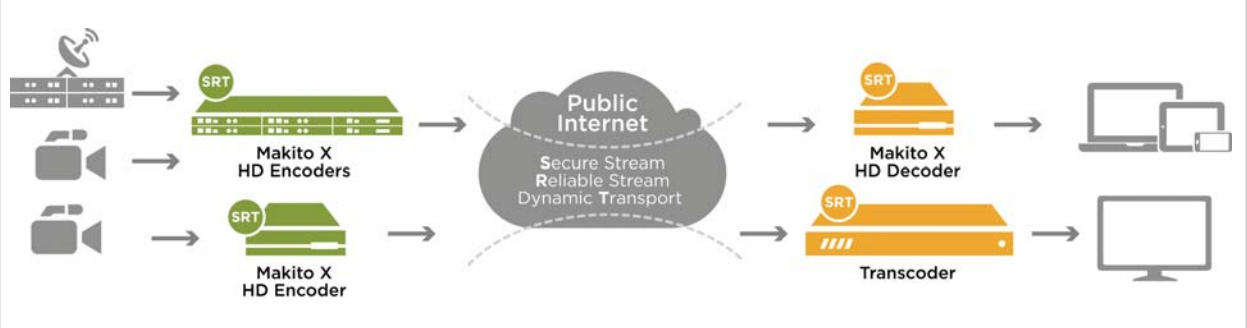
NOTE Both SRT and KLV are licensed features; however, the SRT and KLV licenses are currently included at no extra cost with each Makito X decoder purchased.

Secure Reliable Transport (SRT)

Haivision's Secure Reliable Transport (SRT) technology is available on Makito X Series encoders and decoders. The SRT streaming protocol is designed to provide reliable and secure end-to-end transport between two SRT-enabled devices over a link which traverses the public Internet. SRT optimizes video streaming performance across unpredictable Internet networks, recovering from packet loss, jitter, network congestion and bandwidth fluctuations that can severely affect the viewing experience.

SRT is applied to contribution and distribution endpoints as part of a video stream workflow. After encoding (or transcoding), SRT applies encryption and provides error recovery. Prior to decoding (or transcoding), SRT decrypts the stream and enables recovery from packet loss typical of Internet connections. At the same time, SRT detects the real-time network performance between the encode / decode / transcode endpoints. The endpoints can be dynamically adjusted for optimal stream performance and quality.

Figure 1-2 Makito X SRT Workflow



For information required to set up and tune SRT streams from the encoder to the decoder, please see the SRT Deployment Guide (available through Haivision's Download Center at: https://support.haivision.com.

Single/Dual Channel Variants

The dual-height Makito X decoder (shown following) supports decoding of a single or dual stream containing AVC/H.264 or High Efficiency Video Coding (HEVC/H.265) compressed video content.

On the dual-channel Makito X decoder, one or two streams may be actively decoded at any given time. Each video decoder is independent. The configuration of one does not affect the other video decoder.

The Makito X decoder is also available in a single channel variant allowing mirroring of the decoded stream to all interfaces and supporting up to eight (8) channel pairs of AAC-LC audio decoding for a stream.

Figure 1-3 Front View (Dual Height Chassis)

Figure 1-4 Rear View (Dual Height Chassis, H.264 and HEVC, #S-292D-HD1-HEVC)

The Makito X decoder channel variants are as follows:

- H.264-only single or dual channel (single-height blade/appliance)
- H.264 and HEVC single or dual channel (dual-height blade/appliance)

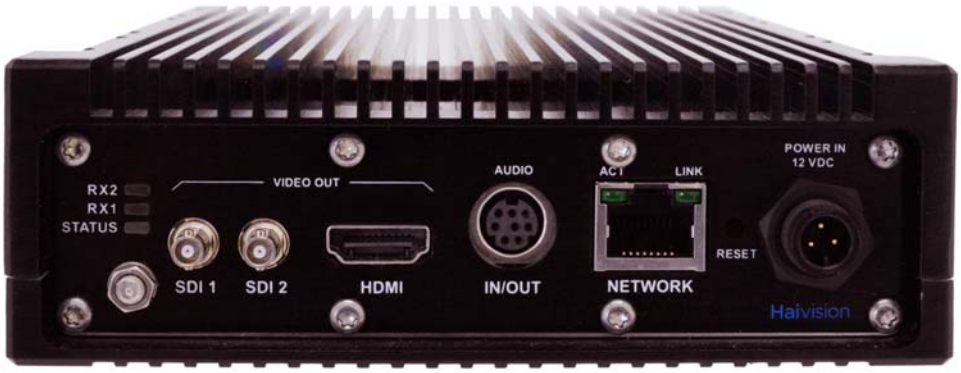
Chassis Styles

The Makito X decoder is available in the following chassis styles:

- as an ultra-compact appliance (single-height or dual-height) for single or dual-channel decoding (Figure 1-5 shows the single-height chassis, while Figures 1-3 and 1-4 show the dual-height chassis),
- the Makito X "Harsh" semi-ruggedized, industrial SDI decoder appliance (H.264-only, shown in Figure 1-6).
- as a blade within a 1RU chassis (MB6X) that can contain up to six single-height or three dual-height Haivision encoder/decoder blades (shown in Figure 1-7),
- as a blade within a 4RU chassis (MB21) that can contain up to 21 single-height or ten dual-height Haivision encoder/decoder blades (Figure 1-8),

Figure 1-5 Front and Rear Views (Single Height Chassis, H.264, #S-292D-HD2)

Figure 1-6 Makito X Harsh Environment (Dual H.264 Decoder Appliance)



NOTE For instructions on installing the Makito X Harsh decoder, please refer to the Makito X Harsh Decoder Installation Guide, available through Haivision's Download Center.

Figure 1-7 MB6X Multichannel Chassis (Front and Rear Views, #F-MB6X-MED)

NOTE The MB6X is available with a single AC, DC, or medical grade AC power supply.

For instructions on installing the MB6 or MB21 chassis, please refer to the MB6 and MB21 Multichannel Chassis Installation Guide, available through Haivision's Download Center.

Figure 1-8 MB21 Multichannel Chassis (Front and Rear Views, #F-MB21B-R)

Applications

Typical examples of Makito X decoder applications include:

- General low-latency decoding over an enterprise class network - The Makito X decoder is used as a point-to-point device paired with a Makito X encoder. Video is captured live at a the encoder and transmitted over an enterprise class network to the decoder. Low latency and image quality are primary drivers for this application. Use cases include broadcast backhaul, FED range video transport, Medical intra-room video transport, and intra-stadium video transport (using multicast stream tuning).
- Over a fixed link between remote sites - When two different locations are connected with a dedicated link, the Makito X encoders and decoders can be used to transport audio, video and metadata content between the different sites.

- Over the public Internet streaming using SRT - The Makito X decoder is used as an Internet streaming solution to transport content over the public Internet using the SRT streaming technology. Configuration is point-to-point between two locations geographically distant and passing through a firewall. Firewall ports must be manually opened to allow traffic through.

Physical Description

Following is a description of the Makito X decoder (single chassis) interfaces, connectors, and LED status indicators:

System Interfaces (Rear Panel)

The Makito X decoder comes with a 10/100/1000 Base-T Ethernet Network interface for both traffic and management (RJ45).

Figure 1-9 Ethernet Connection

Related Topics

- "Connecting the Decoder to the Network and a Computer" on page 37

Audio/Video Interfaces (Rear Panel)

NOTE The Makito X decoder supports one or two independent video decoders that feed the two SDI interfaces. On the single channel variants, the second mini-BNC is used only to mirror the single channel output.

The HDMI port can be configured to mirror the same content that is seen on either Decoder 1 or Decoder 2. If the stream contains computer graphics resolutions, that content can only be displayed on the HDMI interface.

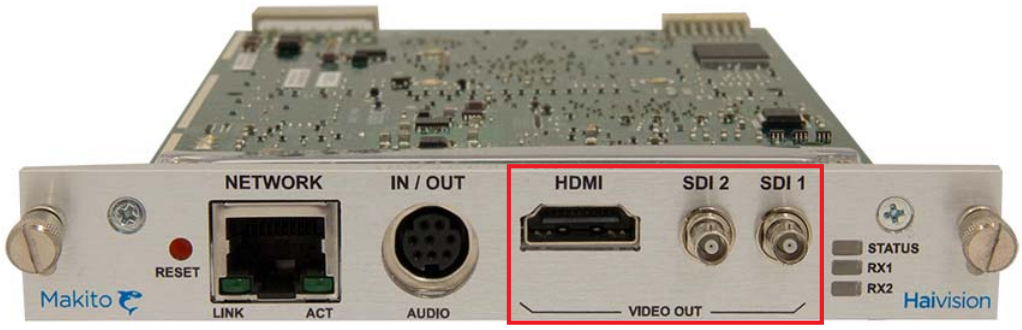
All of the decoder's Video Output connectors are active, and *both* Analog Audio and Embedded Digital Audio are active. This means that the decoder is capable of simultaneously outputting analog and digital audio as well as both SDI and HDMI digital video.

Video and Embedded Digital Audio Output Interfaces

The Makito X decoder video interface consists of two BNC connectors (SDI 1 and SDI 2) and one HDMI connector (faceplate shown below).

- The BNC connectors are used for the SD/HD/3G-SDI video signals. A 75Ω coaxial cable connects from Video Out to a video monitor. HD-BNC to BNC Adapter Cable(s) are included in the package.
- The HDMI connector is used for High Definition audio/video output signals. An HDMI Type-A cable connects from HDMI Out to a video monitor. Note that HDCP content protection is not applied to the HDMI output.

Figure 1-10 Video Output Connections



The audio is also embedded in the SDI and HDMI video. The SDI video supports up to 16 audio channels (8 pairs) and the HDMI supports 8 channels (4 pairs).

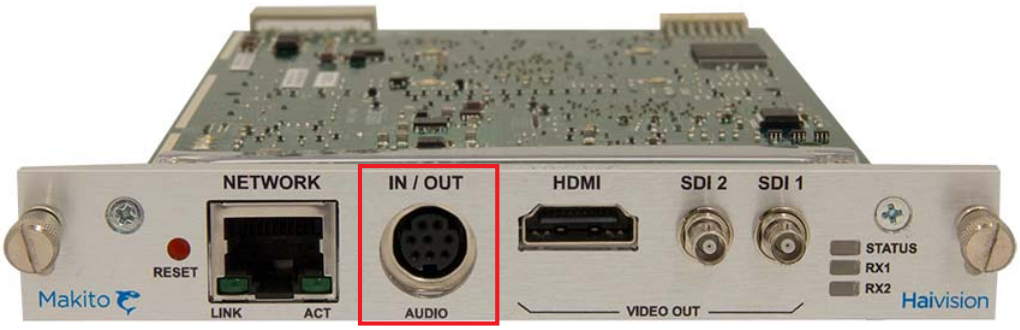
Related Topics

- "Connecting the Decoder to A/V Displays" on page 38

Analog Audio Interface

The Makito X decoder analog audio interface consists of a single 8-pin Mini-DIN connector used for two-channel balanced/unbalanced analog audio output (one stereo pair) and a mono audio input (for Audio Talkback).

Figure 1-11 Analog Audio Interface



For the pinout, see "Audio Connector Pinout" on page 41.

An adapter is required to interface with the audio port. An RCA cable adapter for unbalanced audio is included in the package. An adapter for balanced audio may be ordered from Haivision. For details, see "Audio Breakout Cables" on page 44.

Related Topics

- "Connecting the Decoder to A/V Displays" on page 38
- "Audio Talkback" on page 32

LED Status Indicators (Rear Panel)

The LED colors and flashing (blinking) speed indicate the status (operational state) of the Makito X decoder.

Figure 1-12 LED Status Indicators

Function	Color	Description	Indication
STATUS	RED/ GREEN	OFF	No power
		RED Solid	Error / Fault
		GREEN Blinking	Booting / Initialization
		GREEN Solid	No Fault / OK
RX1 and RX2	AMBER/ GREEN	OFF	No active stream is being decoded
		AMBER Solid	At least one of the conditions below is sufficient to turn on the LED AMBER: • Decoder booting • NO video stream is being decoded • NO audio stream is being decoded
		GREEN Solid	When ALL the conditions below are met: • A video stream is being decoded • An audio stream is being decoded
Network port			
LINK	GREEN	OFF	Not Connected
		GREEN Blinking once per second	Connected at 10 Mbps
		GREEN Blinking twice per second	Connected at 100 Mbps
		GREEN Blinking three times per second	Connected at 1000 Mbps

Function	Color	Description	Indication
ACT	GREEN	OFF	No Activity
		GREEN Intermittent	Little activity (e.g., management). The LED should be lit when there is activity
		GREEN Solid	Intense Activity (e.g., transmitting video traffic)

Related Topics

- "Powering Up the Unit" on page 46

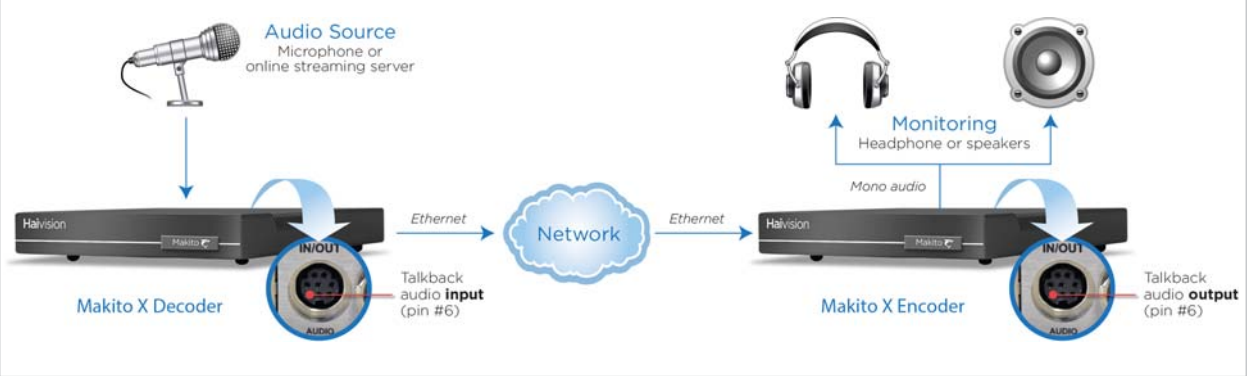
Audio Talkback

The Audio Talkback network service allows users to stream a mono channel of audio back to a Makito X encoder over a reliable LAN or WAN. Audio talkback uses the decoder's audio input to enable end users monitoring a streaming session to "talk back" to individuals at the encoder. For example, talkback enables students at remote classroom locations to ask their teacher questions, or a chief surgeon observing a surgery to collaborate.

The talkback audio stream is input via a microphone connected to the decoder's 8-pin Mini-DIN connector (see "Analog Audio Interface" on page 29).

The following picture illustrates a sample signal path from the audio source through the Makito X's audio input when using the talkback feature.

Figure 1-13 Audio Talkback Signal Path



Administrators can enable or disable audio talkback on the decoder and specify the UDP port to transmit (i.e., the destination port used by the encoder). They can also select the talkback activation mode (either Push Button or Toggle Switch) from the Web interface.

- Push Button provides "push-to-talk" functionality, which requires that the user push a button to transmit audio. The user must keep pushing the button to use the talkback channel.
- The Toggle Switch stays active until the user clicks the button again.

The Talkback network service may be enabled and disabled from the Web interface (Services page, see "Enabling and Disabling Network Services" on page 120) or using the service command (see "service" on page 216).

NOTE For Talkback to start automatically when the unit is rebooted, a default preset should be created while talkback is active and the button mode is set to Toggle Switch.

Once the Talkback service is enabled, a user simply selects the stream and presses the Talkback button from the Web Interface (Streams page) to start streaming the audio from

the microphone to the encoder of that stream. For details, see "Starting and Stopping Audio Talkback" on page 76.

CLI commands may be used to start or stop transmission of talkback audio, specify the talkback port, clear talkback statistics, and display talkback information. For details, see "talkback" on page 225 (CLI). Talkback audio is not configurable through SNMP.

The audio is only sent to the source video encoder; it is not distributed to other viewers of the stream.

NOTE Audio talkback is uncompressed audio (using approximately 350 kbps of network bandwidth).

Related Topics

- "Enabling and Disabling Network Services" on page 120
- "service" on page 216

Hardening

Hardening is a term used to describe the process of securing a networked device's various interfaces. This includes removing or limiting certain features to prevent their abuse, and securing the data hosted by the device.

The Makito X decoder includes features that allow the administrative interface to be secured.

These features are described in detail in the Makito X Hardening Guide, available from Haivision's Download Center at: https://support.haivision.com.

NOTE Any Makito X at Version 1.2 or higher can be hardened by following the procedures described in this guide.

The Makito X Hardening Guide provides the procedures to install and configure Makito Xs to be hardened. This guide is written for administrators and assumes that the reader is familiar with networks and network terminology. No encoder-specific knowledge is required. This guide also assumes that the reader is a trusted individual.

CHAPTER 2: Installing the Decoder

This chapter explains how to set up and connect the Makito X decoder. It also includes the instructions for factory reset.

NOTE For instructions on installing the Makito X Harsh decoder, please refer to the Makito X Harsh Decoder Installation Guide.

For the steps to install the MB6 or MB21 chassis, please refer to the MB6 and MB21 Multichannel Chassis Installation Guide.

Both guides are available through Haivision's Download Center.

Topics In This Chapter

Setting Up the Decoder

Always read the instructions carefully and keep this user's guide for future reference.

Please choose a suitable location for operating the decoder(s). By doing so you will preserve long lifesaving and stability of the unit(s).

Set up the decoder on a reliable and flat surface when using the single Makito X chassis, or mount in a rack, when using the 1U or 4U chassis.

Safety First

Please pay particular attention to the following points in order to help protect yourself and the decoder:

- Refer to "Safety Guidelines" on page 5.
- The Makito X decoder is an indoor appliance and should be kept in a dry, dust free environment.
- There are no user-serviceable parts inside the unit. Making unauthorized changes will void the warranty.
- Only connect the unit to a compatible power source.
- If an electrical fault occurs, disconnect the unit and contact Haivision Technical Support.
- Never try to force the connections when setting up the system as this may damage the unit.

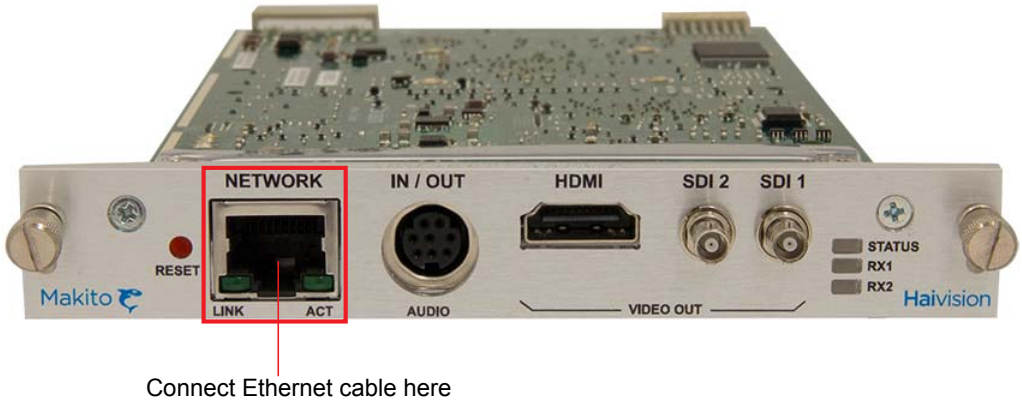
Connecting the Decoder to the Network and a Computer

To connect the Network Interface:

1. Connect the Ethernet port to the IP network using an Ethernet UTP cable (Type Cat 5 or higher).

   This will allow you to telnet to the unit or connect via the Web interface.

Figure 2-1 Network Connector



Connecting the Decoder to A/V Displays

NOTE The Makito X decoder supports two independent video decoders that feed the two SDI interfaces. The HDMI port can be configured to mirror the same content that is seen on either Decoder 1 or Decoder 2. If the stream contains computer graphics content, that content can only be displayed on the HDMI interface.

All of the decoder's Video Output connectors are active, and *both* Analog Audio and Embedded Digital Audio are active. This means that the decoder is capable of simultaneously outputting analog and digital audio as well as both SDI and HDMI digital video.

To connect the Decoder to A/V Displays:

1. 3G-SDI Video Output with Embedded Audio:
   Connect one or both of the decoder's SDI outputs to TV or display monitors, using the HD-BNC to BNC Adapter Cable(s) (included in the package for appliances).

Figure 2-2 Decoder A/V Output Connectors

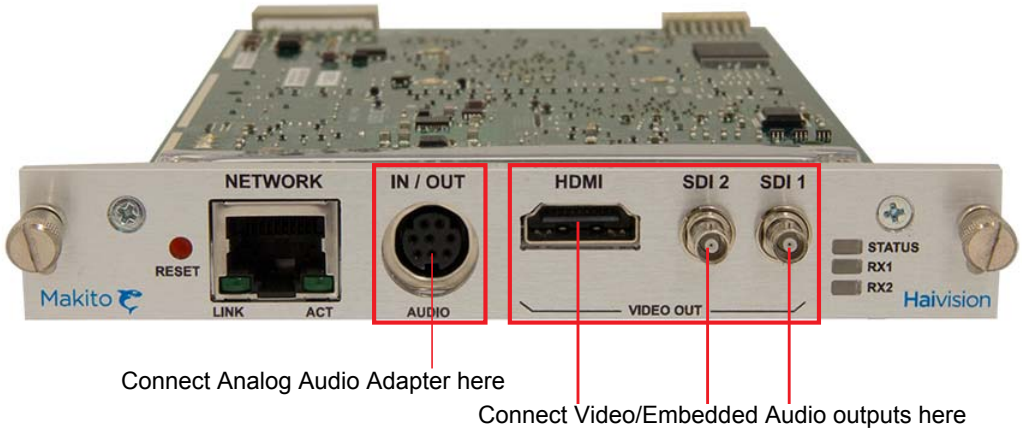


Figure 2-3 HD-BNC to BNC Adapter Cable

NOTE To install blades in an MB6X or MB21 chassis, see "HD-BNC Connector Assembly" on page 44 to mount the HD-BNC connector directly on the cable run.

All blades manufactured by Haivision are can be installed and removed with the chassis powered on (i.e., are hot-swap capable).

2. HDMI Video Output with Embedded Audio:
   Connect the decoder's HDMI output to a TV or display monitor, using the HDMI connector (shown in Figure 2-2).

   Refer to Figure 2-5 on page 40 for the HDMI Connector Pinout.

NOTE By default, HDMI displays the SDI 1 content. To monitor the SDI 2 channel, see "Configuring the HDMI Display" on page 98.

3. Analog Audio Out: Connect the decoder's audio output to the audio sound system/speakers, using the audio 8-pin Mini-DIN connector (shown in Figure 2-2).
   - For unbalanced audio, use the 8-pin audio to 3-RCA female cable adapter (included in the package, shown in Figure 2-4).
   - A balanced audio cable adapter is available from Haivision upon request. (See "Audio Breakout Cables" on page 44.)

Figure 2-4 Audio to RCA Female Cable Adapter (Unbalanced)

White - Channel 1 / Left Out
Red - Channel 2 / Right Out
Black - Talkback In (future use)

Refer to "Audio Connector Pinout" on page 41 for the balanced/unbalanced audio pinout.

NOTE Selection between analog and digital (SDI) audio may be done via the Web interface or the Command Line Interface (CLI).

To configure the decoders, see "Managing the Decoder" on page 69 (Web interface), or "CLI Command Reference" on page 169 (CLI).

HDMI Audio/Video Output Connector Pinout

The Type A 19-pin HDMI audio/video output connector has the following pinout:

Figure 2-5 HDMI Connector Pinout

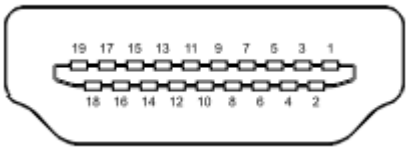


Table 2-1 HDMI Connector Pinout

HDMI Pin #	Description
1	TMDS Data2+
2	TMDS Data2 Shield
3	TMDS Data2–
4	TMDS Data1+
5	TMDS Data1 Shield
6	TMDS Data1–
7	TMDS Data0+
8	TMDS Data0 Shield
9	TMDS Data0–
10	TMDS Clock+
11	TMDS Clock Shield
12	TMDS Clock–
13	Reserved (N.C. on device)
15	SCL
16	SDA
17	DDC/CEC Ground
18	+5 V Power
19	Hot Plug Detect

Audio Connector Pinout

The mini-DIN-8 analog audio connector has the following pinout:

Figure 2-6 Mini-DIN-8 Audio Connector Pinout (Front View)

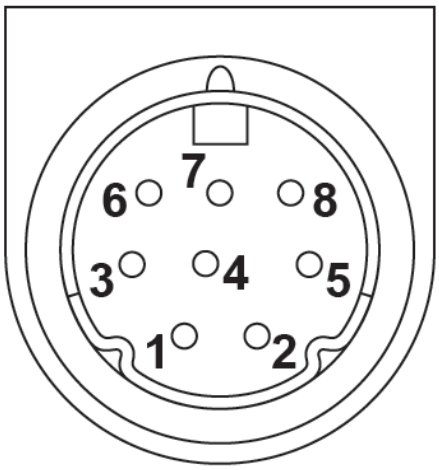


Table 2-2 Mini-DIN-8 Audio Connector Pinout

Pin #	Description
1	Reserved / Not Connected
2	Reserved / Not Connected
3	Reserved / Not Connected
4	Channel 2 / Right Negative Signal
5	Channel 1 / Left Negative Signal
6	Talkback Positive Signal
7	Channel 2 / Right Positive Signal
8	Channel 1 / Left Positive Signal

Unbalanced and Balanced Audio Connection Details

Figure 2-7 Unbalanced Audio Connection Details

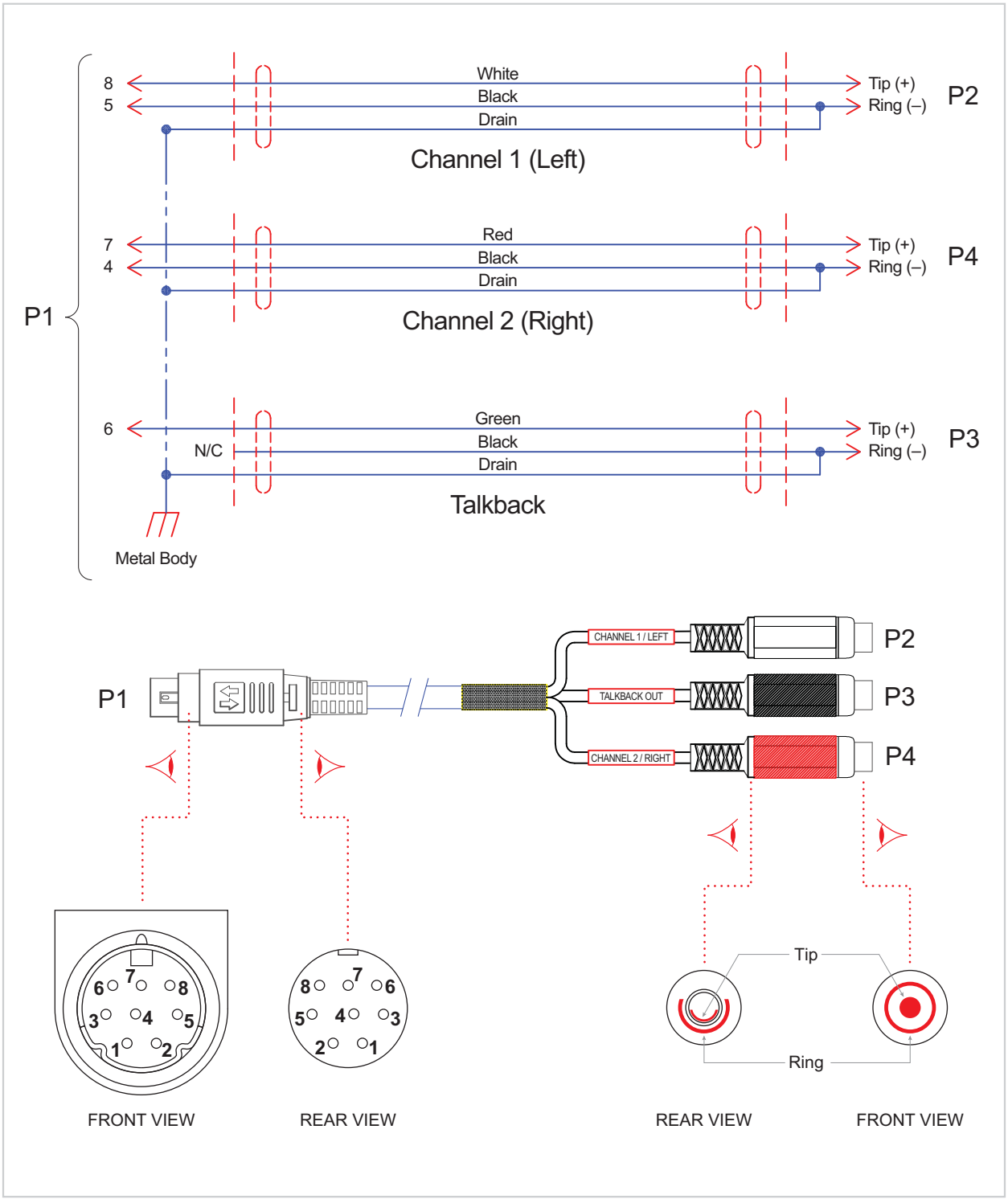
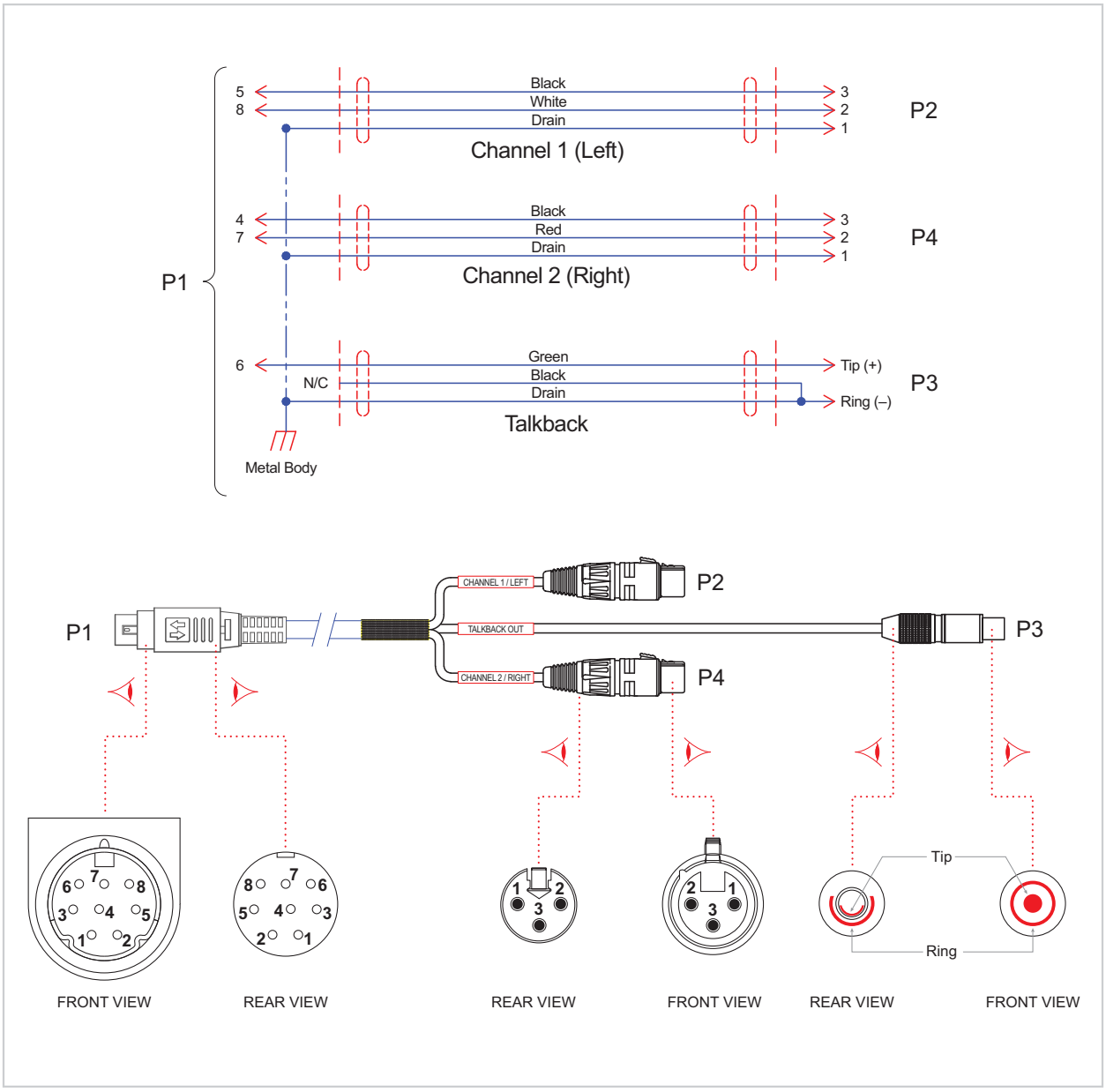


Figure 2-8 Balanced Audio Connection Details



Related Topics

- For more information on the audio connections, see "Audio/Video Interfaces (Rear Panel)" on page 28.

Audio Breakout Cables

The following table list the audio breakout cables available for the Makito X decoder, including description and Haivision part numbers.

Table 2-3 Audio Breakout Cables for the Makito X decoder

Cable	Description	Part Number
Makito X decoder Series Audio Breakout Cable, Unbalanced	Unbalanced mini-DIN 8 to RCA Female • 2 channels output • 1 channel input for talkback support (future use) Included in the package (shown in Figure 2-4 on page 39).	CA-292-2RTB
Makito X decoder Series Audio Breakout Cable, Balanced	Balanced mini-DIN 8 to XLR Female • 2 channels output • 1 RCA female channel input for talkback support (future use) May be ordered from Haivision. Please contact your sales representative or email Haivision at: sales@haivision.com	CA-292-2XFTB
Makito X decoder Series Audio Breakout Cable, Balanced	Balanced mini-DIN 8 to XLR Male • 2 channels output • 1 RCA female channel input for talkback support (future use) May be ordered from Haivision. Please contact your sales representative or email Haivision at: sales@haivision.com	CA-292-2XMTB

HD-BNC Connector Assembly

Although the HD-BNC to BNC adapter cables are provided with Makito X blades, for long cable runs, we recommend that you mount the HD-BNC connector directly on the cable (instead of using a converter) to enhance signal levels.

The vendor and ordering part-number for an HD-BNC extractor/mating tool is as follows: Amphenol p/n 227-T2000

The HD-BNC plug can be mounted on many 75 Ohm coaxial cables. Following are the most popular coaxial cables from Belden following by the HD-BNC connector part number recommended by Amphenol.

Description	Part Number
Plug for Belden Cable 1855A	Amphenol 34-1026
Plug for Belden Cable 1505A	Amphenol 34-1025
Plug for Belden Cable 1695A	Amphenol 34-1027
Plug for Belden Cable 1694A	Amphenol 34-1017-300

Powering Up the Unit

Once all the cables are in place, the decoder is ready to be powered up.

Single-Height or Double-Height Chassis

Figure 2-9 Rear Panel (Single-Height Chassis #S/B-292D-HD2) showing Locking Power Connector

Connect power supply here (Power Input jack)

Figure 2-10 Single-Height Chassis Power Adapter 12VDC with 3-pin Connector

Conxall 3-pin Connector (power supply)

Figure 2-11 Rear Panel (Dual-Height Chassis, with Dual-Channel HEVC #S/B-292D-HD2-HEVC)

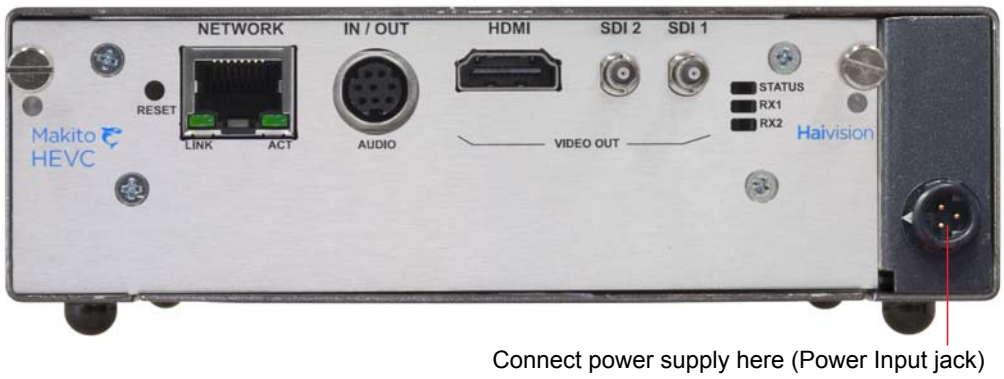


Figure 2-12 Dual-Height Chassis Power Adapter 12VDC with 3-pin Connector

NOTE There is no power switch on the Makito X appliance. The power is automatically on when the unit is plugged in. The power supply cord is used as the main disconnect device.

Ensure that the AC power outlet is located near the equipment and is easily accessible.

To power up the Single-Height or Double-Height Chassis:

1. Insert the 3-pin connector on the 12V power supply into the Power input jack at the rear of the decoder.

CAUTION To prevent damage to the decoder and/or power supply, be sure to connect the power supply to the chassis *first* and then to the AC source.

Always use the AC power cord and power supply provided with the unit. The single and dual-height chassis have different power supply units and chassis connectors.

Make sure the connector is properly inserted and locked to avoid intermittent power problems.

2. Connect the power cord to the power supply and plug the cord into an AC power source.

   The Status LED will start blinking green, indicating that the decoder is booting up.

3. Wait until the Status LED stays solid green, indicating that the decoder is ready for operation.

To begin configuring the decoder, you can either open the Web interface, or log in to the CLI.

- To use the Web interface, see "Logging In to the Web Interface" on page 61.
- To enter CLI commands, see "CLI Command Reference" on page 169.

Resetting the Decoder

This section describes the procedures to perform either a Power Reset or Factory Reset.

- A Power Reset is equivalent to simply powering the unit off and on.
- A Factory Reset powers the unit off and on, and returns the decoder to the same settings it originally had when shipped from Haivision, including the factory default IP address, subnet, and gateway.

  After a Factory reset, only the firmware revision, serial number, and MAC address are preserved. All other data is deleted (including saved configurations, modified passwords, and decoding settings), and all settings are returned to their factory preset conditions (including the IP address).

To reset the decoder:

1. With the decoder on, insert a small plastic tool into the small opening labeled Reset on the decoder faceplate.

Figure 2-13 Reset micro switch

Power Reset

2. For a power reset, press the micro switch (you will feel the button depress) for at least one second and release. Be sure to release the button in less than 5 seconds.

   This resets the unit.

Factory Reset

3. To reset the decoder to its factory default settings, press the micro switch (you will feel the button depress) and hold for five (5) seconds.

   The decoder will reboot on its own. As soon as the lights stop blinking and the Status LED is solid green, the decoder is ready.

Default Network Settings

After a factory reset, the Network settings are reset to:

IP Address	Subnet Mask	Gateway
10.5.1.2	255.255.0.0	10.5.0.1

Hardware Maintenance

The following maintenance tasks are recommended for the Makito X decoder appliance.

Cleaning the Ventilation (Intake/Outtake)

To clean the intake and outtake vents, use a dry cloth or an aspiration device approved for electronic equipment.

Maintenance should be done every 6 months (more often in a dusty environment).

Monitoring of the Fan Operation

There is no system level monitoring of the fan operation. However, it is recommended that you check to see if the fan is operating in one of two ways:

- If the appliance is easily accessible, turn the unit over and listen (an operational fan makes a humming noise).
- Use the CLI (`temperature get` command) to get information from the built-in temperature sensors (see "temperature" on page 228). If the internal temperature of the unit is rising, that is an indication that the fan may not be operating properly.

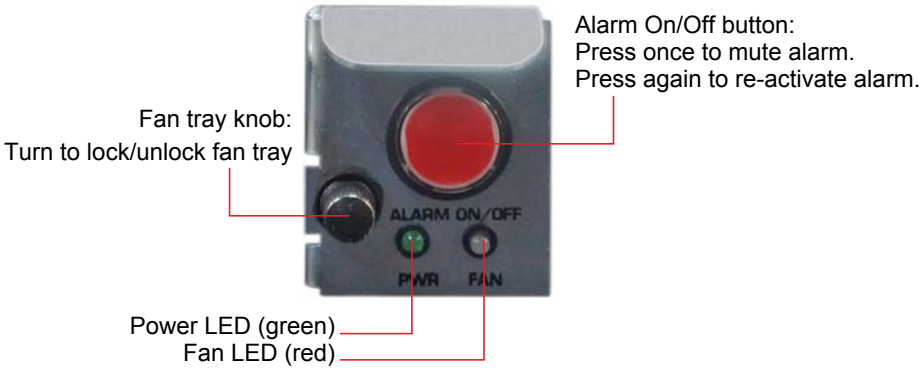
Replacing the MB6X Chassis Fan Tray

Some MB6X chassis models have a removable fan tray, located on the far right side of the chassis. The fan tray may be removed from the front of the chassis. This procedure applies to those units supporting field swappable fan trays.

NOTE You can replace the fan tray without powering off the Makito X decoder, which allows you to perform this maintenance procedure without stopping the decoder service.

However, do so only if you are able to replace the fan tray within five minutes. Otherwise, we recommend that you power off the unit before replacing a fan tray.

Figure 2-14 MB6X Removable Fan Tray (close-up view, Chassis Front)



To replace the MB6X Chassis fan tray:

1. Turn the fan tray knob clockwise to unlock the fan tray.
2. Remove the fan tray by pulling it away from the chassis.
3. Insert a new fan tray in the slot and slide it all the way into the chassis. (This will apply Power to the fan tray.)
4. Turn the fan tray knob counterclockwise to lock the fan tray into the slot.

Replacement fan trays are available from Haivision. Please contact your sales representative or email Haivision at: sales@haivision.com

Replacing the RTC Battery

The Makito X decoder appliance contains a real-time clock (RTC) powered by the following battery:

- Varta CR2032 with 2-wire connector Mfr. Part#: 06032101030

At the end of its life (7-10 years), the battery should be replaced by the end user with the same battery or an equivalent model approved by Haivision.

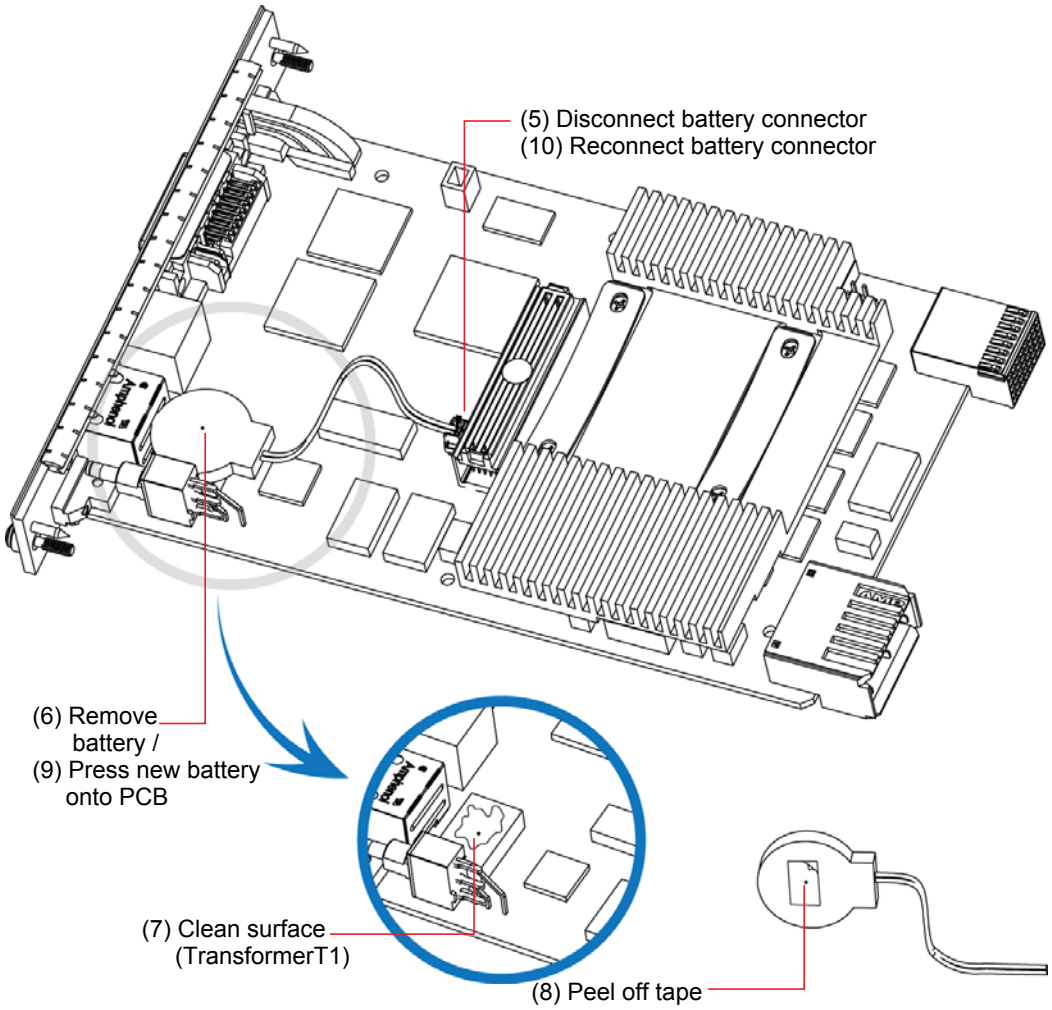
NOTE The used battery should be disposed of and recycled in accordance with your national/local battery collection schemes.

To replace the RTC battery:

1. Disconnect all external devices connected to the appliance.
2. Disconnect the power from the appliance by unplugging the power cord from the AC outlet.
3. To open the chassis, unfasten and remove the two screws on the rear of the appliance.

4. Slide the PCB board out of the chassis.
5. Disconnect the battery connector by pulling it upward from the PCB.

Figure 2-15 RTC Battery Removal and Installation



6. Remove the battery by pulling it upward from the PCB.
7. Clean the surface of transformer T1 with alcohol if there is glue residue.
8. Peel off the protective layer on the tape on the new battery.
9. Press the new battery onto the PCB (top of transformer T1) with a force of 3 pounds-force per square inch for three (3) seconds.
10. Reconnect the battery connector.
11. Reassemble the chassis, reconnect any external devices to the appliance, and reconnect the power to the appliance.

CHAPTER 3: Getting Started with the Web Interface

This chapter begins with a management overview of the Makito X decoder, followed by system access control information.

NOTE Before proceeding, make sure that the decoder is set up correctly and all necessary network and A/V connections are established. See Chapter 2: “Installing the Decoder”.

Topics In This Chapter

Management Overview

NOTE Most Audio/Video settings are defined at the encoder end, and the decoder adjusts to the settings embedded in the received stream.

All Makito X decoder interfaces and applications such as Audio/Video services and IP links may be configured, managed, and monitored through the Web Interface, the Command Line Interface (CLI), or an SNMP server. All methods require access to the decoder through its Ethernet LAN port.

Using the Web Interface

Managing the Makito X decoder from the Web interface requires a connection from the unit's LAN port to your network. You must then connect a computer with a Web browser to the network to access the Web interface.

The remainder of this chapter provides information on how to configure and manage the decoder from the Web interface.

Using the CLI

Management via the CLI is possible through a telnet session or SSH.

For a list and description of the CLI commands to configure and manage the Makito X decoder, see Appendix A: "CLI Command Reference".

SNMP-based Management

(Simple Network Management Protocol) SNMP-based management uses Network Management Stations (NMSs) to collect data or configure devices (SNMP agents) across a TCP/IP network. The NMS communicates with the Makito X decoder through the exchange of SNMP messages.

For information on SNMP management of the Makito X decoder, see Chapter 6: "Configuring A/V Services Using SNMP".

Accessing the Decoder

Accessing the Web Interface

To access the decoder configuration Web page:

1. From your computer, open a Web browser of your choice, such as Chrome, Firefox, Safari, or Internet Explorer.

NOTE The Makito X supports the latest production versions (as of this document date) of the Chrome, Firefox, Safari, and Internet Explorer browsers. Please see the Release Notes for any limitations for specific versions of these browsers.

2. Type the decoder's IP Address in the browser's address field and press Enter (see "Default Decoder IP Address" below).
3. Log in (see "Logging In to the Web Interface" on page 61).

Security Steps

Only secured HTTP (HTTPS) is supported for the Web interface; therefore, a server certificate is required. The decoder automatically generates a self-signed certificate and your browser will recommend that you do not proceed.

If you have not changed the factory defaults on the decoder, a certificate with factory default subjects exists (DNS: haivision-ace, IP: 10.5.1.2). Proceed temporarily if you can since this default certificate will be deleted and re-generated (see below).

If you or your system administrator do not install your own certificate, a new one will be generated upon reboot the first time a non-factory IP address is detected with the configured hostname, DNS, and IP address. Accept this certificate and proceed to the Web interface.

NOTE The Makito X decoder identity certificate and trusted root certificates are managed using the CLI certificate command or Web interface Certificates page. For details, see "certificate" on page 181 or "Managing Certificates" on page 144.

Accessing the CLI

To access the decoder CLI:

1. Open a telnet session to the decoder (see "Default Decoder IP Address" below).
2. At the login prompt, type the username and password (see "Role-based Authorization" on page 59).

Default Decoder IP Address

NOTE If you haven't changed the factory presets, and if not specified elsewhere in the shipment, the decoder's IP Address is set by default to: 10.5.1.2.

To be able to log in to the Makito X decoder Web interface, your computer has to be in the same IP Address range (subnet).

You may have to temporarily change your computer's IP Address to be in the same subnet as the decoder. Only then you will be able to access the decoder and change the decoder's IP Address, and then afterwards change your computer's IP Address back.

TIP After you change the decoder IP Address, be sure to document it somewhere or label the chassis. Otherwise if you do not know the current IP Address, you will need to reset the Makito to its factory settings, which will return the unit to the default IP address (and you will lose any saved configurations and settings). For more information, see "Resetting the Decoder" on page 49.

Role-based Authorization

The Makito X decoder uses role-based authorization control to secure the Web interface and CLI. As of Version 2.1, administrators can create new accounts and thus allocate an account to each user of the system.

The Makito X decoder provides three defined account roles to assign privileges to users:

Role	Default Username	Privileges
Guest	user	Read-only access to the system.
Operator	operator	All rights to configure A/V and stream settings. Does *not* include rights to reboot or upgrade the system, modify the network settings, or manage accounts.
Administrator	admin	All access rights and Administrator privileges.

The table below summarizes role-based access to functional modules:

Functional Module	Role		
	Guest	Operator	Administrator
Operation			
Streams	Read-only	Yes	Yes
Video Decoder	Read-only	Yes	Yes
Audio Decoder	Read-only	Yes	Yes
Administration			
Network Configuration	-	-	Yes
System Status	Read-only	Yes	Yes
(Configuration) Presets	-	Yes	Yes
Firmware Upgrades	-	-	Yes
Services	-	-	Yes
Licensing	-	-	Yes
Still Images	-	-	Yes
Security			
My Account / Accounts	Yes[a]	Yes	Yes
Messages	-	-	Yes
Banner	-	-	Yes
Cryptographic Policies	-	-	Yes

Functional Module (Cont.)	Role (Cont.)		
	Guest	Operator	Administrator
Certificates	-	-	Yes
Security Audit	-	-	Yes

a. Guest and Operator accounts see “My Account” on the ADMINISTRATION side-bar menu and can only view/change their own account settings. Administrator accounts see “Accounts” on the ADMINISTRATION sidebar menu and can view/manage all user accounts.

All three roles provide both Web interface and CLI access to the system. These roles and their privileges are also supported using VACM (View-based Access Control Model) for SNMP access control.

Please refer to the *Important Notice* document (available from the Haivision Download Center) for the default login credentials.

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

Administrators can create, delete, lock, and unlock user accounts, including changing the password, from the Accounts page (see “Managing User Accounts” on page 128). Operators and guests can manage their password from the My Account page (see “Changing Your Password” on page 65).

You can also change your own account password CLI using the passwd command.

Note that 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:

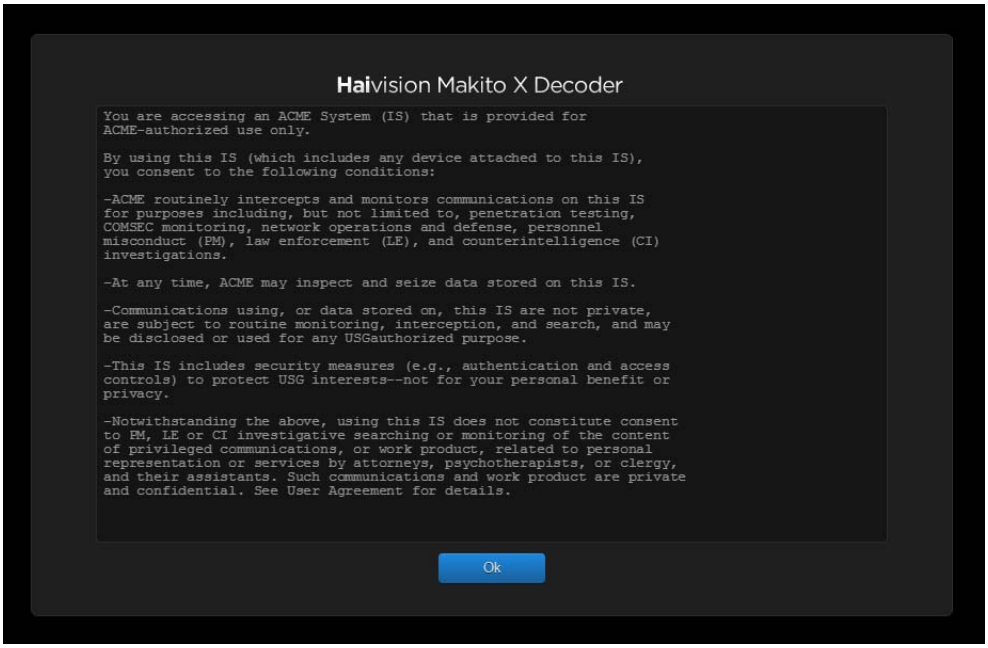
- “CLI Access Control” on page 171

Logging In to the Web Interface

To log in to the Makito X decoder configuration Web page:

1. From your Web browser, type the Makito X decoder's IP Address into the address field and press Enter.

   (Optional) On some systems, you will see an Advisory and Consent Banner, as shown in the following example.



2. Review the Advisory and Consent terms as required for your system and click OK.

   The browser will now display the Login page for the Web configuration interface.

3. On the Login page, type the Username and Password and click Log In (or press Enter).

   Makito X provides three pre-defined user accounts. For information, see the previous section, "Role-based Authorization".

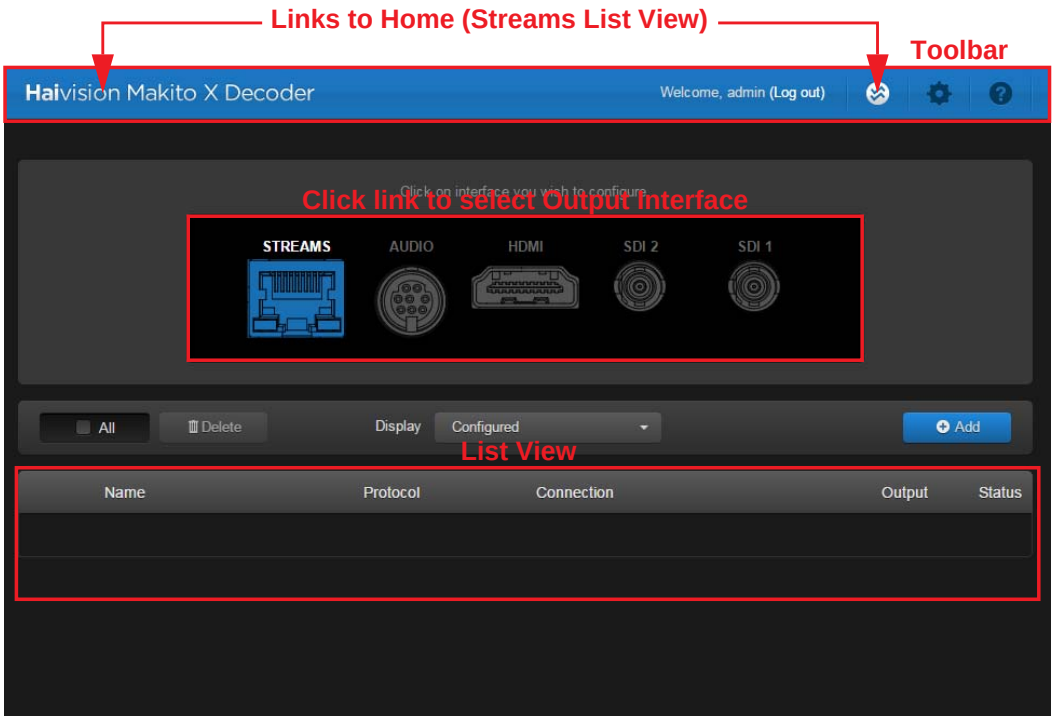
Exploring the Web User Interface

TIP Clicking from the toolbar will launch the online help. For more information, see "Online Help" on page 64.

After logging in to the Web interface, you will have access to the decoder configuration settings. All of the settings can be adjusted via the Web browser.

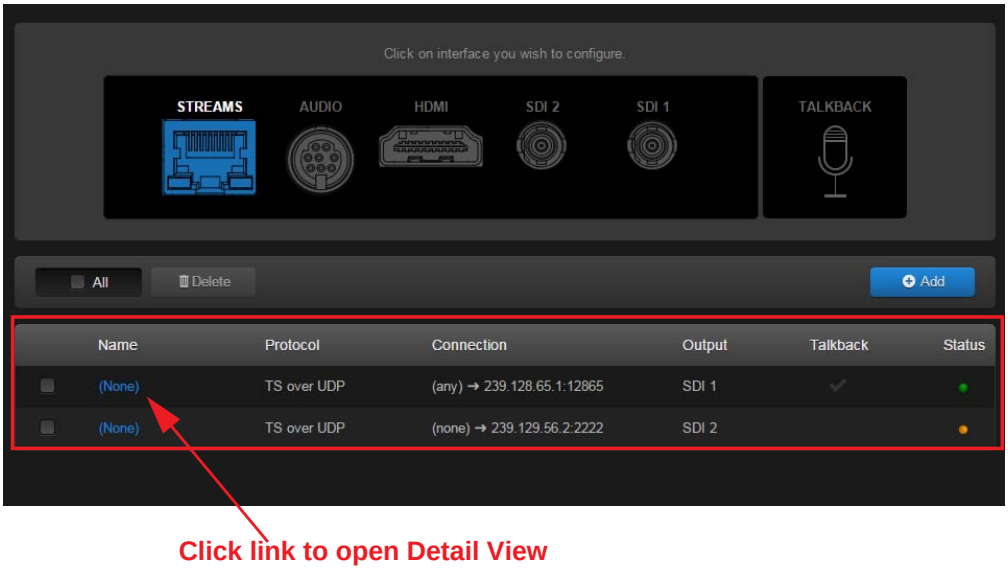
Navigating the Interface

Once you have successfully logged in, the Web interface opens to the Streams List View (as shown in the following example). Your account information is displayed on the toolbar (along the top).



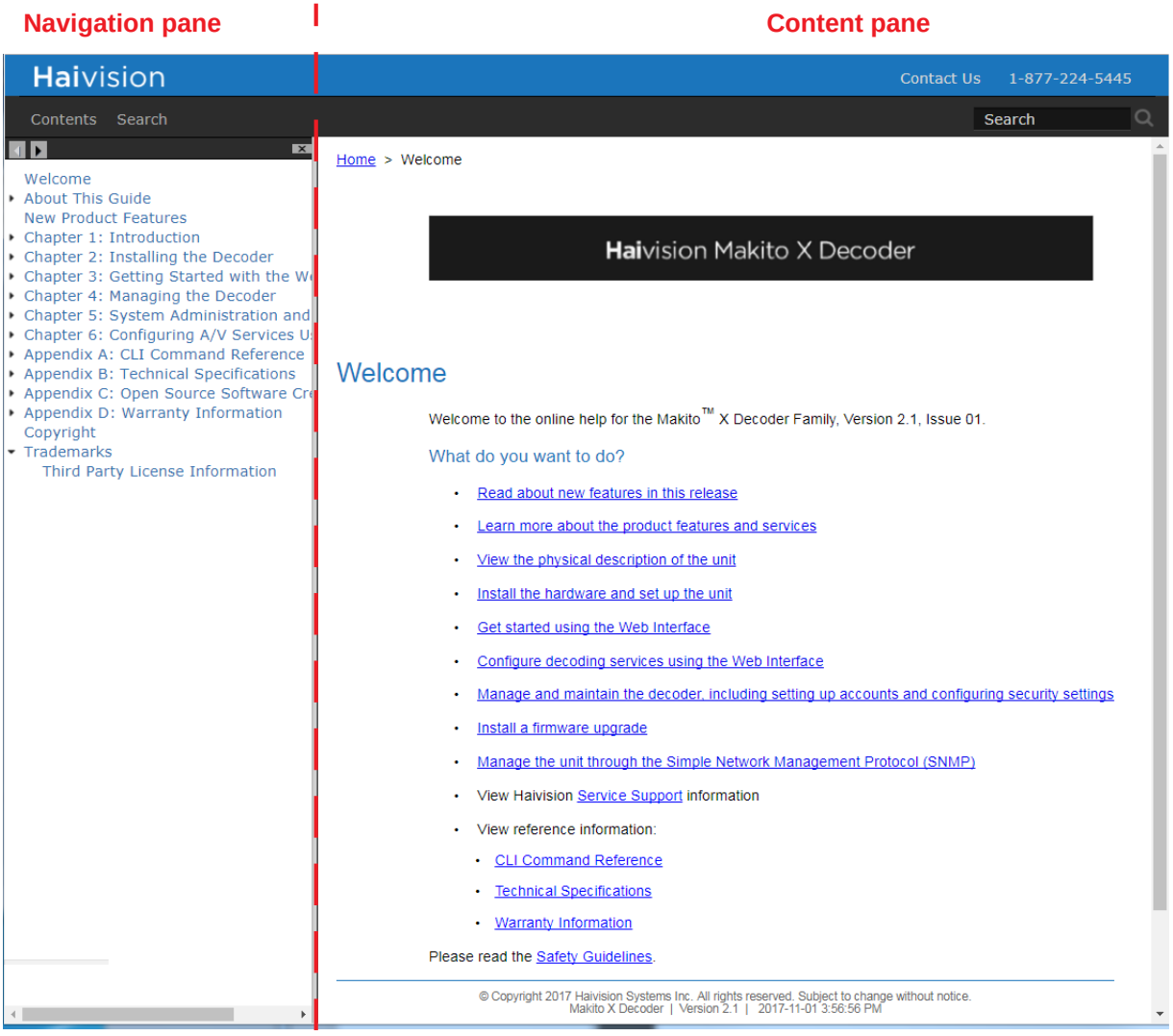
- To create streams or set up decoding, select the output interface, either STREAMS, SDI 1, SDI 2, HDMI, or AUDIO.
- If SAP listening is enabled, you can switch the display between "Configured" and SAP-advertised streams, or "All" from the Display drop-down list. For details, see "Enabling and Disabling Network Services" on page 120.
- If Audio Talkback has been enabled, you will see the Talkback button (as shown in the following figure). Once a stream has started, you can start TALKBACK. For details, see "Starting and Stopping Audio Talkback" on page 76.

- To access the decoder administration settings, click the ADMINISTRATION icon on the toolbar, and then select the area from the sidebar menu, for example NETWORK (under SETTINGS) or ACCOUNTS (under SECURITY).
- (Where applicable) On the List View, click a link in the table to open the Detail View. For example, on the Streams List View (shown below), click a link to open the Streams Detail View.



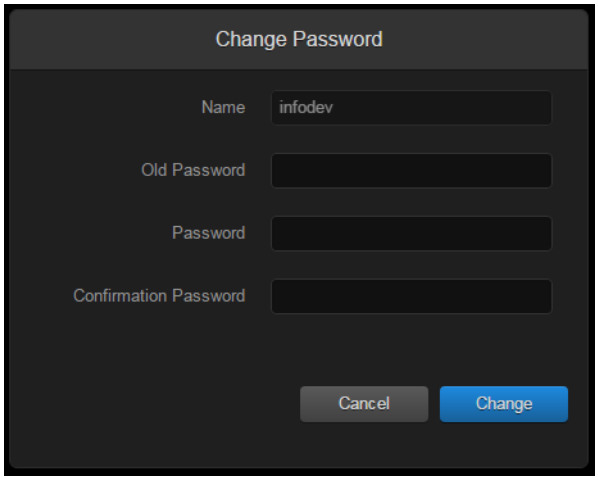
Online Help

Clicking on the toolbar will launch the online help for the Makito X decoder. The figure below shows a sample Welcome page.



Changing Your Password

IMPORTANT For security purposes, be sure to change the default password! The first time you sign into a newly created account as well as any time your password has expired, you will see a Change Password dialog (as shown in the following example).



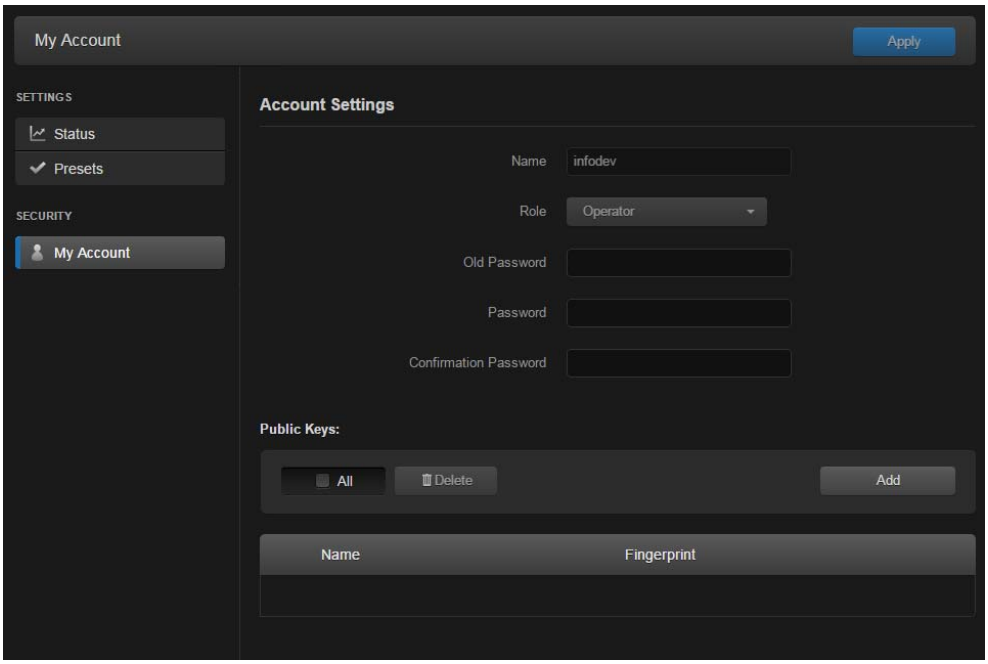
You can also change your own password from the My Account page, as described in this section. This is useful when logging into a Makito X decoder on which the factory defaults have not been changed.

NOTE The My Account page is available to users assigned either Operator or Guest roles. Administrative users may change their passwords from the Accounts page.

To change your password:

1. To navigate to the Administration page, click the ADMINISTRATION icon on the toolbar, and then click MY ACCOUNT from the sidebar menu.

   The My Account page opens as shown in the following example.



2. Type your current password in the Old Password field.
3. Type the new password in the Password field and again in the Confirmation Password field.
4. Click Apply.

   The new password will take effect immediately.

You can also upload and manage personal public keys for your account to enable public key authentication (instead of password-based authentication). Note that in the current release, this only applies to SSH CLI access to the decoder. For more information, see "Managing Public Key Authentication" on page 133.

Password Requirements

Passwords may be up to 80 characters and composed of any combination of upper and lower case letters, numbers, and the following special characters:

"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "~", "`", "_", "-", "+", "=",
"{", "}", "[", "]", ":", ";", "", "'", "<", ">", ",", ".", "?", "/", " "(space)

NOTE Basically, all printable characters of the QWERTY keyboard are supported.

Your system may have in place security policies that determine the minimum password length as well as other requirements such as minimum number of upper case characters, digits, and symbols. In this case, you will be prompted to modify your password to comply with these policies.

Logging Out

After you finish using the Makito X decoder, be sure to log out. To do so, click LOG OUT from the toolbar.

Logging out prevents misuse and unauthorized access to the decoder.

CHAPTER 4: Managing the Decoder

This chapter explains how to set up and manage video decoding using the Web interface.

Topics In This Chapter

Setting Up Decoder Streams

The Makito X decoder provides a Streams List View and separate Detail Views for creating and configuring streams to map the decoder inputs to output interfaces.

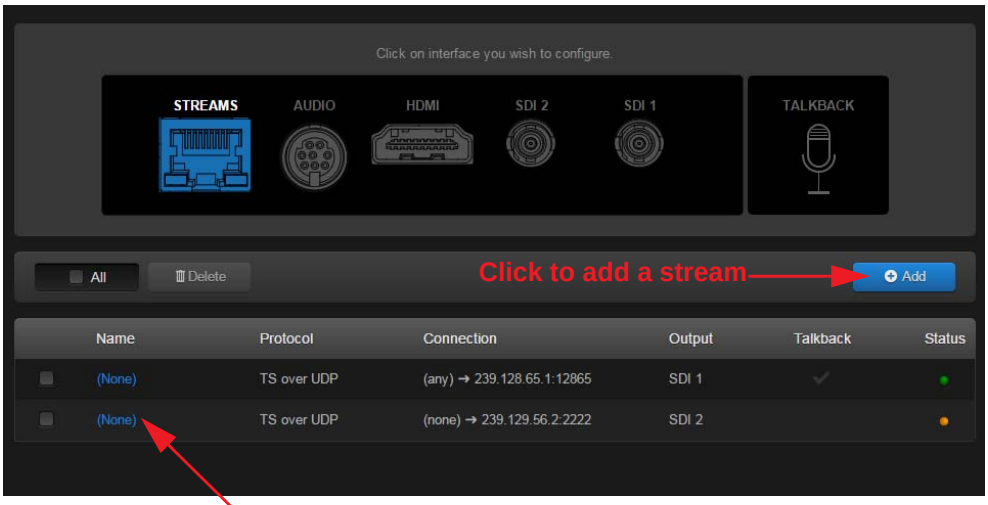
Streams List View

The Streams List View displays a summary of defined streams for the decoder, including the Name, Protocol, Connection details, and status LED for each stream. It also shows the selected Outputs (once streams have been bound to the SDI 1 and SDI 2 output interfaces). If Talkback is enabled, it shows the stream selected for Talkback.

To display the Streams List View:

1. (If not already on the Streams List View) Click the STREAMING icon on the tool-bar.

   The Streams List View opens, showing the defined streams for the decoder (see following example).



   The following LEDs (gray, yellow and green) indicate the stream status:

Status LED Color	Indication
Grey	Stopped or not associated with a decoder.
Yellow	Configured and listening (waiting to receive data).
Green	Receiving data.
Red	Stream connection has failed or a fault has occurred.

The general form of the Connection information is:

SenderIP[:SenderPort]→[ListeningIP]:RecvPort

where:

SenderIP	Can be any, none, hostname, or a unicast IP Address.
SenderPort	(SRT modes only) Is the UDP destination port of the peer SRT device used for the connection.
ListeningIP	Can be a Multicast IP address or optionally the unicast IP address of the decoder.
RecvPort	Is the UDP port on which the decoder is receiving the stream.

2. To add a decoder stream, click Add. See "Configuring Decoder Streams" on page 72.
3. To view details of an existing stream, click a link in the table to open the Streams Detail View. See "Configuring Decoder Streams" on page 72.
4. To display SAP-advertised streams, select "Discovered (SAP)" or "All" from the Display drop-down list. (SAP listening must be enabled; for details, see "Enabling and Disabling Network Services" on page 120.)
5. To start Audio Talkback (if enabled), click TALKBACK and begin talking into your microphone. For details, see "Starting and Stopping Audio Talkback" on page 76.
6. To delete an existing stream, check the checkbox next to one or more streams in the list (or check All), and click Delete.

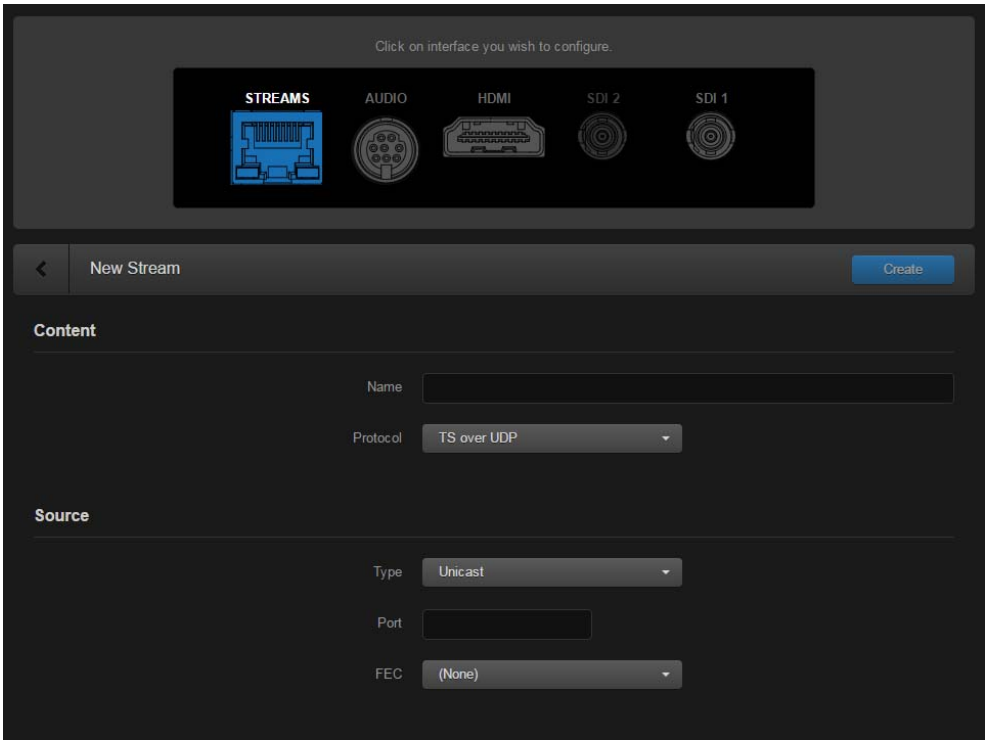
Configuring Decoder Streams

From the Streams Detail View, you can create streams and define the stream settings.

To add a stream:

1. From the Streams List View, click Add.

   The New Stream (Detail View) opens, as shown in the following example.



2. Under Content, type a name for the stream in the Name field.
3. Select the stream Protocol, either TS over UDP, TS over RTP, or TS over SRT.

   The remaining fields vary depending on the stream Protocol. For details see "Stream Settings" on page 78.

NOTE The Multicast address range is from 224.0.0.0 to 239.255.255.255. Multicast addresses from 224.0.0.0 to 224.0.0.255 are reserved for multicast maintenance protocols and should not be used by streaming sessions. We recommend that you use a multicast address from the Organization-Local scope (239.192.0.0/14).

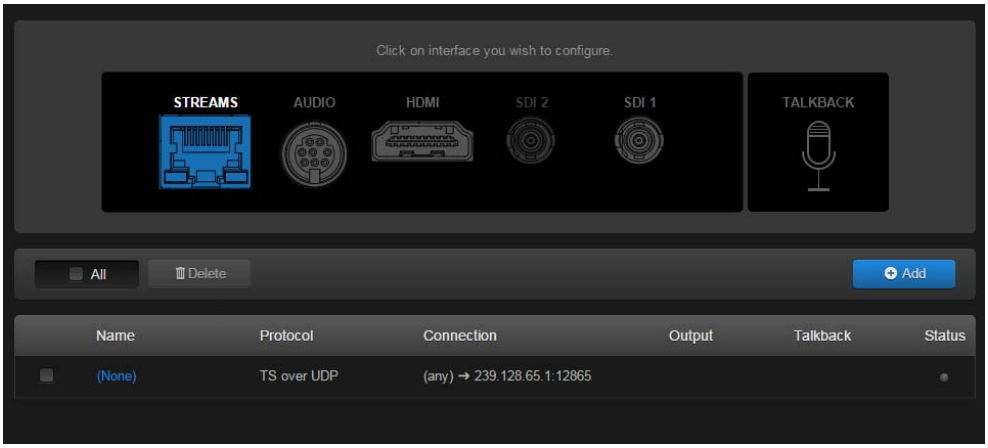
4. Click Create to create the stream.

TIP Intra-refresh (video encoding support) requires that the decoder and streams be started first.

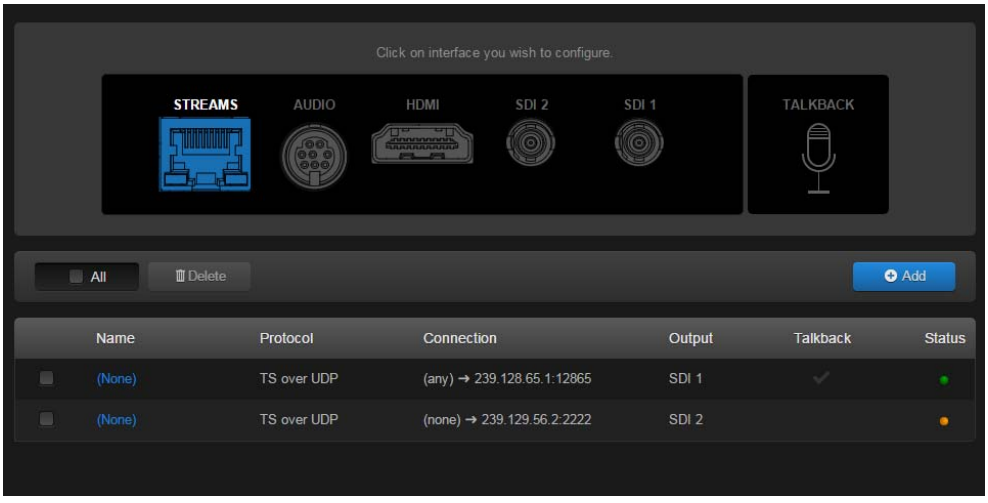
5. To view statistics for the stream, click Statistics. For details, see "Stream Statistics" on page 81.

6. To return to the Streams List View, click < (Back).

   The stream you have created is added to the list. The following example shows the List View after a stream has been created, but not yet bound to output interfaces. (Audio Talkback is available but not enabled.)

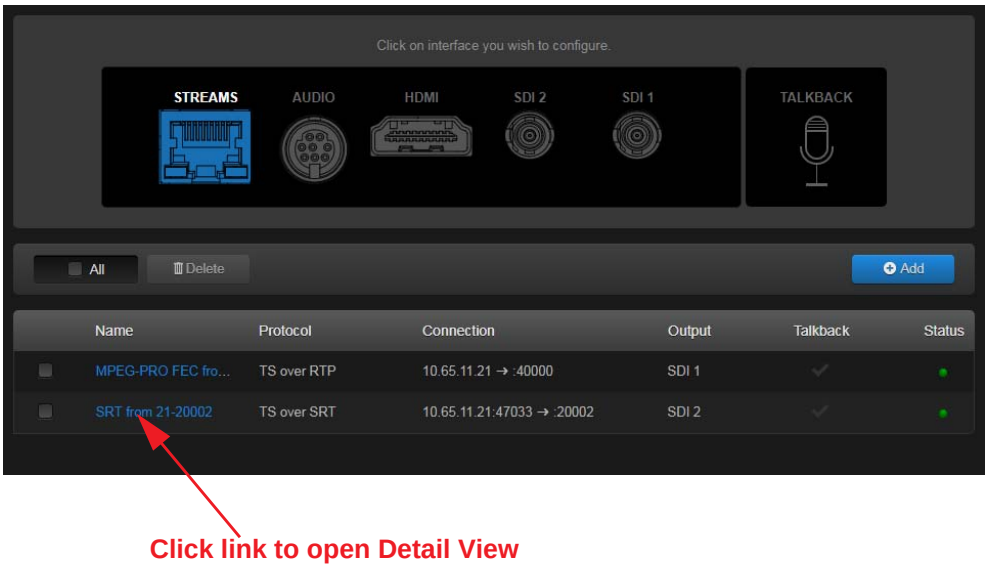


   After streams have been bound to the SDI 1 and SDI 2 output interfaces (see "Configuring Decoder Outputs" on page 86), the outputs will be listed.



To edit a stream:

1. From the Streams List View, click a link in the table to open the Streams Detail View.



2. Select or enter the new value(s) in the appropriate field(s). See "Stream Settings" on page 78.
3. To apply your changes, click Apply.

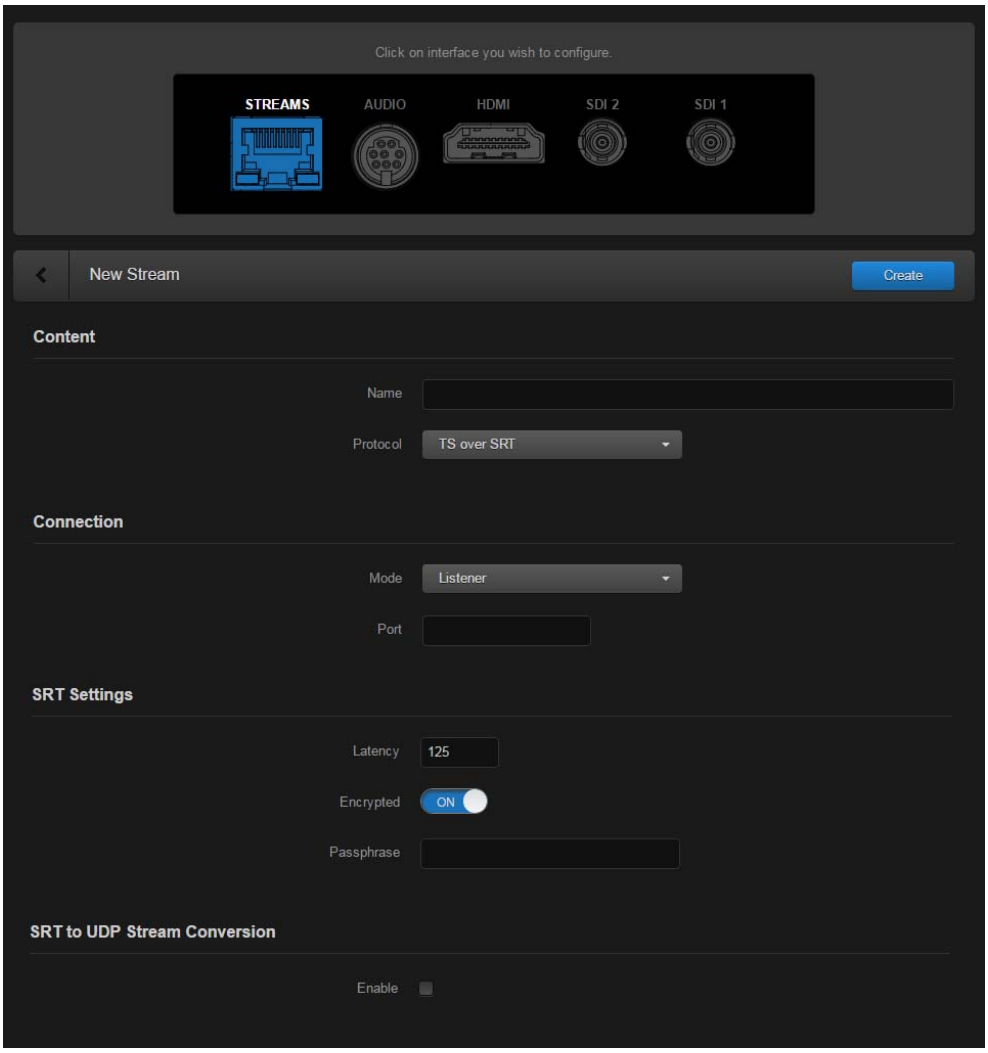
   The changes will take effect immediately but will not be saved and will be lost after a reboot.

TIP To save the current configuration, open the ADMINISTRATION > PRESETS page. See "Saving and Loading Presets" on page 108.

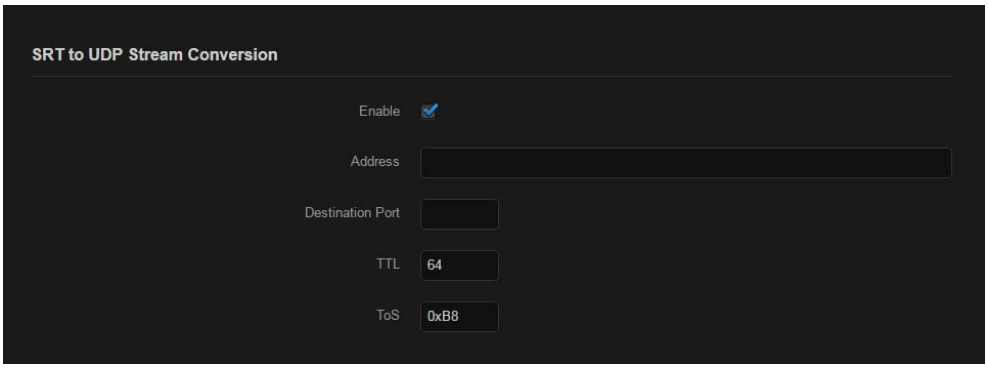
Configuring TS over SRT

For more information, see "Secure Reliable Transport (SRT)" on page 21.

1. On the Streams Detail View, follow Step #1 through Step #3 (page 72) to add a decoder stream.
2. Select the SRT call Mode (Listener, Caller or Rendezvous) for the stream and fill in the Connection settings. (See "Connection (TS over SRT only)" on page 79.).
3. (Optional) Fill in the SRT settings. (See "SRT Settings (TS over SRT only)" on page 80.)



4. (Optional) To convert SRT streams to UDP, check the Enable (SRT to UDP Conversion) checkbox and fill in the fields. (See "SRT to UDP Stream Conversion (TS over SRT only)" on page 80.)

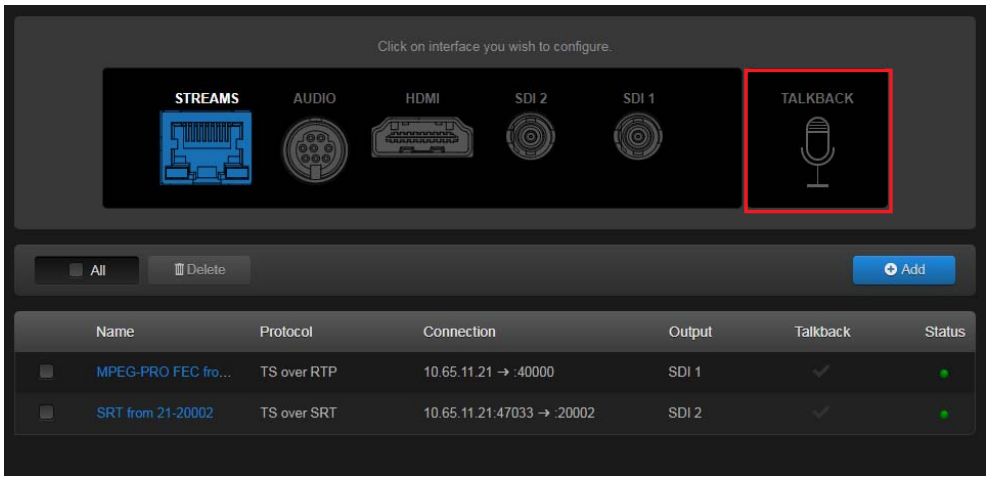


5. Click Apply to create the stream.
6. To view statistics for the stream, click Statistics. For details, see "SRT Stream Statistics" on page 84.

Starting and Stopping Audio Talkback

The Audio Talkback feature allows users to stream a mono channel of audio back to a Makito X encoder over a reliable LAN or WAN. Audio talkback uses the decoder's audio input to enable end users monitoring a streaming session to "talk back" to individuals at the encoder. Audio Talkback must be enabled and configured by an administrative user. For more information, see "Audio Talkback" on page 32.

If Talkback is enabled on your system, you will see the Talkback button on the Streams List View (as shown in the following figure).



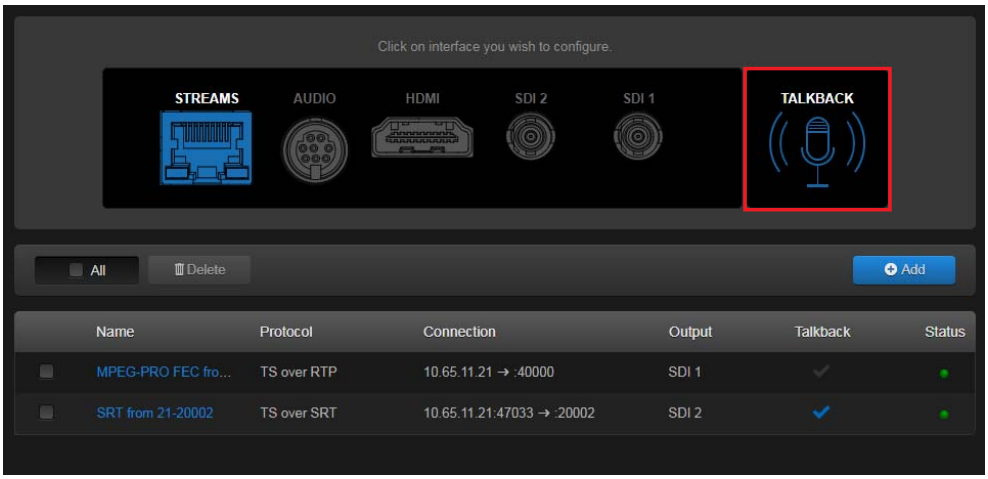
Your system will have been configured to one of two possible talkback activation modes:

- Push-button ("push-to-talk") requires you to click and hold the TALKBACK button to transmit audio.
- Toggle switch stays active until you click the TALKBACK button again.

To start Audio Talkback:

1. From the Streams List View, click the checkmark under Talkback to select the stream. (The stream must have been started.)
2. Click TALKBACK and begin talking into your microphone.

   When Talkback is active, the TALKBACK button icon is blue with a radio wave.



3. To stop a Talkback session, release the TALKBACK button (if using "push-to-talk" mode) or click TALKBACK again to toggle the return audio channel off.

Stream Settings

The following table lists the decoder stream controls and settings:

Stream Setting	Default	Description/Values
Content		
Name	n/a	Specify a name for the stream. 1 to 32 characters
Protocol	TS over UDP	Select the Encapsulation Protocol type for the decoded stream. • TS over UDP: MPEG transport stream over UDP (no RTP header) • TS over RTP: MPEG2 transport stream over RTP • TS over SRT: Haivision's Secure Reliable Transport (see "Secure Reliable Transport (SRT)" on page 21) • RTSP: Real Time Streaming Protocol (RFC2326) with control over RTSP. For RTSP streams, you can specify the address as addr= rtsp://user:password@ip.add.re.ss/ path?var=value& var2=value2...
Source (TS over UDP and TS over RTP only)		
Type	Unicast	Select the Stream Type for the decoded stream. • Unicast • Multicast
Multicast Address	n/a	(Multicast streams only) Enter the multicast IP address in dotted-decimal format.
Source Address	n/a	(Multicast streams only) The Source Address specifies where the multicast stream is coming from (i.e., what address is broadcasting). In cases where many devices are sending multicast streams on the same multicast address, specifying the source encoder address can reduce the amount of multicast traffic being forwarded on your network. Only the multicast traffic from that specific source to that address will be forwarded (instead of all of them).

Stream Setting	Default	Description/Values (Cont.)
Address	n/a	(TS over RTP, Unicast streams only) Enter the source IP address in dotted-decimal format.
Port	n/a	Enter the source UDP port for the stream. Enter a number in the range 1025..65,535. Note that RTP streams use *even numbers only* within this range.
FEC	None	(Optional) Enable Forward Error Correction (FEC). Select either: • (None) • VF (TS over UDP only) • Pro-MPEG FEC (TS over RTP only) NOTE: VF FEC is a proprietary FEC and is not interoperable with devices outside of the Haivision family. On the Encoder, you set all these parameters, whereas on the decoder they are detected from the stream, and are available in the stream stats.
Connection (TS over SRT only)		
Mode	Listener	Specifies the SRT Connection Mode (to simplify firewall traversal): • Caller: The decoder acts like an SRT caller and connects to a server listening and waiting for an incoming call. • Listener: The decoder acts like an SRT listener and listens for a server to connect to it. • Rendezvous: Allows calling and listening at the same time. To simplify firewall traversal, Rendezvous Mode allows the encoder and decoder to traverse a firewall without the need for IT to open a port.
Address	n/a	(Caller and Rendezvous Connection modes) Specifies the destination IP address for the SRT stream.
Source Port	Auto-Assign	(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.

Stream Setting	Default	Description/Values (Cont.)
Destination Port	n/a	(Caller and Rendezvous Connection modes) Specifies the UDP destination port for the SRT stream.
Port	n/a	(Listener Connection mode only) Specifies the UDP local port for the SRT stream.
SRT Settings (TS over SRT only)		
Latency	20	Specifies how long the decoder will buffer received packets. Range = 20 - 8000 ms NOTE: The SRT buffer, configured as "Latency'", is the time reserved in the decoder to recover missing packets. Because real-time video cannot be paused, restarted, slowed down, or accelerated, the buffer adds a fixed delay in the end-to-end latency. If a lost packet cannot be recovered, this may result in an A/V artifact. In this case, you should increase the SRT latency as it is likely too low. Please see the Makito X SRT Addendum for tuning guidance.
Encrypted	Off	Toggle to On to enable decryption of encrypted streams.
Passphrase	n/a	(Encrypted must be On; 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 UTF8 characters
SRT to UDP Stream Conversion (TS over SRT only)		
Enable	Disabled	Check this checkbox to enable UDP retransmission of SRT streams on the local network. NOTE: The SRT input stream may be encrypted and includes error correction. Enable this to rebroadcast the SRT stream on the local LAN without the encryption and error correction elements over UDP. A single multicast or unicast destination TS/UDP stream is supported for re-streaming.
Destination IP Address	n/a	Specifies the destination IP address for the stream.

Stream Setting	Default	Description/Values (Cont.)
Destination Port	n/a	Specifies the UDP source port for the stream.
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops the stream packet is allowed to travel/pass before it must be discarded. 1..255
ToS	184 or 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)

Stream Statistics

The following table lists the Stream statistics:

Stream Statistic	Description/Values
State	The current operating status of the stream, either: • STREAMING • STOPPED • PAUSED
Bitrate	The stream bitrate (in kbps).
Received Packets	Number of RTP or UDP packets received for that stream.
Received Bytes	Number of Bytes received for that stream.
Received Errors	The number of errors received for that stream.
Corrupted Frames	Number of audio or video frames that were corrupted by missing packets.
Pauses	The number of times the decoder has sensed that no new stream has been received for > 1 second.
Source Address	IP address of the stream source (sender).
Reset	Click to reset the Stream statistics.

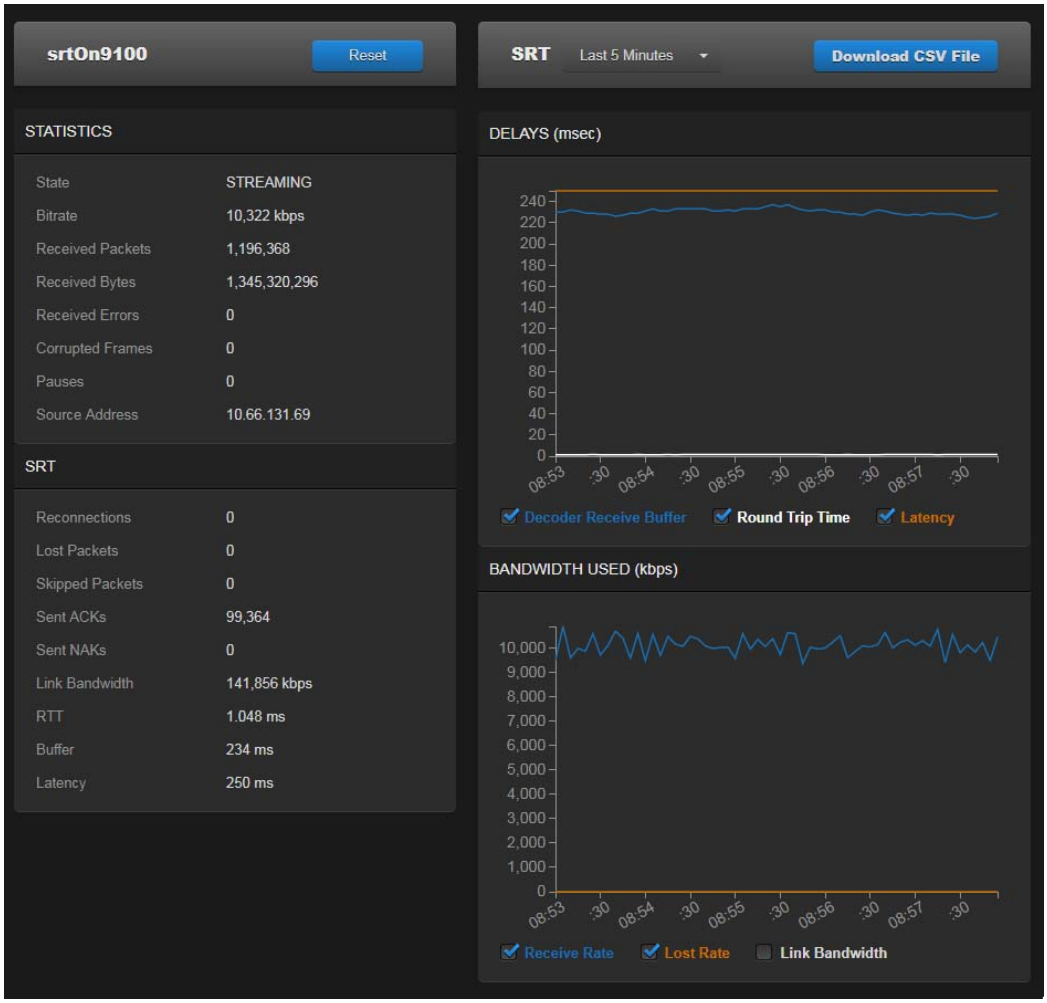
Stream Statistic (Cont.)	Description/Values (Cont.)
SRT	
Reconnections	Number of reconnections since the stream started. Severe network congestion may cause the connection to drop and automatically reconnect. See "SRT Stream Statistics" on page 84.
AES Encryption	Indicates whether AES encryption has been enabled. Either On or Off.
Key Length	The key length for AES encryption. Either None, AES-128 or AES-256.
Decryption	Indicates whether the decoder can decrypt the stream. Either Active, Initializing, Inactive (no passphrase), or Inactive (invalid passphrase).
Lost Packets	Number of SRT packets reported missing by the decoder. 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.
Skipped Packets	Number of SRT packets reported skipped. NOTE: These are packets that have arrived at the destination device too late, or that never arrive at all. The time to play the packet has arrived and the lost packet was not recovered, so the decoder/receiver will continue playing. Some type of video artifact may result (i.e., a replayed frame or video blocking artifacts). • If this statistic increments slowly, the best thing to do is increase the SRT Latency. • If this statistic increments in large jumps, the best thing to do is lower your video bitrate or increase your overhead if you have available BW.
Sent ACKs	Transmission progress acknowledgment and feedback sent.
Sent NAKs	Lost packet reports sent.
Link Bandwidth	An estimate of the actual link bandwidth.
RTT	Measured Round Trip Time.

Stream Statistic (Cont.)	Description/Values (Cont.)
Buffer	Decoder buffer in milliseconds. SRT decoder buffers are the received stream packets waiting to be decoded. This statistic shows the portion of the decoder 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 decoder buffer in absence of packet lost is just below the latency value. In presence of packets lost, it is between 0 and the latency value. TIP: If the Buffer goes to 0 often, then there is most likely insufficient BW to support the desired bitrate. in this case, decrease your bitrate. If the Buffer occasionally goes to 0, then the SRT Latency should be increased.
Latency	Maximum of the decoder and encoder configured Latency. For example: Encoder Configured SRT Latency = 750 ms Decoder Configured SRT Latency = 20 ms The SRT Stats Latency (which is the current SRT connection applied Buffering Latency) = 750 (largest of the two). At startup, handshake exchanges the value configured on both sides and the largest one is selected. The decoder default is set to the minimum (20ms) so it can be completely controlled from the encoder side.
Download CSV File	Click to download the statistics in CSV ("Comma Separated Value") file format, which may be used to exchange data with applications such as Microsoft Excel.
TS over RTP: Pro-MPEG FEC	
Level	The level of FEC protection: • A (Column only): uses the column FEC stream. • B (Row and Column): uses both column and row FEC streams.
Number of Columns/Rows	Number of columns and number of rows are the dimensions of the FEC matrix.

Stream Statistic (Cont.)	Description/Values (Cont.)
Block Aligned	The type of FEC matrix scheme: • Yes: Sequential columns within a group start on the same row. • No: Each column starts on the row below the row on which the previous column started.

SRT Stream Statistics

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



NOTE Not all browsers can support the statistics graphics for SRT. You need an up-to-date version of Firefox, Chrome (Chromium), Safari (WebKit), Opera, or IE9 (or higher) to support the graphics in the SRT statistics page.

TIP For both the Delays and Bandwidth Used displays, you can select the inputs, such as the link bandwidth available over the time period.

Configuring Decoder Outputs

From the SDI 1 and SDI 2 Decoder pages, you can manage video decoding for the SDI 1 and SDI 2 ports. This includes binding the video output(s) to the stream(s) you have created and configuring properties such as the Output Resolution and Frame Rate.

Each decoder channel can support an alternate (secondary) stream as input which is switched to if the primary fails in order to minimize down-time.You can also select a Still Image such as a black screen that the decoder will display if it is no longer receiving video (for example, if the encoder stream has stopped or the network connection is lost).

The SDI Decoder pages also display a status summary of embedded digital audio and metadata inputs.

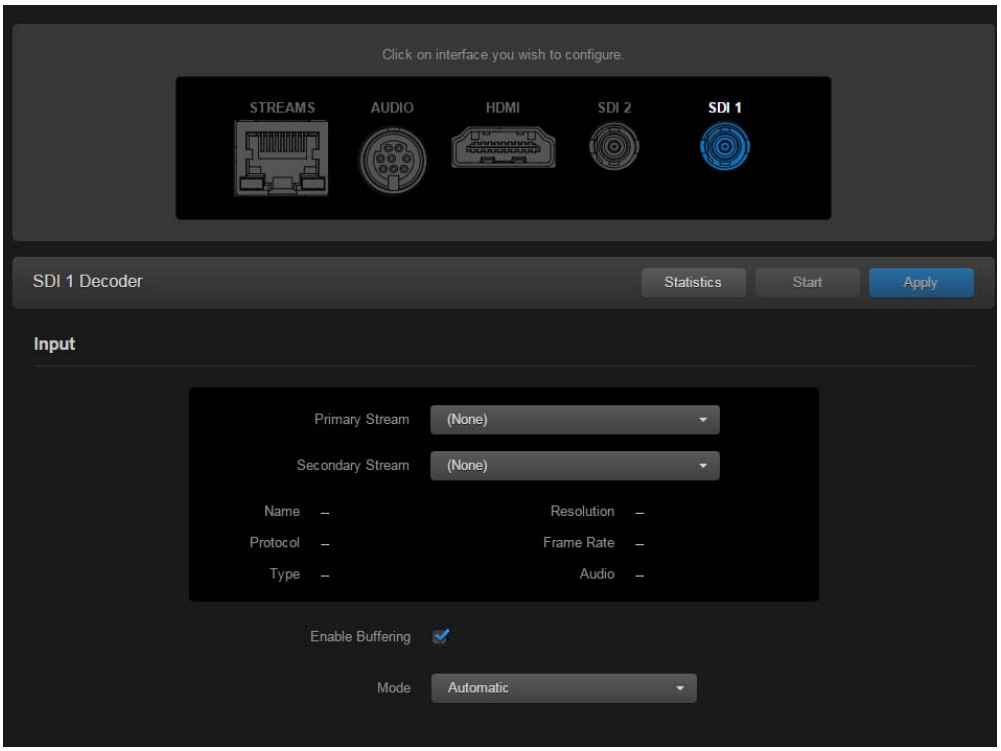
NOTE The Makito X decoder supports two independent video decoders that feed the two SDI interfaces. The HDMI port can be configured to mirror the same content that is seen on either Decoder 1 or Decoder 2. If the stream contains computer graphics content, that content can only be displayed on the HDMI interface.

Configuring the SDI Decoder Output

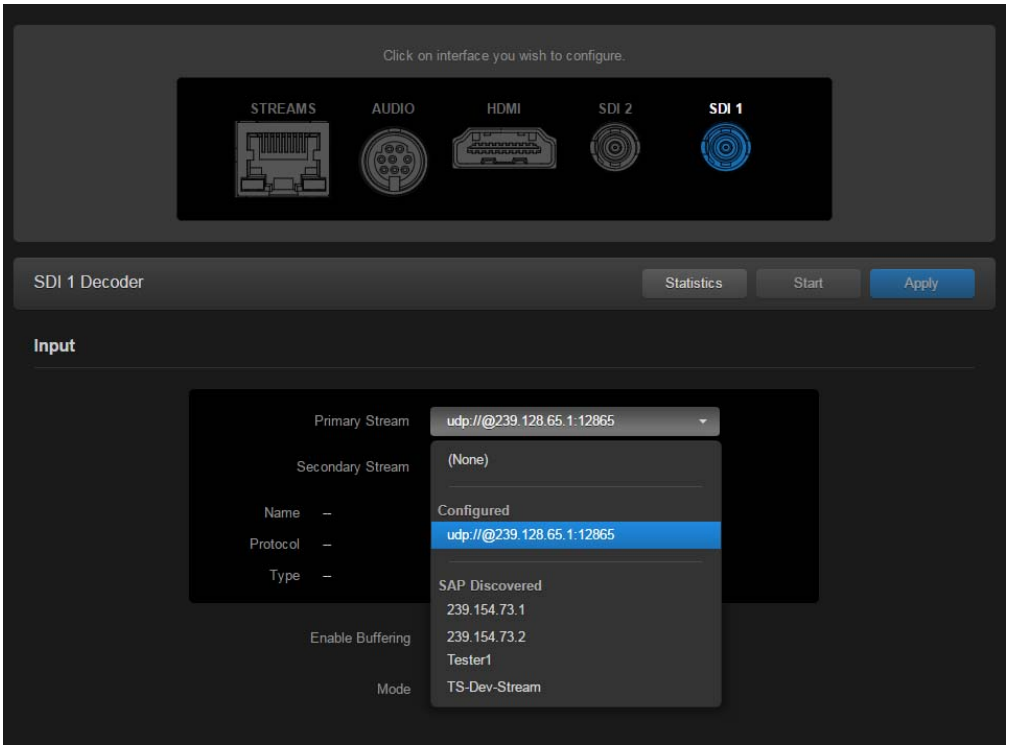
To display the SDI Decoder Settings:

1. Click SDI 1 or SDI 2 from the output interface bar.

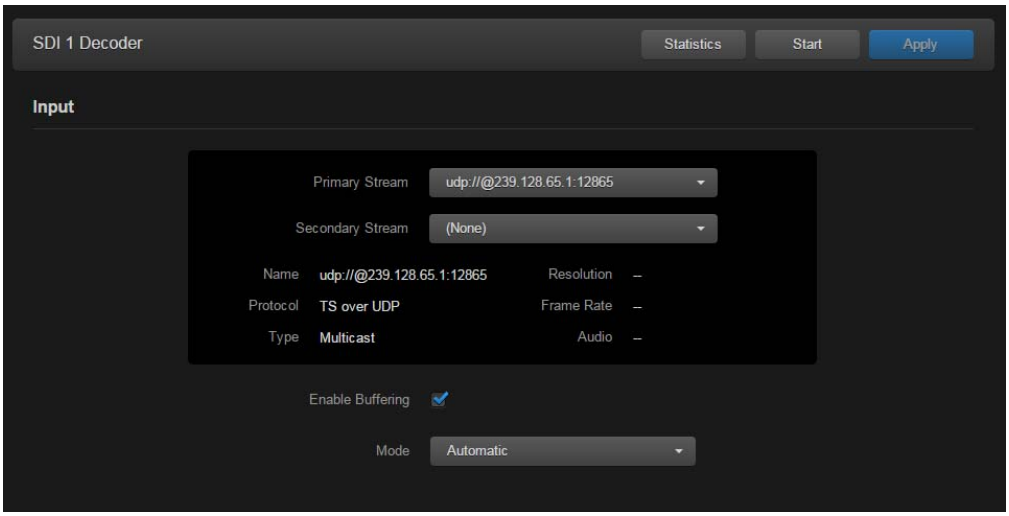
The SDI 1 or SDI 2 Decoder page opens, displaying the current video decoding settings (see SDI 1 example, following page).



2. Under Input, select the Primary input stream from the drop-down list of the stream(s) you have created or “SAP Discovered” if SAP listening is enabled.

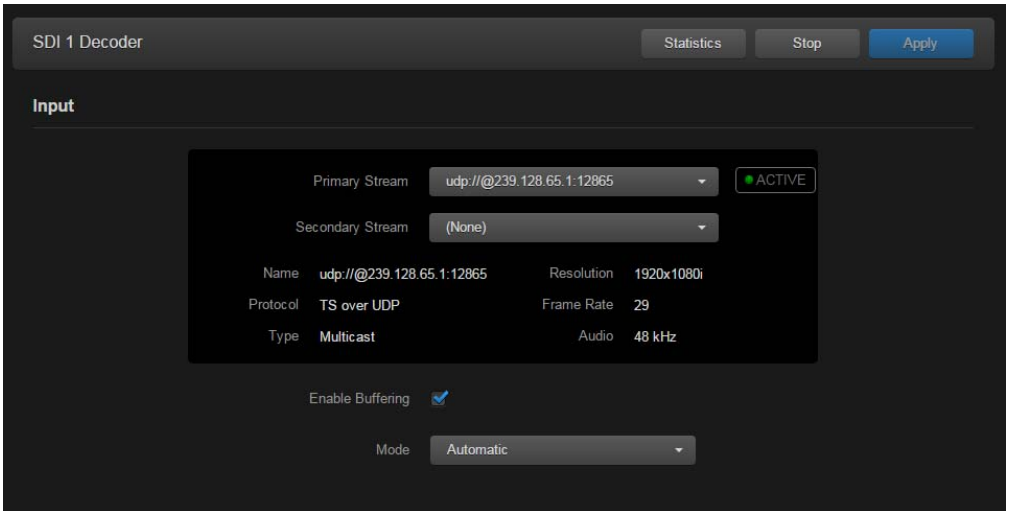


The Name, Protocol, Type, incoming Resolution, Frame Rate, and Audio Sampling Rate for the selected stream now are displayed.



3. To start decoding, click Start.

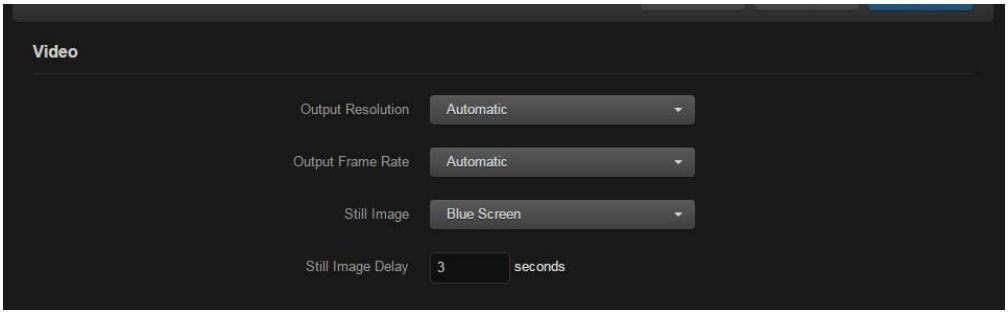
   The Active status LED turns on if the decoder is receiving data.



4. (Optional) Select a Secondary (alternate/redundant) stream for the decoder channel.

NOTE The stream's encapsulation protocol must match the Primary Stream. The decoder will automatically switch to the Secondary Stream if the Primary Stream is lost and vice-versa.

5. If required, adjust the video settings. For details, see the following section, "SDI Decoder Settings".

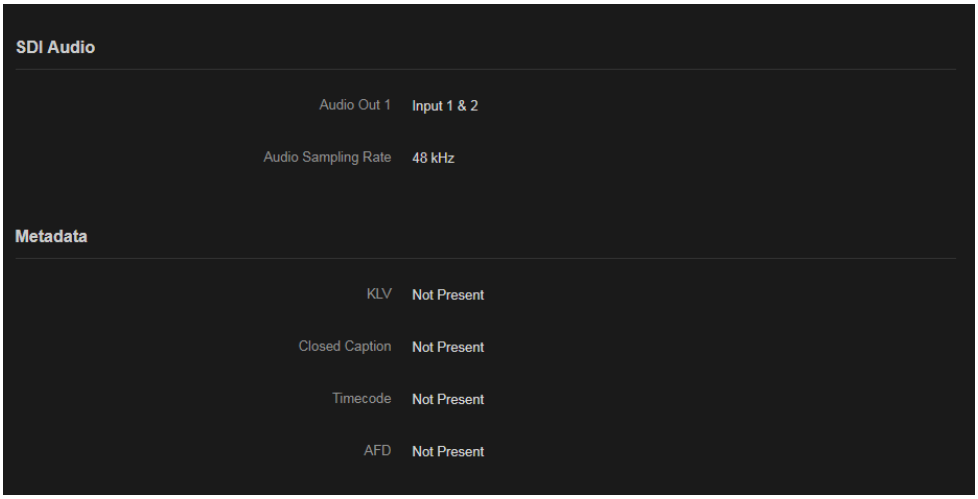


6. To apply your changes, click Apply.

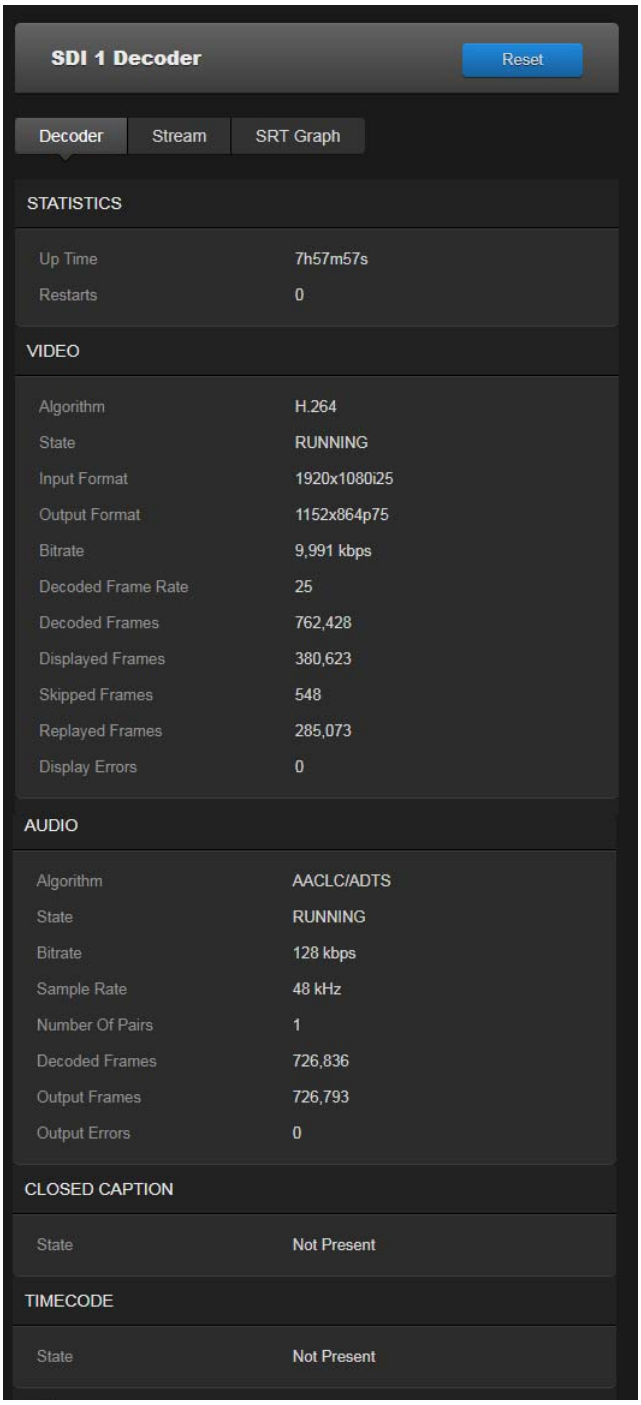
   The changes will take effect immediately but will not be saved and will be lost after a reboot.

TIP To save the current configuration, open the ADMINISTRATION > PRESETS page. See "Saving and Loading Presets" on page 108.

When you scroll down the page, you will see a status summary of embedded digital audio and metadata inputs (as shown in the following example).



7. To view statistics for the decoder, primary stream, and secondary stream (if configured), click Statistics (example shown following page).



TIP The stream type is automatically determined on decoder startup. The decoder Video Algorithm statistic shows which codec algorithm (H.264 or HEVC) is in use for a decode channel.

SDI Decoder Settings

The following table lists the SDI decoder settings:

Decoder Setting	Default	Description/Values
	Input	
Primary Stream	(None)	Select the primary input stream from the drop-down list of the stream(s) you have configured or "SAP Discovered" streams (if SAP listening is enabled). See "Setting Up Decoder Streams" on page 70.
Secondary Stream	(None)	(Optional) Select an alternate (secondary) stream for the decoder channel.
Name	n/a	(Read-only) The Name of the selected primary input stream.
Protocol	n/a	(Read-only) The encapsulation Protocol for the stream, e.g., TS over SRT.
Type	n/a	(Read-only) The stream Type, e.g., Unicast or Multicast.
Resolution	n/a	(Read-only) The input signal detected from the incoming video stream. It includes the number of pixels per line, and whether the video is interlaced or progressively scanned (indicated by i or p).
Frame Rate	n/a	(Read-only) The frame rate per second of the incoming video stream.
Audio	n/a	(Read-only) The sampling rate of the incoming audio signal.
Enable Buffering	Enabled	Check or clear this checkbox to enable or disable buffering (see Mode following). NOTE: When buffering is disabled, the decoded picture buffer is passed to the output interface with no buffering to compensate for stream jitter. This is the lowest latency mode, but may have noticeable skip and replay artifacts.

Decoder Setting	Default	Description/Values (Cont.)
Mode	Automatic	(Enable Buffering must be checked) The type of buffering to use. A jitter buffer temporarily stores arriving packets in order to remove the effects of jitter from the decoded stream. • Automatic: Automatic mode favors smooth playing content with good synchronization between audio and video. The incoming stream is monitored and the optimal required delay is determined so that stream packet and video picture jitter is absorbed. The calculated delay may change slowly as network and video conditions change. NOTE: The added delay will not decrease with time even if the video jitter disappears. The added delay depends on the monitored video jitter. It also depends on the audio arrival time; if the audio is late, this delay will be added to the current calculated delay. For example, if the audio is late by 500 ms (vs Video), an additional 500 ms delay will be added to allow the Audio/Video synchronization. • Fixed: Fixed mode allows users to specify a delay to be added to the decode pipeline after the content is decoded. The amount of delay does not vary and artifacts may result if a too low value is used. NOTE: The decoder has a minimum buffer set based on the resolution and frame-rate of the stream content. In addition, users can add more delay if desired: (1) to achieve a specific decoding latency for inter-channel synchronization purposes; (2) to deal with unusually large amounts of jitter in the stream; or (3) to allow A/V sync to occur when the stream content is highly out of sync. (See Delay below.)

Decoder Setting	Default	Description/Values (Cont.)
		• Adaptive Low-Latency: The decoder measures the stream packet and video picture jitter and adds in a delay so that artifacts are minimized while also minimizing video latency. Provides backward compatibility with older decoder versions. NOTE: Audio artifacts may occur if audio is streamed after video when using Adaptive Low Latency. This mode does not consider the audio arrival time. If the audio is late by 500 ms, the audio /video will be unsynchronized by at least 500 ms. In theory the audio should play smoothly as long as there is not significant jitter. If the audio jitter is over 40 ms, audio artifacts will be noticeable. NOTE: The maximum delay is 2000 ms. If for any reason the system requires more than this value to play smoothly, video or audio artifacts will be noticed.
Delay	0 ms	(Enable Buffering must be checked and Mode must be Fixed) The delay in ms when using buffering in Fixed mode. 0...2000 ms delay
		Video
Output Resolution	Automatic	The dimensions of the frames (width and height) to send to the display with an indicator (i or p) whether the video is interlaced or progressively scanned. • Automatic: Allows the decoder to choose a suitable display format based on the stream parameters and the connected display's capabilities. NOTE: Attempts to up/down-scale incoming video that is not supported to a nearest or best matching supported resolution. • Native: If the stream's encoded format is supported as a display format, the display format chosen will always be the same as stream's encoded format regardless of the connected display's capabilities. Otherwise, no video will be displayed. When selected, Output Frame Rate is disabled.

Decoder Setting	Default	Description/Values (Cont.)
		NOTE: Native maintains the output resolution/frame rate exactly as received in the stream and overrides HDMI triggered settings. Otherwise, if an HDMI device is detected, the decoder will scale to match an available resolution/frame rate supported by the HDMI device. • TV Resolutions: 1920x1080p…720x480i • Computer Resolutions: 1920x1200… 640x480
Output Frame Rate	Automatic	The frame rate per second generated for the displays: • Automatic: The decoder will select the best display frame rate based on the stream parameters and the connected display's capabilities. • 75, 60, 59, 50, 30, 29, 25, 24 or 23 NOTE: If Automatic is selected, the actual frame rate generated will be the next highest valid frame rate supported by the SDI and HDMI interface, plus the one that gives the best decimation factor. For example, 30 Hz could be chosen instead of 29.970 Hz.
Still Image	Freeze	The type of static image to display when the decoder is not receiving a video stream. • Freeze: continues to display the last decoded video frame. • Black Screen: displays a black screen. • Blue Screen: displays a blue screen. • Color Bars: displays a series of vertical color bars across the width of the display. • Mute: disables the video output. • Select Image: opens the Still Images selection dialog for you to select a custom still image. Images must be uploaded by an administrative user. For details, see "Configuring Still Image Streaming" on page 126 NOTE: When the still image is substituted on the display outputs, the video frame rate and resolution will be maintained.
Still Image Delay	3	The delay in seconds before the still image is displayed. 1…1000

Video Decoder Statistics

The following table lists the SDI1 and SDI2 Decoder statistics:

Decoder Statistic	Description/Values
Statistics	
Up Time	The length of time the decoder is actively decoding (e.g., 5d22h15m25s).
Restarts	The number of times the decoder was internally restarted due to a change in encoded stream parameters (resolution and/or frame rate) or because of excessive errors in the stream.
Video	
Algorithm	The compression algorithm detected in the decoded stream, either: • AVC/H.264 • HEVC/H.265 • MPEG2 • Invalid (the video compression algorithm is not recognized)
State	The current operating status of the decoder, either: • INACTIVE: Decoder has not been started • RUNNING: Decoder is currently running with signal • INVALID: Decoder is currently running with no signal
Input Format	The input signal detected from the encoder.
Output Format	The output signal sent from the decoder.
Bitrate	The bitrate for the decoded video.
Decoded Frame Rate	The video frame rate per second.
Decoded Frames	The number of decoded video frames. TIP: Video frames are complete pictures sent in a cascade for display at a distinct point in time. See Audio “Decoded Frames” on page 97.
Displayed Frames	The number of decoded frames.

Decoder Statistic (Cont.)	Description/Values (Cont.)
Skipped Frames	Skipped frames occur when the time to play a video frame has already passed when the decoder is finished producing a new video frame. In this case, the video frame is dropped (never displayed) and it is counted as skipped. The decoder does this to minimize the latency and maintain audio/video sync. The most likely reason for this to occur is that the video is complex and takes more time to decode than is expected by the decoder.
Replayed Frames	A replay frame occurs when the same video frame is played twice in a row on a decoder output. It occurs when the decoder is too slow to produce a video frame and there is nothing else to display. In this case, the decoder will replay the last frame played. Conditions such as network congestion and packet loss, complex video scenes, and the decoder attempting to minimize latency can all cause replay frames. TIP: If the Replayed Frames stat increments periodically and video playback is not smooth, we recommend that you try running the decoder using Fixed mode with a delay added of up to 2000ms of buffering, or less as playback quality permits. This should take care of most non-congestion related skip/replay situations.
Display Errors	The number of display errors.
Audio	
Algorithm	The audio compression algorithm, either: • AACLC / ADTS: decodes audio using the ISO/IEC 14496-3 MPEG-4 AAC-LC algorithm with ADTS headers. • AAC-LC / LATM: decodes audio using the 14496-3 MPEG4 AAC-LC algorithm with LOAS/LATM headers. • MPEG1 Layer 1/2/3 (ISO/IEC 11172-3) designated as MP1, MP2 and MP3, respectively.
State	The current operating status of the decoder, either: • RUNNNG • STOPPED
Bitrate	The bitrate for the decoded audio.
Sample Rate	The number of audio samples per second taken from the output signal. 48 kHz only.

Decoder Statistic (Cont.)	Description/Values (Cont.)
Number of Pairs	The number of audio channel pairs played as surround sound over the HDMI interface.
Decoded Frames	The number of decoded audio frames. TIP: Audio frames are same-sized groups of audio samples to be played back. See Video "Decoded Frames" on page 95.
Output Frames	The number of output frames
Output Errors	The number of output errors.

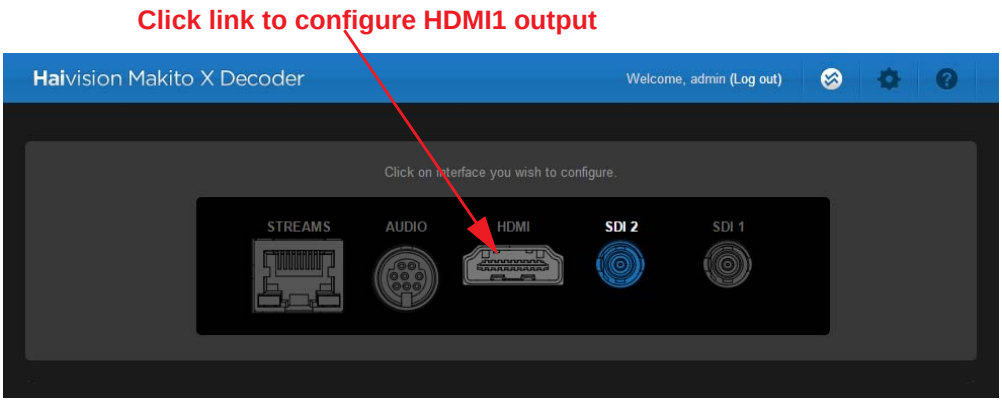
Configuring the HDMI Display

From the HDMI Display page, you can manage audio/video decoding for the HDMI port. You can configure the HDMI port to mirror the same content that is seen on either SDI 1 or SDI 2. The decoder also can support the display of computer graphics content over the HDMI port.

NOTE By default, HDMI displays the SDI 1 content, so you only need to change the HDMI setting to monitor the SDI 2 channel.

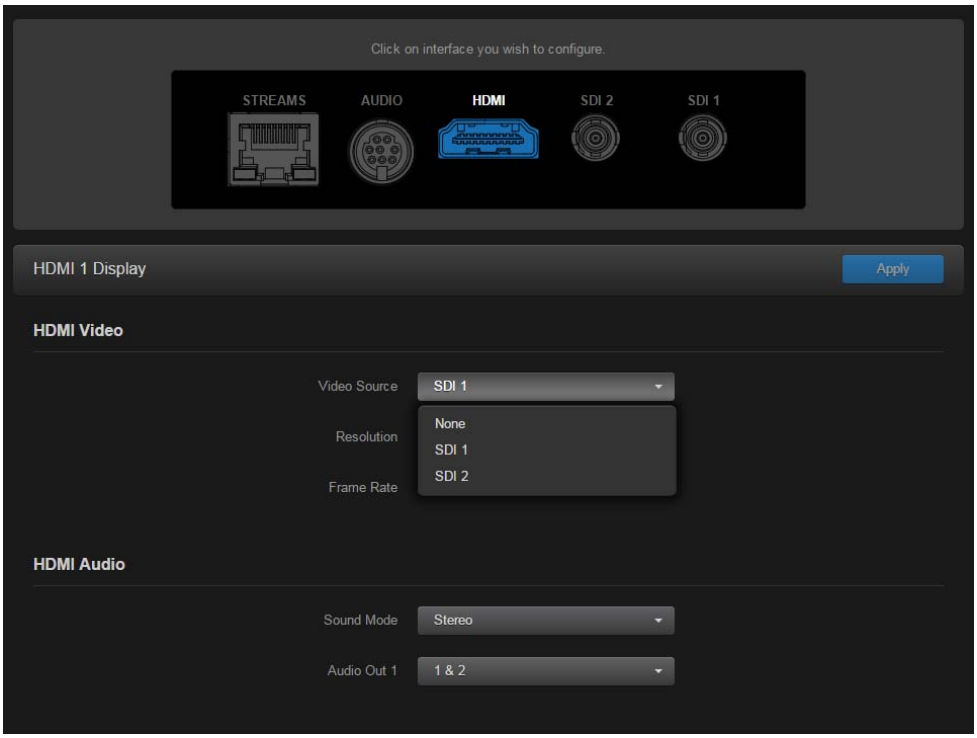
To display the HDMI Display Settings:

1. Click HDMI from the output interface bar.



   The HDMI page opens, displaying the current HDMI decoding settings.

2. To change the HDMI video source, select either SDI 1 or SDI 2.



3. To play streams containing multiple audio channel pairs as surround sound over the HDMI interface, select Surround for the Sound Mode.
4. For (Stereo) Audio Out 1, select which audio source to play on the HDMI audio channels 1 (left) and 2 (right). You can select from the set of audio channel pairs available for the selected decoder driving the HDMI video. The default audio source is the first pair in the input stream.

NOTE When the decoder is licensed for one channel only, the SDI2 interface is not available.

5. To apply your changes, click Apply.

Configuring the Analog Audio Output

NOTE On the dual channel decoder, two streams are received and can be displayed on either SDI video port. Analog audio can be selected from embedded channels on either stream.

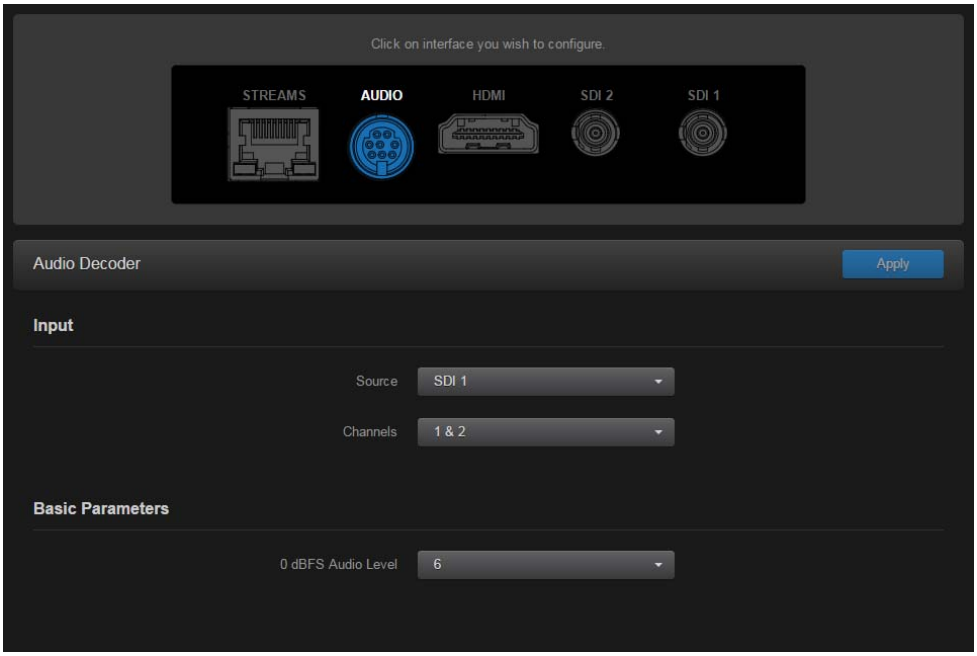
Both Analog Audio and Embedded Digital Audio are active.

From the Audio Decoder page, you can bind the analog audio output to either the SDI 1 or SDI 2 video decoder. You can also configure audio settings such as the Audio Level and view the Audio Sampling Rate.

To display the Decoder Audio Settings:

1. Click AUDIO from the output interface bar.

   The Audio page opens, displaying the current analog audio decoding settings, as shown in the following example.



2. Select or enter the new value(s) in the appropriate field(s). For details, see "Analog Audio Settings" on page 101.

3. To apply your changes, click Apply.

   The changes will take effect immediately but will not be saved and will be lost after a reboot.

TIP To save the current configuration, open the ADMINISTRATION > PRESETS page. See "Saving and Loading Presets" on page 108.

Analog Audio Settings

The following table lists the decoder analog audio controls and settings:

Audio Setting	Default	Description/Values
Input		
Source	SDI 1	The input source for analog audio, either: • SDI 1 • SDI 2 NOTE: When the decoder is licensed for one channel only, the SDI2 option is not available. The content on SDI2 mirrors the content from the SDI1 interface.
Channels	1&2	The input channel for analog audio, either: • 1&2 • 3&4 • 5&6 • 7&8 NOTE: When the decoder is licensed for one channel only, the channel pairs 9&10, 11&12, 13&14, and 15&16 are also available.
Basic Parameters		
0 dBFS Audio Level (dBu)	+6 dBu	(Analog Input only) Adjusts the maximum analog Audio Output level (0 dBfs) from +5dBu up to +20dBu. NOTE: This is useful in applications such as broadcast and streaming to allow higher audio headroom.

CHAPTER 5: System Administration and Security

This chapter explains how to manage and maintain the decoder, set up accounts, and configure security settings for the Makito X using the Web interface.

NOTE Most of these pages/functions require Administrator privileges. The exceptions are Status and My Accounts, which are accessible to all users, and Presets, which is accessible to Operators as well as Administrators.

Topics In This Chapter

Settings

Media

Security

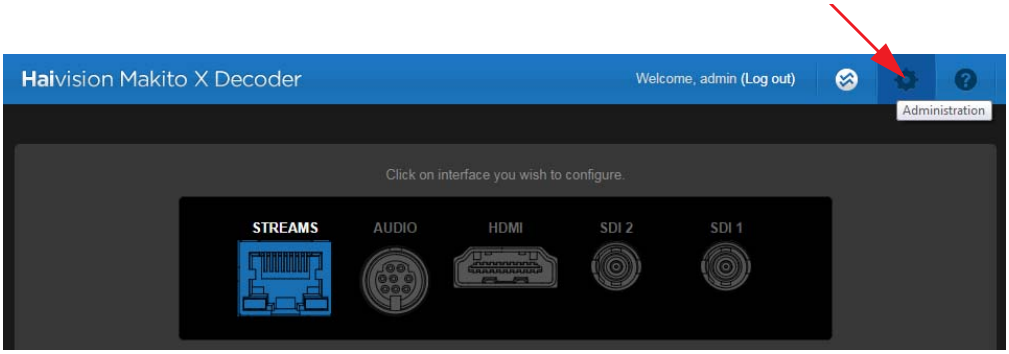
Viewing System Status Information

From the Status page, you can view status information about the Makito X, such as the operating system up time, along with information about the hardware and software components. You can also reboot the decoder and take a system snapshot from the Status page.

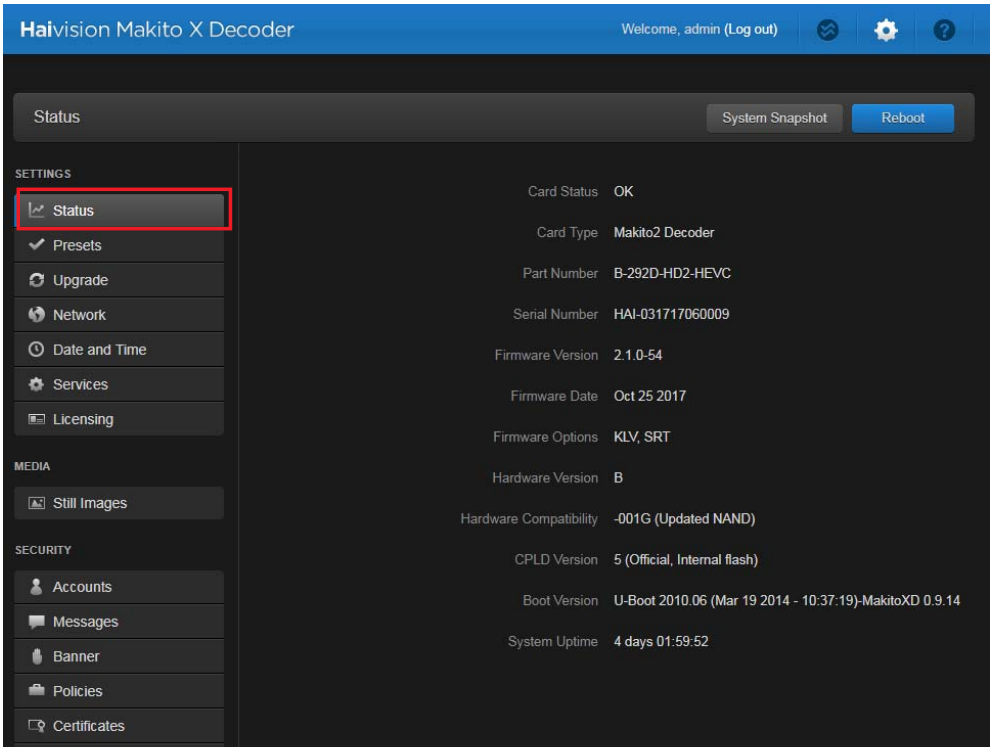
The Status page is available to Operator and Guest users as well as Administrators.

To view status information:

1. Click the ADMINISTRATION icon on the toolbar, and then click STATUS from the sidebar menu.



The Status page opens, as shown in the following example.



The Status settings are read-only. For details, see the following section, "Status Settings".

2. To reboot the decoder, see "Rebooting the Decoder" on page 106.
3. To display a snapshot of system information, see "Taking a System Snapshot" on page 106.

Status Settings

The following table lists the Status settings and controls. 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
Card Status	OK (or error message if applicable).
Card Type	The type of decoder, e.g., Makito2 Decoder.
Part Number	The Haivision part number for the decoder, e.g., B-292D-HD2
Serial Number	The serial number for this decoder appliance or card.
Firmware Version	The firmware version of the decoder.
Firmware Date	The firmware release date.
Firmware Options	(If applicable) Firmware options installed, e.g., SRT. For more information, see "Secure Reliable Transport (SRT)" on page 21.
Hardware Version	The hardware version of the decoder.
Hardware Compatibility	-001G (basic card assembly).
CPLD Version	The CPLD version of the decoder.
Boot Version	The Boot version of the decoder.
System Uptime	The length of time (mm:ss) the decoder has been "up" and running.
System Snapshot	Displays a snapshot of system information in a new window. See "Taking a System Snapshot" on page 106.
Reboot	Reboots the decoder. See the following section, "Rebooting the Decoder".

Rebooting the Decoder

To reboot the Decoder:

1. Click the ADMINISTRATION icon on the toolbar, and then click STATUS from the sidebar menu.
2. On the Status page, click Reboot.

   The decoder will reboot and you will be returned to the Login page. Any active streaming sessions will be momentarily disrupted.

TIP You can also reboot the decoder from other pages such as Network, Date and Time, and Policies. See "Configuring Network Settings" on page 114.

Taking a System Snapshot

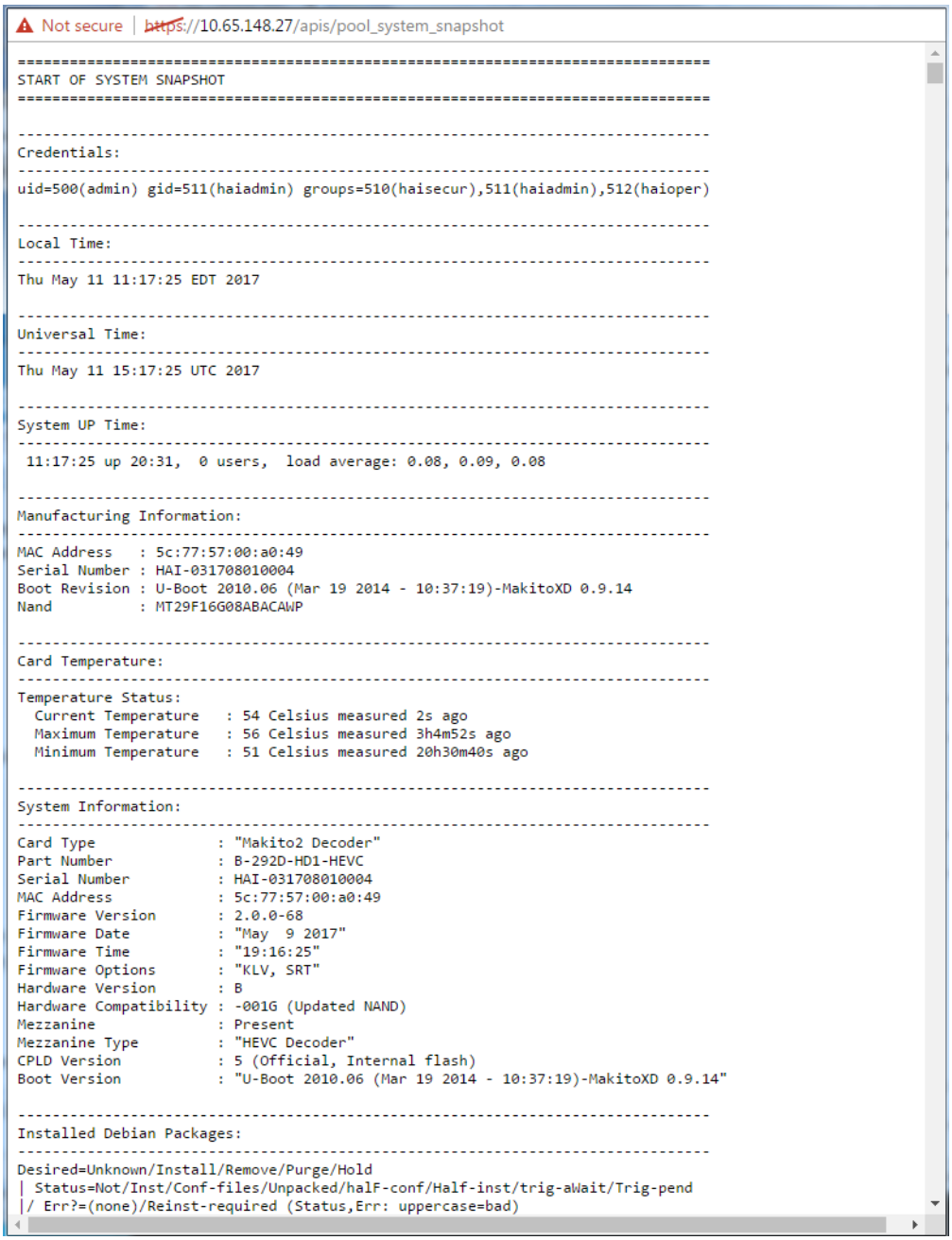
Taking a system snapshot can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

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 decoders and status checks, configured audio decoders 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.

To take a system snapshot:

1. From the Status page, click System Snapshot.

   The system will display a snapshot of system information in a new window, as shown in the example on the following page:


Not secure
https://10.65.148.27/apis/pool_system_snapshot
START OF SYSTEM SNAPSHOT
Credentials:
uid=500(admin) gid=511(haiadmin) groups=510(haisecur),511(haiadmin),512(haioper)
Local Time:
Thu May 11 11:17:25 EDT 2017
Universal Time:
Thu May 11 15:17:25 UTC 2017
System UP Time:
11:17:25 up 20:31, 0 users, load average: 0.08, 0.09, 0.08
Manufacturing Information:
MAC Address : 5c:77:57:00:a0:49
Serial Number : HAI-031708010004
Boot Revision : U-Boot 2010.06 (Mar 19 2014 - 10:37:19)-MakitoXD 0.9.14
Nand : MT29F16G08ABACAWP
Card Temperature:
Temperature Status:
Current Temperature : 54 Celsius measured 2s ago
Maximum Temperature : 56 Celsius measured 3h4m52s ago
Minimum Temperature : 51 Celsius measured 20h30m40s ago
System Information:
Card Type : "Makito2 Decoder"
Part Number : B-292D-HD1-HEVC
Serial Number : HAI-031708010004
MAC Address : 5c:77:57:00:a0:49
Firmware Version : 2.0.0-68
Firmware Date : "May 9 2017"
Firmware Time : "19:16:25"
Firmware Options : "KLV, SRT"
Hardware Version : B
Hardware Compatibility : -001G (Updated NAND)
Mezzanine : Present
Mezzanine Type : "HEVC Decoder"
CPLD Version : 5 (Official, Internal flash)
Boot Version : "U-Boot 2010.06 (Mar 19 2014 - 10:37:19)-MakitoXD 0.9.14"
Installed Debian Packages:
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)

Saving and Loading Presets

NOTE The Presets page is only accessible to administrators and operators.

Preset Management

Each Makito X is configured by users' selecting and setting values of applicable system settings, such as decoder 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 apply them to other streams.

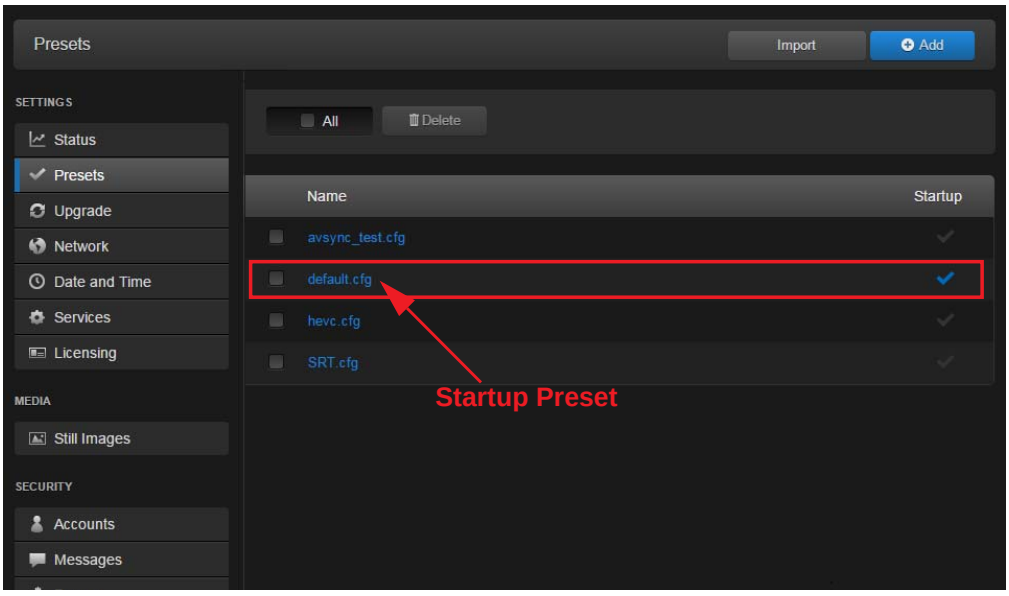
Configuration settings saved as presets will continue to be used after a reboot, or when the unit is turned off and on. You can also direct the system to apply a preset to restore settings when the system startup process performs the configuration autoload.

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.

To view and manage presets:

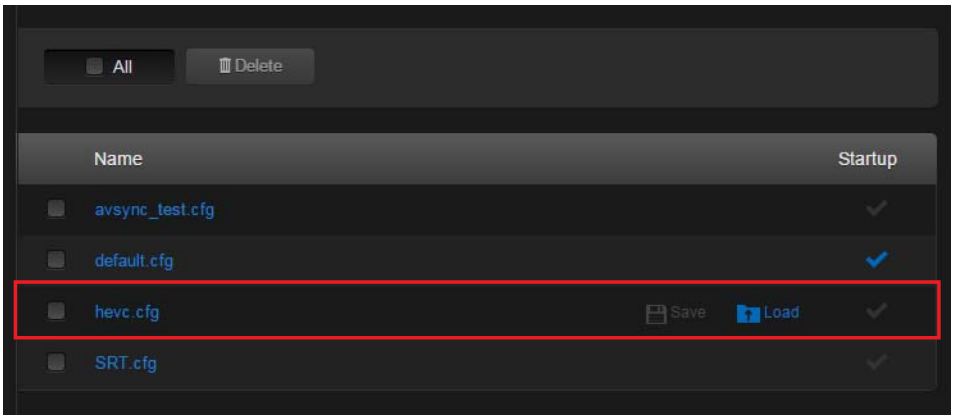
1. Click the ADMINISTRATION icon on the toolbar, and then click PRESETS from the sidebar menu.

   The Presets List View opens displaying the list of saved presets for the decoder, as shown in the following example.

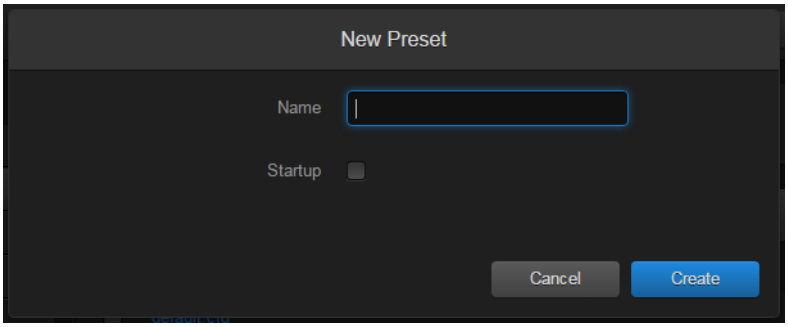


   The startup preset is indicated with a blue check.

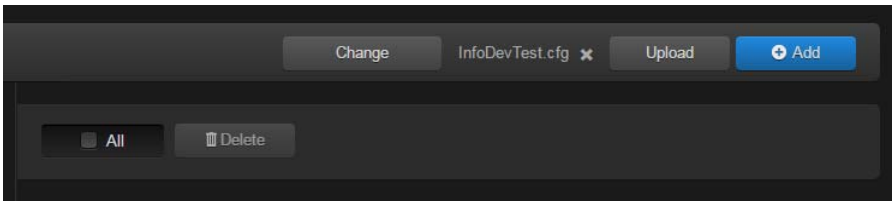
2. To load an existing preset into the current session, hover over the preset name or anywhere in the row and click Load.



3. To select an existing preset to load at startup, hover over the preset row and click the (greyed out) checkmark under Startup.
4. To save the current settings as a new preset, click Add.
   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 Apply.
5. To save the current settings as an existing preset, hover over the preset row and click Save. You can (optionally) check the Startup checkmark.
6. To save the preset as a text file to view or export to other Makito Xs, click the preset name and save it in the Save As dialog. Note that the file is in Unix format.
7. To import a preset, for example, from another Makito X, click Import and select the file in the Open File dialog box.
8. 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 .

9. To delete one or more presets, check the checkbox next to one or more preset names (or check All) and click Delete.

Installing Firmware Upgrades

NOTE The Upgrade page is only accessible to administrators.

When you first receive the Makito X, the necessary firmware is pre-installed on it. Upgrades of the firmware are issued through Haivision's Download Center on our website at: https://support.haivision.com.

Please note that you may download the latest firmware and documentation by registering via the Haivision Support Portal.

When a firmware upgrade becomes available, you can easily install it from the Web interface. You will first need to copy the upgrade file to your local computer or network.

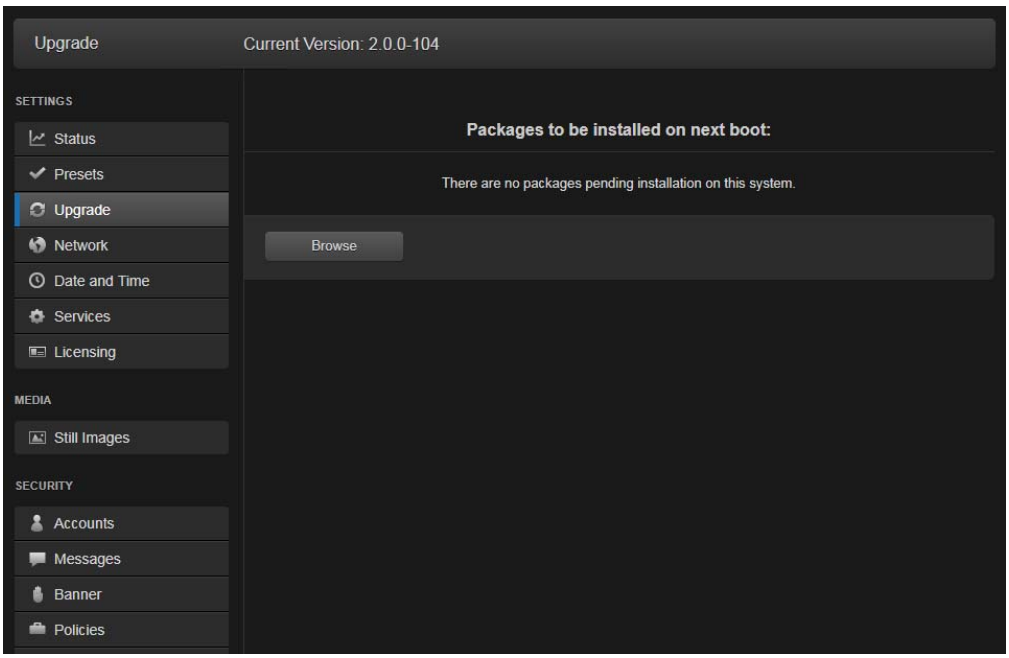
The firmware upgrade comes in the form of a file with the extension .hai, which when loaded will replace the application on your Makito X. The firmware upgrade components are digitally signed, and these signatures are all verified before performing the installation.

This section provides instructions to install a firmware upgrade from the Web interface.

To install a firmware upgrade:

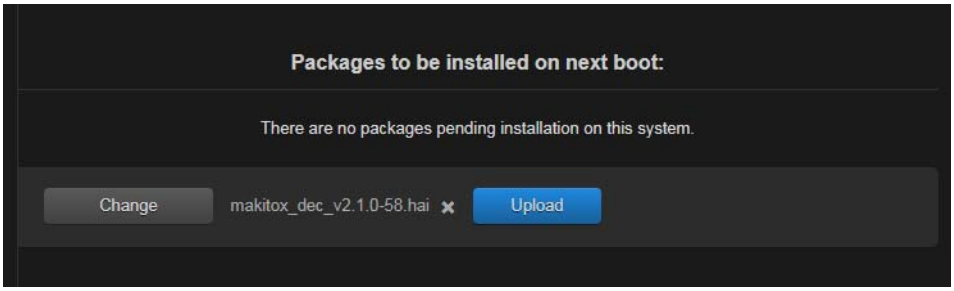
1. Click the ADMINISTRATION icon on the toolbar, and then click UPGRADE from the sidebar menu.

   The Upgrade page opens, as shown in the following example.



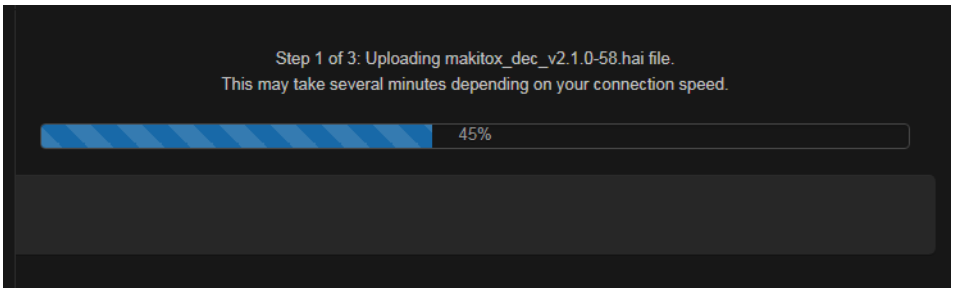
2. Click Browse and select the file in the Open File dialog box.

3. When you see the filename in the text box, click Upload.



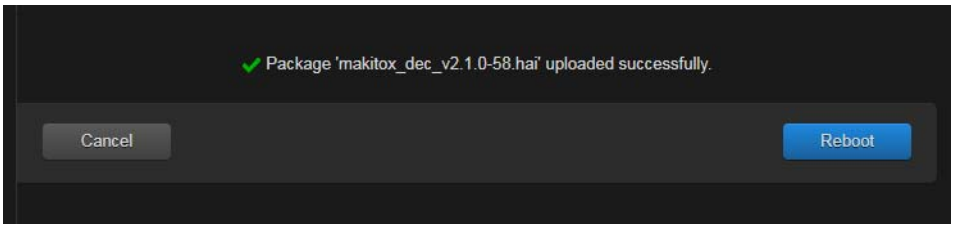
TIP To select a different file, click Change.

IMPORTANT Wait for the file to be uploaded and verified and the file system synced. Remain on this page and do *not* click anything else in the Makito X Web interface during the upload.



If any of the package components has been modified or is not signed by a valid certificate, the verification will fail and the downloaded package will be discarded.

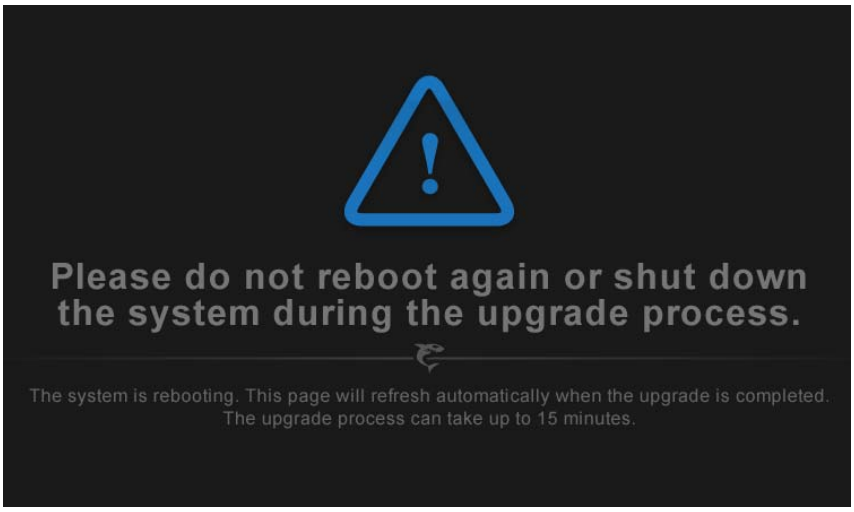
When the file is uploaded and verified successfully, you will see a confirmation page (as shown in the following example).



4. Click Reboot.

While the unit is rebooting, the Status LEDs will flash, and you will see a warning page.

CAUTION Do not proceed or shut down the system while the Status LEDs are still flashing. Failure to wait could result in damage to your system.



Once the unit has rebooted, the browser will display the Login page for the Web interface (depending on your Web browser and settings). If not, reload the Login page.

TIP It's a good idea to clear your browser cache after the firmware upgrade.

5. Log in again in order to access the decoder. For more information, see "Logging In to the Web Interface" on page 61.

NOTE You can verify the result of the installation on the Messages page.

Configuring Network Settings

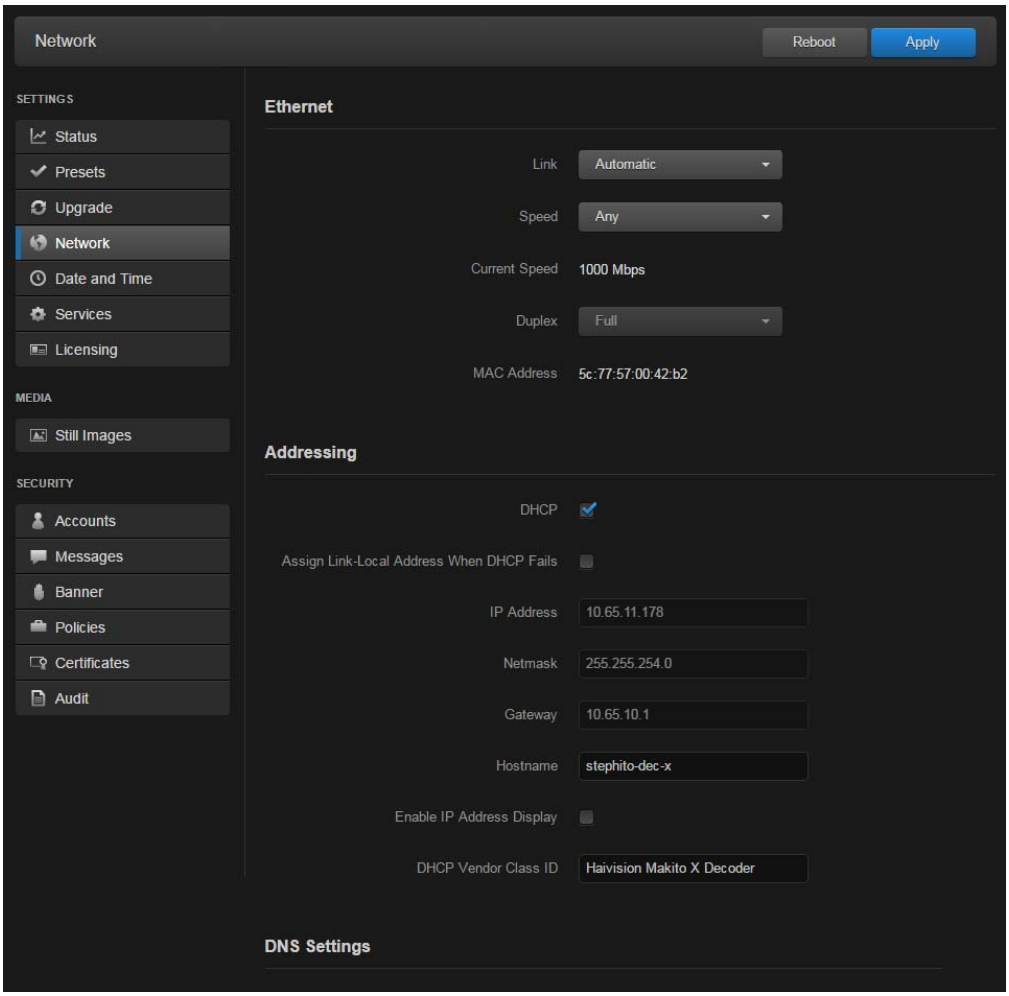
From the Network Configuration page, you can modify the network interface settings for the decoder, including the unit's IP Address.

CAUTION When you make changes to the Network settings, be sure to write down the new decoder IP Address or label the chassis. After you apply 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 decoder.

To view and configure the Network settings:

1. Click the ADMINISTRATION icon on the toolbar, and then click NETWORK from the sidebar menu.

   The Network configuration page opens, as shown in the following example.



2. Select or enter the new value(s) in the appropriate field(s). See "Network Settings" on page 115.
3. To apply your changes, click Apply.

   You must reboot the system for the changes to take effect. After the decoder reboots, you will be returned to the Login page.

Network Settings

The following table lists the Network settings:

Network Setting	Description/Values
	Ethernet
Link	Determines whether the Ethernet link settings will be negotiated automatically or configured manually: • Automatic - 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.
Speed	Select the Ethernet Speed (in Mbps): • Any (default) • 1000 • 100 • 10 NOTE: When Link is set to Automatic, setting the Ethernet speed to anything other than Any means that only that specific value will be advertised to the connected hub/switch during the negotiation process. This makes it possible, for instance, when connected to a GigE switch to force the link down to 100Mb when some network problems are encountered.
Current Speed	(Read-only) Displays the actual Ethernet Speed.
Duplex	If Link is Auto, displays the actual value for the Duplex Mode (read-only). If Link is Manual, select the Duplex Mode: • Full • Half
MAC Address	(Read-only) The Media Access Control address assigned to the Makito X.

Network Setting	Description/Values (Cont.)
Addressing	
DHCP	Check or clear this checkbox to enable or disable the Dynamic Host Configuration Protocol. NOTE: When DHCP is enabled, the decoder will get an IP Address from a DHCP server on the network. When it is disabled, you must manually enter the decoder's IP Address, Netmask & Gateway Address.
Assign Link-Local Address When DHCP Fails	(DHCP must be enabled) When this checkbox is checked, and DHCP is used but no DHCP server is present to assign an IP address to the device, the device will automatically assign itself an IP address in the 169.254.0.0/16 range. This allows you to use the device locally on a LAN (the address is NOT routable) in situations where DHCP is not available or failed.
IP Address	Displays the IP Address for the Makito X. 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.
Netmask	Displays the Subnet Mask for the Makito X. This is a 32-bit mask used to divide an IP address into subnets and specify the network's available hosts. If DHCP is disabled, you may enter a Netmask in dotted-decimal format.
Gateway	Displays the gateway address of the network (typically the address of the network router). If DHCP is disabled, you may enter a gateway address in dotted-decimal format.
Hostname	You may, optionally, enter a unique name for the Makito X.
Enable IP Address Display	Check this checkbox to display the IP address of the decoder during the boot sequence of the device. This provides a simple way for users to determine the IP address by examining the HDMI or SDI outputs on a display. The IP address is displayed as an overlay in the top left corner of the monitor.
Duration	(Enable IP Address Display must be enabled) The duration for the display of the IP address: 15, 30, 45, or 60 seconds.

Network Setting	Description/Values (Cont.)
Resolution	(Enable IP Address Display must be enabled) The resolution for the display of the IP address (default = 720p60).
DHCP Vendor Class ID	(DHCP must be enabled) You may, optionally, specify the DHCP Vendor Class ID (option 60). This allows IT departments to identify Makito X devices on their networks. The default Device Identification value for the Makito X is "Haivision Makito X Decoder".
DNS Settings	
Obtain DNS Settings Automatically	(DHCP must be enabled) Check this checkbox to obtain DNS settings from DHCP. DHCP servers often provide DNS information to the device on top of the IP address. When DHCP is enabled and this checkbox is enabled, the system will attempt to learn its DNS settings from the DHCP servers (which avoids unnecessary user configuration).
Primary DNS Server Address	(Obtain DNS Settings Automatically must be disabled) Enter the primary DNS server address for your network.
Alternate DNS Server Address	(Obtain DNS Settings Automatically must be disabled) Enter an alternate DNS server address for your network. The alternate DNS server is used only if the primary server is not responding.
Domain Name	(Obtain DNS Settings Automatically must be disabled) Enter the domain for the Makito X.
Enable mDNS	Check this checkbox to enable the Multicast DNS (mDNS) protocol as a means for third party entities to discover the IP address of the Makito X. TIP: Enabling mDNS allows an mDNS application to automatically find the decoder.
mDNS Identifier	(Optional) Enter a unique name for the decoder. By default, the system creates a unique name “MakitoXD (%HOSTNAME%)”) for the device.
Reboot	Reboots the decoder. See “Rebooting the Decoder” on page 106.

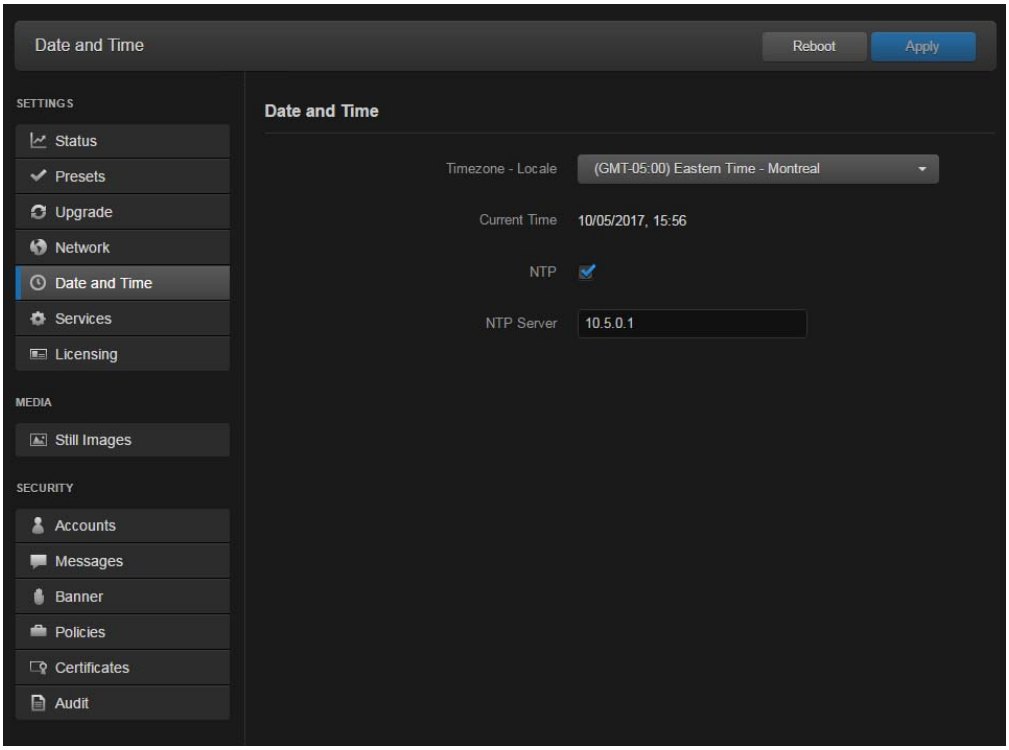
Configuring Date and Time

From the Date and Time page, you can configure Network Time Protocol (NTP) support to synchronize the decoder clock with the selected time zone.

To view and configure the date and time:

1. Click the ADMINISTRATION icon on the toolbar, and then click DATE AND TIME from the sidebar menu.

   The Date and Time page opens, as shown in the following example.



2. Select or enter the new value(s) in the appropriate field(s). See "Date and Time Settings" on page 119.
3. To apply your changes, click Apply.

Date and Time Settings

The following table lists the Date and Time settings:

Network Setting	Description/Values
Timezone-Locale	Select the desired time zone and corresponding city. NOTE: The times are based on hours added to or subtracted from Greenwich Mean Time (GMT).
Current Time	(Read-only) The current local date and time.
NTP	Check this checkbox to connect to an NTP (Network Time Protocol) server to synchronize the decoder clock.
NTP Server	If NTP is enabled, enter the IP address of the NTP server.
Manually Set Date & Time	If NTP is disabled, select the date and time from the calendar.

Enabling and Disabling Network Services

NOTE The Services page is only accessible to administrators.

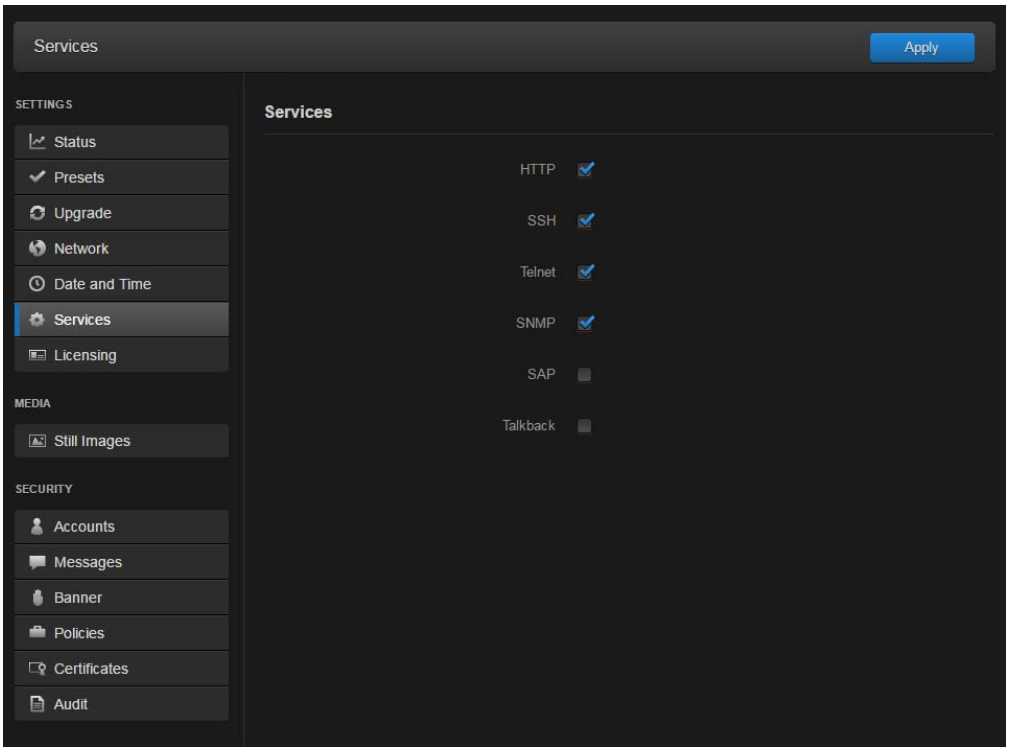
For security purposes, an administrator may need to stop one or more network services from accessing the Makito X. From the Services page, you can enable and disable the following network services: HTTP, SSH, Telnet, SNMP, SAP, and Talkback.

When SAP is enabled, you can specify the multicast IP address and port on which the device will listen for advertised sessions. The SAP service will populate the device's Streams table with the learned (i.e., announced) sessions, which users can then select as the input for the SDI 1 or SDI 2 decoders.

To enable or disable network services:

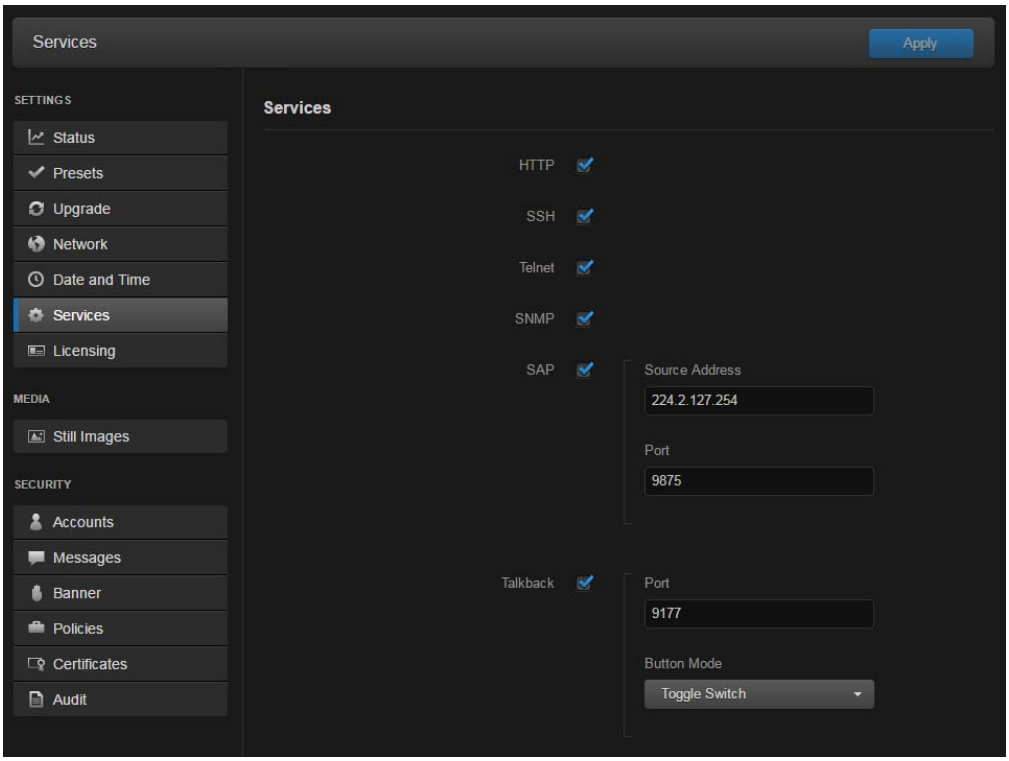
1. Click the ADMINISTRATION icon on the toolbar, and then click SERVICES from the sidebar menu.

   The Services page opens displaying the current status of network services, as shown in the following example.



2. To enable or disable a service, check or clear the associated checkbox. See the following section, "Service Settings".

3. To specify an IP address and port for the SAP service other than the defaults provided, fill in the Source Address and Port.



4. To enable Audio Talkback (to the source encoder), check the Talkback checkbox, type in the port number (if the encoder is using a different port), and select the Button Mode.

NOTE By default, the Talkback port is 9177, which is the default port used by the Makito X encoder.

5. To apply your changes, click Apply.

   The service(s) will be stopped or started immediately.

Service Settings

The configurable Services are as follows:

Service	Description
HTTP	Hypertext Transfer Protocol, used for Web browsers acting as a client. Only secured HTTP (HTTPS) is supported. See "Managing Certificates" on page 144 to manage HTTP TLS certificates.
SSH	Secure Shell, a network protocol that allows data to be exchanged using a secure channel between two networked devices.
Telnet	Telnet, a network protocol used on the Internet or local area networks to provide a bidirectional communications via a virtual terminal connection.
SNMP	Simple Network Management Protocol, a network protocol used mostly in network management systems to monitor network-attached devices.
SAP	Session Announcement Protocol, used to populate the device's Streams table with streams advertised via the SAP protocol.
Talkback	Audio Talkback (a Makito X feature) allows end users monitoring a streaming session to "talk back" to individuals at the video source (encoder), via a microphone connected to the decoder. For details, see "Audio Talkback" on page 32.
SAP only	
Source Address	Specifies the multicast IP address on which the SAP service will listen.
Port	Specifies the UDP port on which the SAP service will listen.
Talkback only	
Port	Specifies the destination port used by the encoder. Default = 9177.
Button Mode	Specifies whether the Web interface provides a push button or toggle switch for users to activate talkback. • Push Button provides "push-to-talk" functionality, which requires that users push a button to transmit audio and keep pushing the button to use the talkback channel. This prevents a user from accidentally locking and not releasing the channel. • Toggle Switch stays active until the user pushes it again.

Managing Licenses

Feature licensing allows you to add new functionality to already deployed systems. As of Version 2.1, you may add the following features to a base Makito X.

Feature	SKU
SRT	SWO-292D-SRT
KLV	SWO-292D-KLV

NOTE In the current release, the SRT and KLV licenses are included at no extra cost with each Makito X purchased.

To acquire a new license, please contact your Authorized Reseller or Haivision at: http://support.haivision.com. Indicate the appropriate feature SKU and provide the hardware serial number (or list of numbers in the case of multiple devices) to which it applies.

The license is delivered by email as a plain-text ASCII license file with the extension .lic to be installed on your Makito X.

You may install and manage licenses from the Web interface or from the CLI using the license command. Both methods allow you to view the content and status (valid/invalid) of the license file to confirm the ordered features.

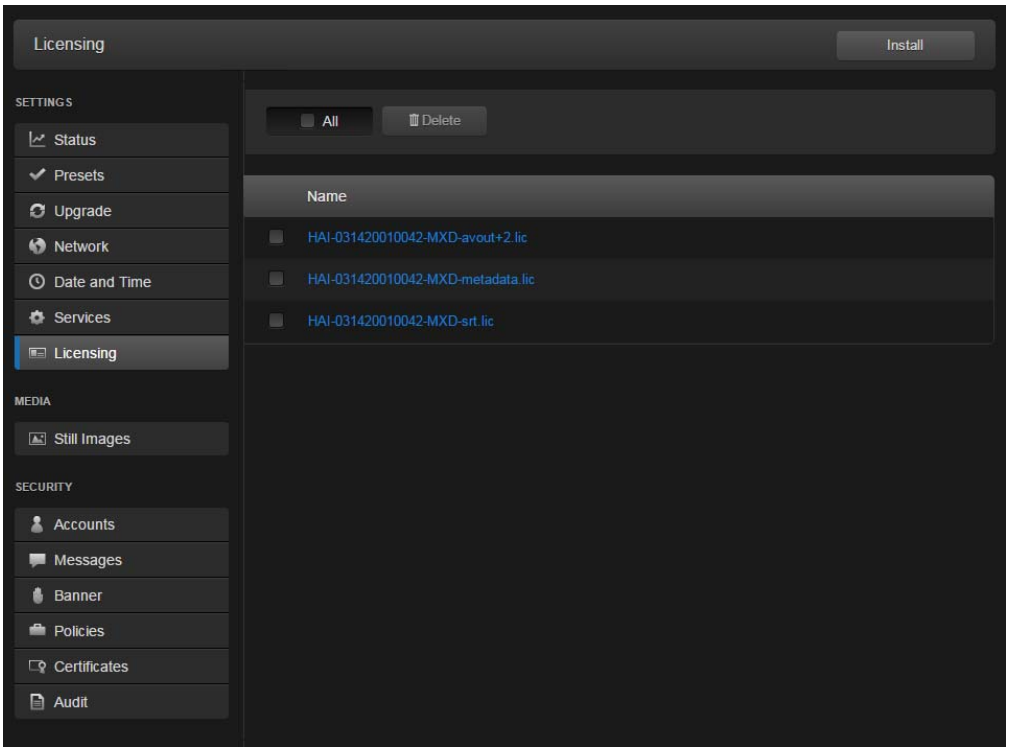
The licensing of the unit will survive a factory reset and upgrade of the firmware.

This section provides instructions to install a license from the Web interface as well as view current licenses on your system.

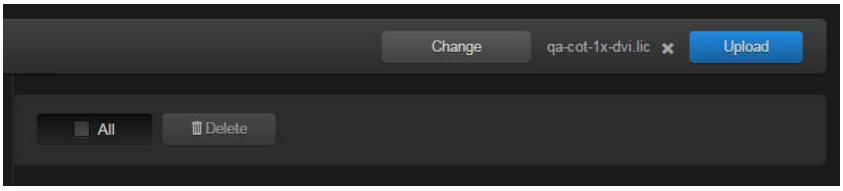
To install a license file:

1. Click the ADMINISTRATION icon on the toolbar, and then click LICENSING from the sidebar menu.

   The Licensing page opens, displaying the list of currently installed licenses (if applicable), as shown in the following example.



2. To select the license file, click Install and select the file in the Open File dialog box.
3. When you see the filename in the text box, click Upload.

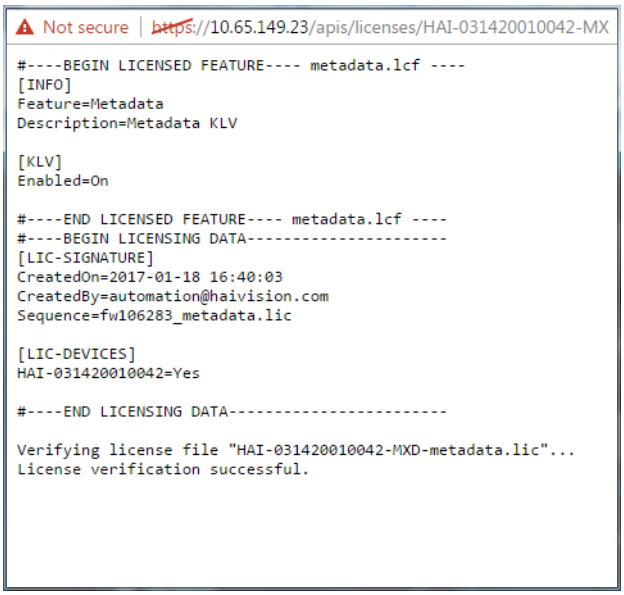


TIP To select a different license file, click Change. To remove the selection, click .

4. To apply your changes, click Reboot.

   The decoder will reboot and you will be returned to the Login page.
5. To view an installed license file, click the file in the list.

   The license file opens in a separate window (as shown in the following example).



6. To delete a previously installed license, select the file in the list and click Delete.

License File Errors

The license file signature check occurs at license installation and system startup time. The following table lists the possible validation errors.

Validation Error	Description
Unrecognized license file format or extension	The file extension or content is not recognized as a licensed features license.
Not for this device (serial number)	The current device's serial number is not specified in the license.
File integrity compromised	Invalid signature: The license file has been corrupted or altered.
File authenticity cannot be confirmed	The license signing certificate cannot be authenticated.

Configuring Still Image Streaming

From the Still Images page, you can manage the collection of custom static images that the decoder can display when there is no input stream present. Once uploaded, the custom still image can be selected from the SDI 1 and SDI 2 Decoder configuration pages.

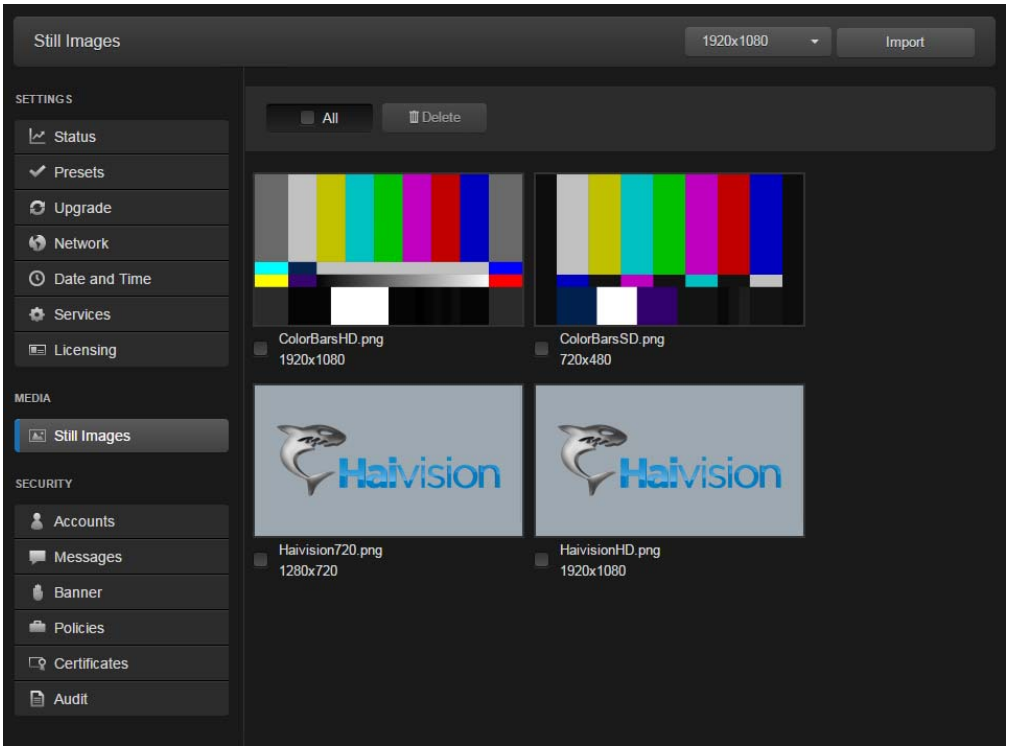
The image file formats supported are JPEG and PNG. Each decoder channel can be configured to display a different custom image.

NOTE It is not necessary to have a different version of the custom still image for every display format. The decoder automatically resizes the selected image for proper display.

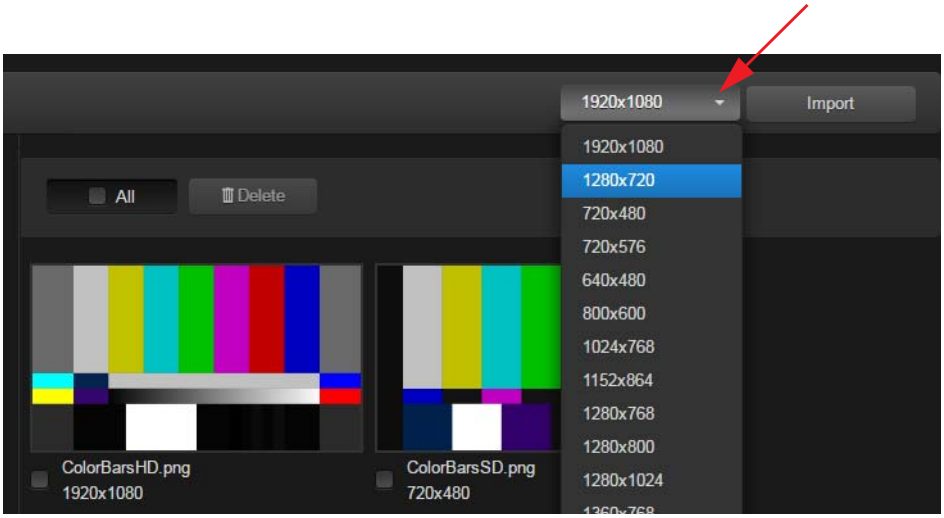
To upload a static image:

1. On the Streaming page, click STILL IMAGES from the sidebar menu.

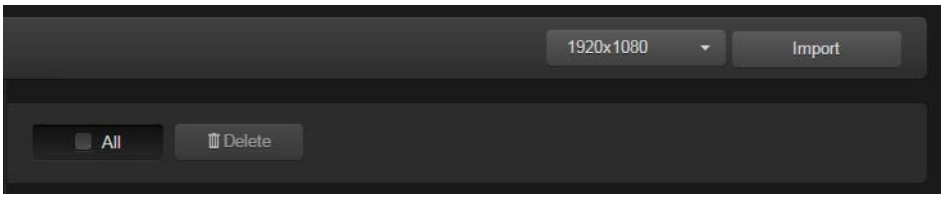
   The Still Images page opens, displaying the list of still images that have been uploaded for the decoder, as shown in the following example.



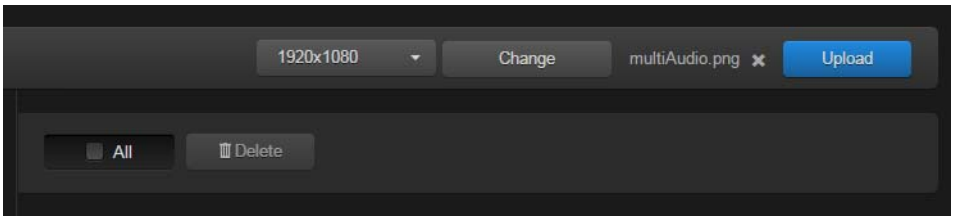
2. To upload a new image file, first select the Output Resolution for the image.



3. Click Import and select the file in the Open File dialog box.



4. When you see the filename in the text box, click Upload. x



TIP To select a different image file, click Change. To remove the selection, click .

5. To delete one or more image files from the Still Images list, check the checkbox next to one or more filenames (or check All) and click Delete on the Content toolbar.

NOTE The resulting still image files are stored on the Makito X file system in the folder /usr/share/haivision/still_images.

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 the Makito X (including their own accounts).

The My Account page is available to users assigned either Operator or Guest roles to change their own account password. For information, see "Changing Your Password" on page 65.

From the Accounts pages, administrators can create, delete and modify user accounts for the Makito X.

An account can be allocated to each user of the system so that the identity of the user can be uniquely determined. The Makito X provides three defined account roles to assign privileges to users: Administrator, Operator and Guest. For details, see "Role-based Authorization" on page 59.

Using system-wide parameters, administrators can configure the allowable password strength and composition (i.e., to force the selection of strong passwords), as well as the periodic change of passwords. For details, see "Managing Password Policies" on page 140.

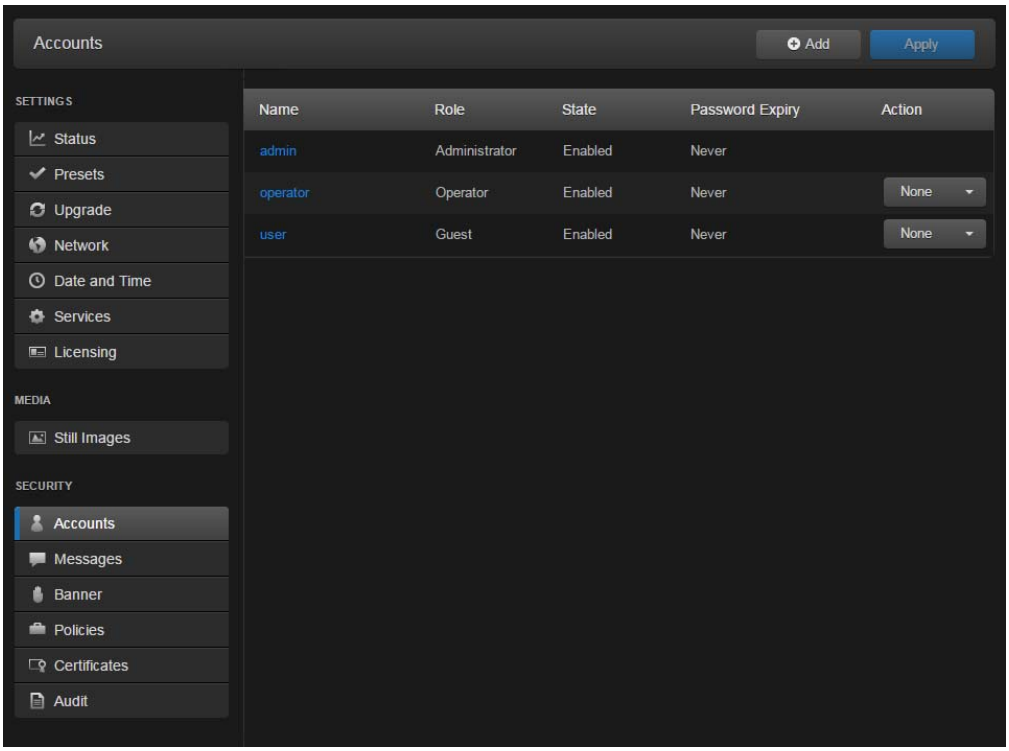
The Makito X can also be configured for Web interface and CLI account sessions to log out after an idle session timeout period. The session timeout period is selectable via a system-wide parameter. For details, see "Managing Password Policies" on page 140.

From the Account Settings pages, administrators can also upload and manage personal public keys for accounts to enable public key authentication (instead of password-based authentication). Note that in the current release, this only applies to SSH CLI access to the decoder.

To open the Accounts List View:

1. Click the ADMINISTRATION icon on the toolbar, and then click ACCOUNTS from the sidebar menu.

   The Accounts List View opens, displaying the list of defined user accounts for the decoder, as shown in the following example.



The Accounts List View displays the Name, Role, State (Enabled or Locked), and Password Expiry status for each account. It also provides an option to lock/unlock or delete an account.

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" on page 130.
3. To add a new account, click Add. For details, "Account Management" on page 130.
4. To lock or unlock an account, click the drop-down list under Actions and select either:
   - Lock (if the current State is Enabled) or
   - Unlock (if the current State is Locked).
5. To delete an account, click the drop-down menu under Actions and select Delete.
6. To apply your changes, click Apply.

   The changes will take effect immediately.

Account Management

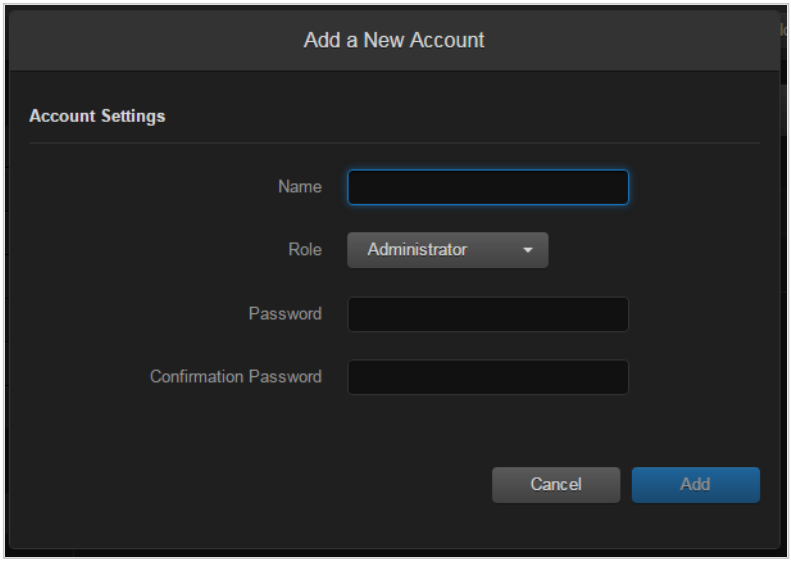
TIP It is recommended to set the Policies for your system before creating users.

The Password Policies do not apply to administrators creating user accounts or setting passwords for accounts other than their own.

To add a new account:

1. From the Accounts List View, click Add.
2. In the Add New Account dialog, type a unique user name in the Name text box.

TIP The user name must comply with Unix restrictions (lower case letters a-z, numbers 0-9, hyphen and underscore).

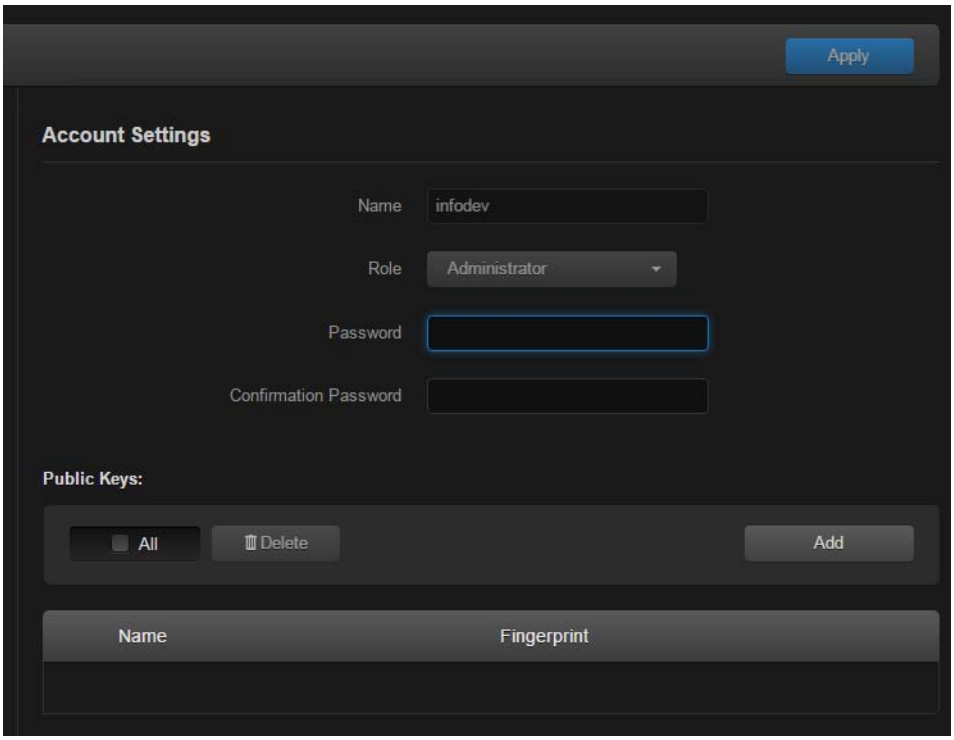


3. Select the Role for the user. See "Role" on page 132.
4. Type the initial password in the Password field and again in the Confirmation Password field. For the allowed characters, see "Password Requirements" on page 66.
5. Click Add.

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).



   For security purposes, you cannot modify the Name or Role for an existing account.

2. To reset the password of an existing account, type the password in the Password field and again in the Confirmation Password field. For the allowed characters, see "Password Requirements" on page 66.

3. To change your own password, type the current password in the Old Password field, type the new password in the Password field and again in the Confirmation Password field.

NOTE New users must change their passwords the first time they log in as well as when the administrator resets the password of an existing account.

When you change your password, the new password will take effect immediately.

---

4. To upload a public key for the account, follow the steps in "Managing Public Key Authentication" on page 133.

5. To get the fingerprint for a public key, select the public key in the list.

For more information, see "Account Settings" on page 132.

6. 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, meeting the following requirements: • Maximum length = 20 characters. • All characters must be lowercase. • The first character cannot be a number. - Can start with [a-z] - After the first character, can contain [a-z 0-9]
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 • Guest For details on roles, see "Role-based Authorization" on page 59.
Old 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.
Password	n/a	Type in the new password. For the allowed characters, see "Password Requirements" on page 66.
Confirmation password	n/a	Re-type the new password.

Account Setting	Default	Description/Values (Cont.)
Public Keys	n/a	Lists any public key files that have been uploaded for this account. • To add a public key, click Upload. • To delete a public key, select it from the list and click Delete. See "Managing Public Key Authentication" on page 133.
Fingerprint	n/a	Displays the fingerprint for the selected public key (when you click a filename in the Public Keys list). TIP: A public key fingerprint is a short sequence of bytes which you can copy and use to identify or look for a public key.

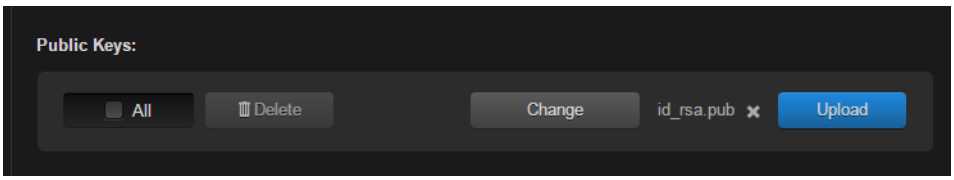
Managing Public Key Authentication

In order to use a public key for account authentication (instead of password-based authentication), you must first get the public key of your SSH client. Note that in the current release, this only applies to SSH CLI access to the decoder.

To upload a public key file for an account:

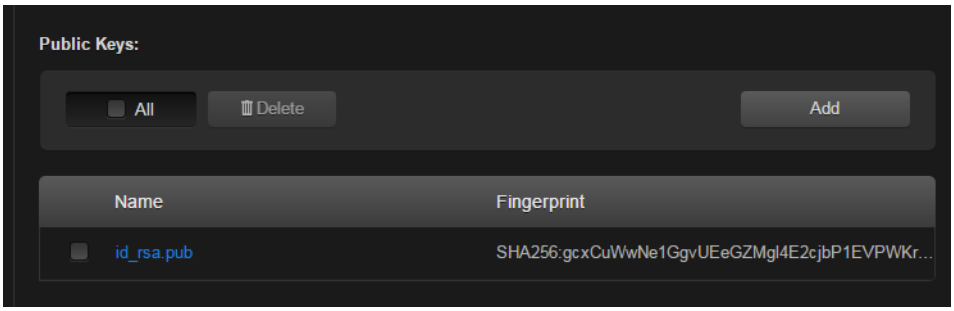
1. From the Accounts List View, click a link in the table for an existing account.
2. On the Account Settings page, under Public Keys, click Add and select the file in the Open File dialog box.

   The public key file must have a .pub extension.
3. When you see the filename in the text box, click Upload.



TIP To select a different public key file, click Change. To remove the selection, click .

The file is then added to the list of public keys along with the fingerprint for the key (e.g., for identification purposes, as shown in the following example).



4. To delete one or more previously uploaded public key file from the list, check the checkbox next to one or more filenames (or check All) and click Delete.

TIP You can now access the CLI interface from you SSH client without providing your account password. You may have to provide a password to decrypt your private key but this is done by your SSH client. If you no longer use password-based authentication to access your account, it is recommended to set a very long password.

Managing Messages

The Messages page displays a limited number of important administrator actions recorded such as installation of a software package, failure to establish or maintain connectivity with a remote syslog server, Power-On Self Test (POST) errors, and other noteworthy events.

These events will result in a message being displayed at the next administrative Web interface or CLI login.

The log of the actions recorded includes the following:

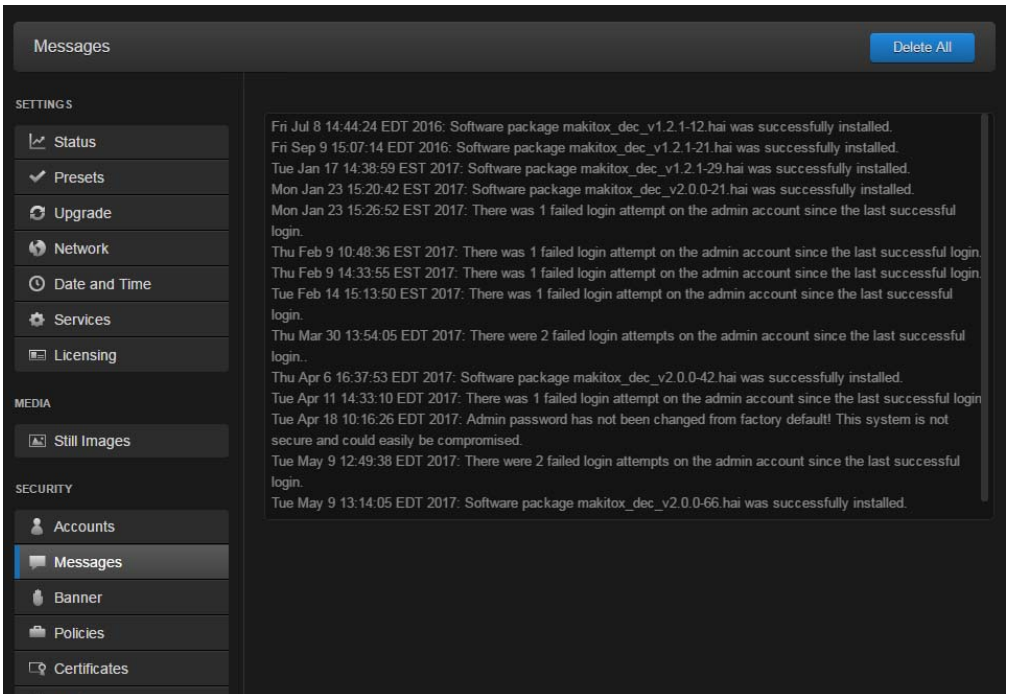
- The user initiating the action and the action being initiated.
- The time of the action.
- The results of the action (success/failure).

NOTE Messages starting with “POST” are Power-On Self Test events. If you repeatedly get POST errors, the cryptographic module of the decoder may be compromised, and it is recommended to re-installed the firmware.

To view the messages:

1. Click the ADMINISTRATION icon on the toolbar, and then click MESSAGES from the sidebar menu.

   The Messages page opens displaying the log as shown in the following example.



2. To delete the messages, click Delete All.

   The messages will be deleted immediately.

Managing Banners

NOTE The Banner page is only accessible to administrators.

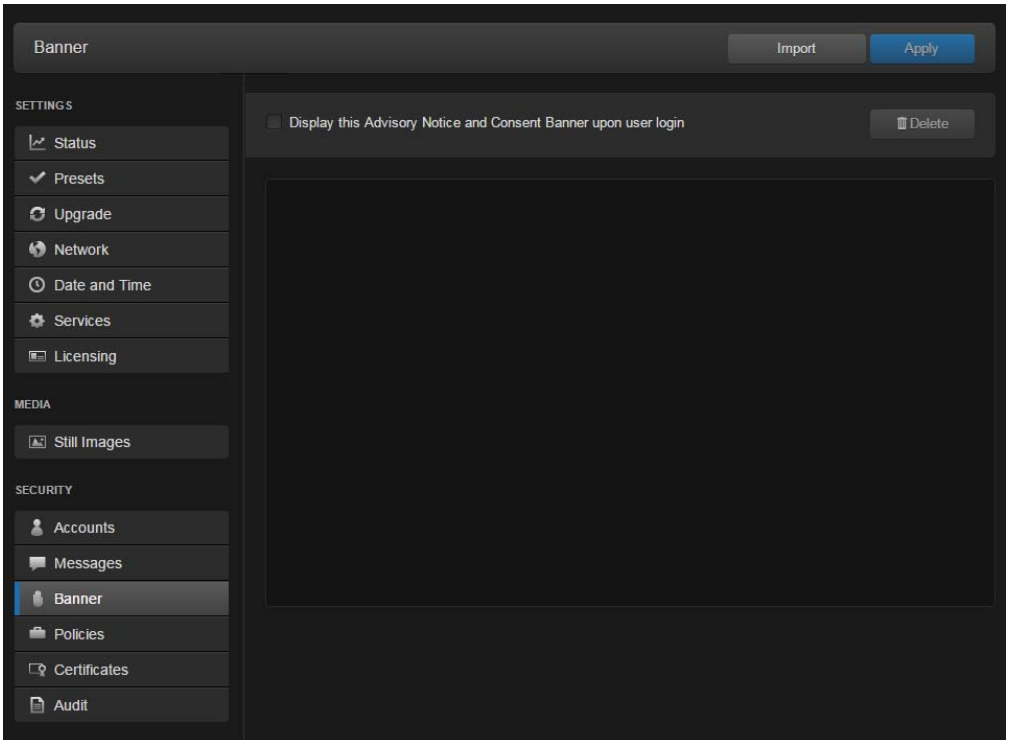
From the Banner page, administrators can upload a text file for the Advisory and Consent Banner page. The banner is typically an advisory/warning notice to be displayed before the Login page.

Only ASCII file format is supported for the banner file; the banner is a single text file with a maximum file size of 4KB.

To upload a text file for the Banner page:

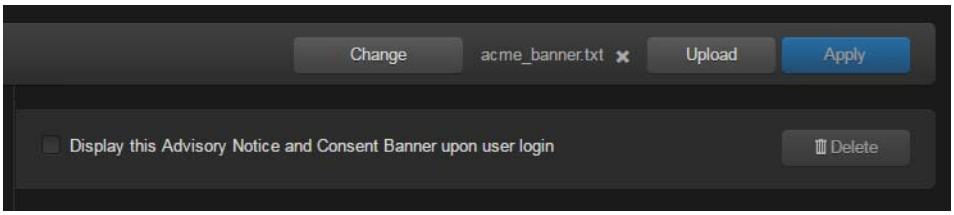
1. Click the ADMINISTRATION icon on the toolbar, and then click BANNER from the sidebar menu.

   The Banner page opens, as shown in the following example. If banner text has been imported, it will be displayed here.



2. Click Import and select the file in the Open File dialog box.

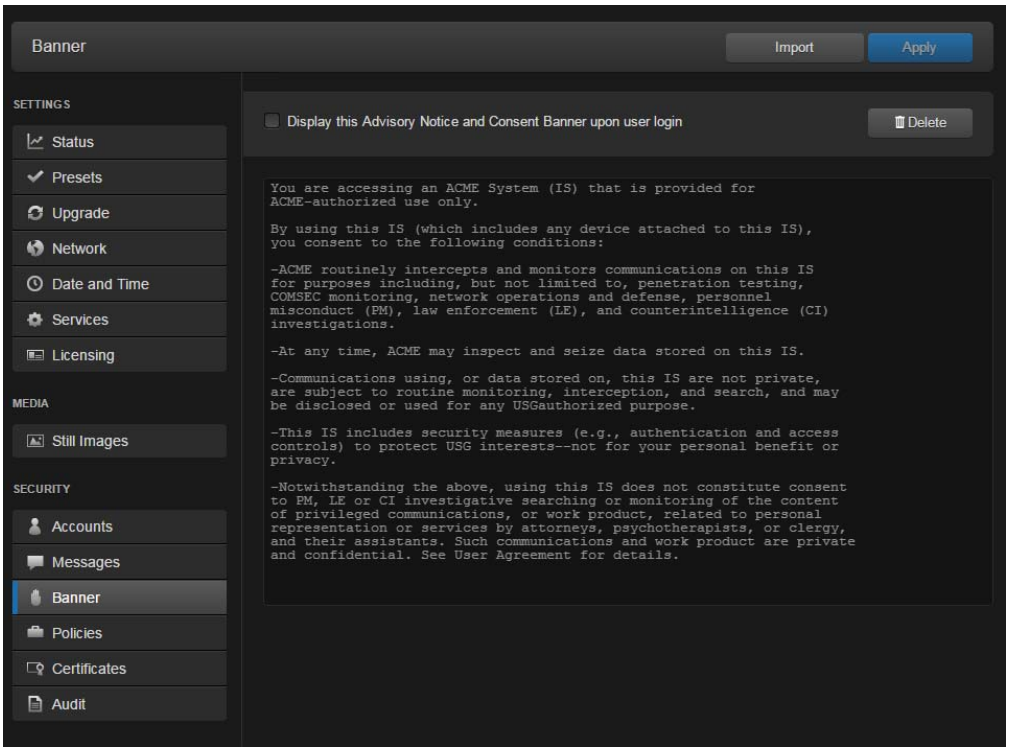
   The banner filename is now displayed on the Upload Banner task bar.



TIP To select a different banner file, click Change. To remove the selection, click .

3. Click Upload.

   The banner text is now displayed in the pane.



4. To display the Advisory Notice and Consent Banner upon user login, check the checkbox.

NOTE When the banner is enabled, the time when the banner actually gets displayed may vary with the service in use (such as SSH, Telnet, serial port, or Web interface) and how the services are configured. For example, in some cases, the banner will be displayed right after the login and before the password is entered, whereas with the Web interface, the banner will be displayed before the user gets to the Login page.

5. To apply your changes, click Apply.
6. To delete the current banner, click Delete.

   The banner will be deleted immediately.

TIP You can also install and manage banner files from the CLI using the banner command. The Makito X supports FTP and TFTP client, as well as SCP client and server.

Managing Password Policies

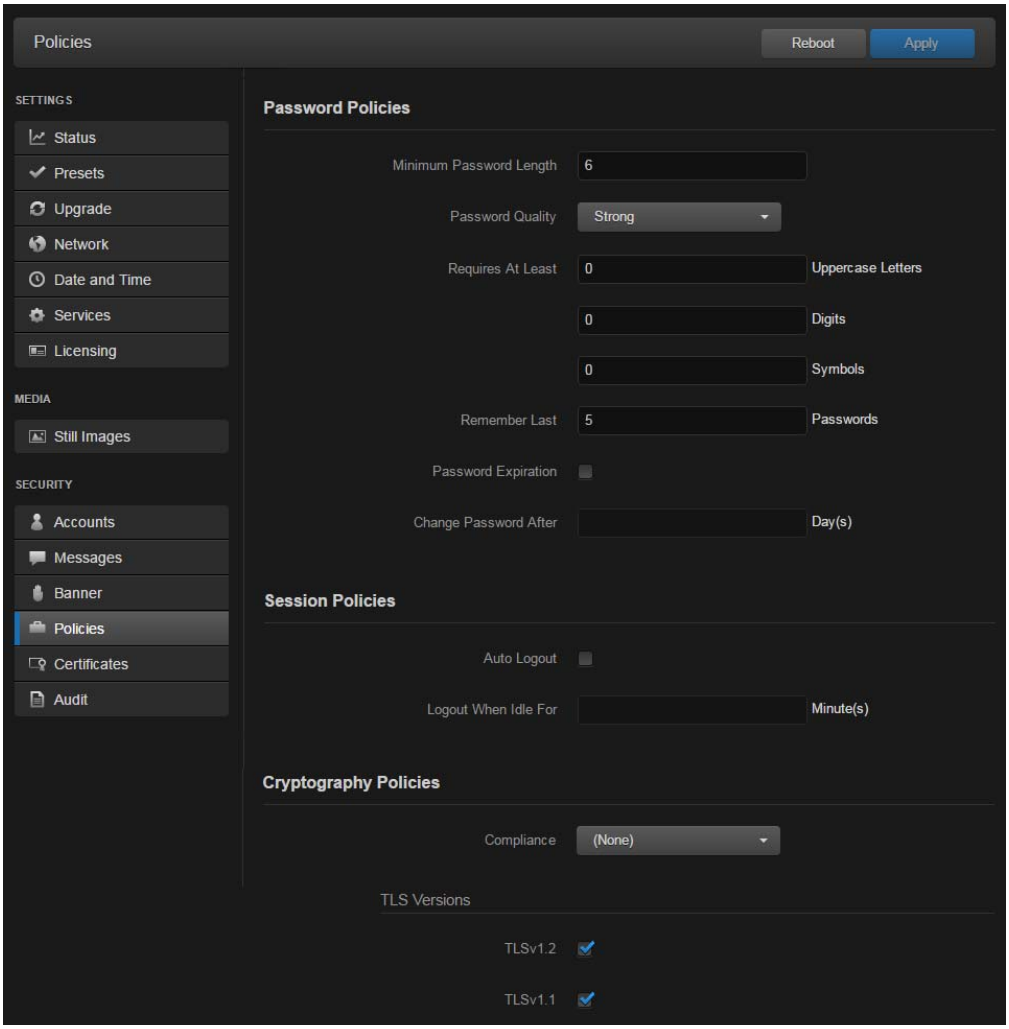
NOTE The Policies page is only accessible to administrators.

From the Policies page, administrators can set policies for passwords, session timeout, and cryptographic strength for Makito X user accounts. These policies will apply to all user accounts; therefore, it is recommended to set the policies before beginning to create accounts.

To view and manage the password policies for the decoder:

1. Click the ADMINISTRATION icon on the toolbar, and then click POLICIES from the sidebar menu.

   The Policies page opens as shown in the following example.



2. Select or enter the new value(s) in the appropriate field(s). See "Policy Settings" on page 141.
3. To apply your changes, click Apply.

Policy Settings

The following table lists the Policy settings for the decoder:

Policy Setting	Default	Description/Values
Password Policies		
Minimum password length	6 characters	Type in the minimum password length (from 6-40 characters). NOTE: Passwords can be up to 80 characters.
Password quality	Basic	Select the required password quality; works in conjunction with Password requires at least below: • Basic: Sets the minimum password length as the only requirement to accept a new password. • Strong: Adds more strict requirements to the password structure. Checks for minimum length as well as other criteria such as minimum number of required upper case characters, digits, and symbols.
Password requires at least	0	(Password quality must be Strong) Specify the minimum required number of: • uppercase letters • digits • symbols The range is from 0 to 40 for all 3.
Remember Last	5	(Password quality must be Strong) This option determines the number of unique new passwords that must be associated with a user account before an old password can be reused. The range is from 5 to 500.
Password expiration	Disabled	To enable Password expiration, check the checkbox.

Policy Setting	Default	Description/Values (Cont.)
Change password after	n/a if Disabled ---------- 90 days if Enabled	(Password expiration must be enabled) Type in the number of days after which users must change their passwords (from 1-180 days).
Session Policies		
Auto Logout	Disabled	To enable Auto Logout, check the checkbox. This configures the Makito X to automatically log the user out after a specified period of idle time. Systems that are left logged on may represent a security risk for an organization. If the user has been inactive for longer than this period of time, he/she will be automatically logged out and redirected to the Login page.
Logout when idle for	n/a if Disabled _____ 15 minutes if Enabled	(Auto Logout must be enabled) Type in the maximum length of time the system may be idle before the user will be logged out (from 1 - 1440 minutes).

Policy Setting	Default	Description/Values (Cont.)
Cryptography Policies		
Compliance	None	Specifies the required cryptographic compliance, either: • None • FIPS 140-2: All management cryptography is operated in the FIPS 140-2 mode. • NDPP v1.1: Activates cryptographic security to a level compliant with the Network Device Protection Profile v1.1. • SP800-52 Revision 1: Applies cryptographic modules accredited under the National Institute of Standards and Technology (NIST) Special Publication 800-52, Revision 1. NOTE: Either selection will reinforce security for all management functions of the decoder in terms of cryptography. This setting will take effect upon the next reboot.
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 • SSLv3 NOTE: NOTE: SSLv3 can be enabled only if Compliance is set to None. At least one TLS version must be enabled.

Managing Certificates

NOTE The Certificates page is only accessible to administrators.

The Certificates page shows the list of Identity and CA Certificates installed on the Makito X.

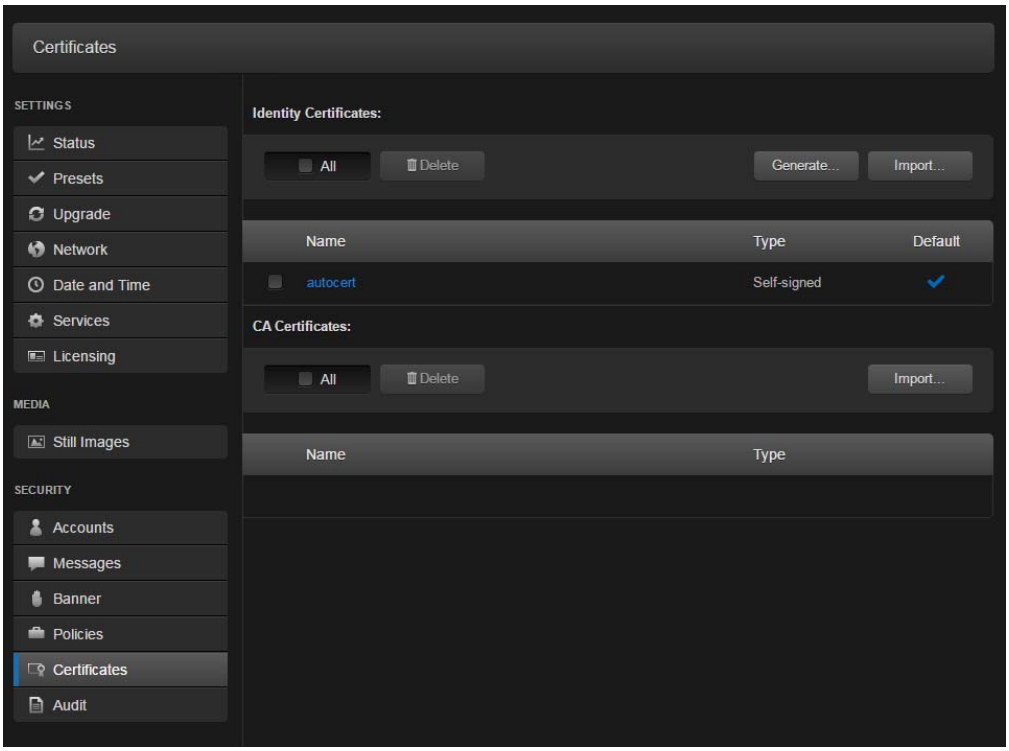
- Identity Certificates: An Identity Certificate identifies the Makito X during the authentication process when trying to establish a TLS connection in Audit or HTTPS session startup. Its Common Name or Alternate Subject Names must match the decoder's IP address and/or its FQDN (Fully Qualified Domain 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 decoder 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 Makito X identity certificate in order to increase your list of trusted root certificates.

From the Certificates page, you can generate, import, view, and delete Identity Certificates, as well as select the default Identity Certificate. You can also import, view, and delete CA Certificates.

To open the Certificates page:

1. Click the ADMINISTRATION icon on the toolbar, and then click CERTIFICATES from the sidebar menu.

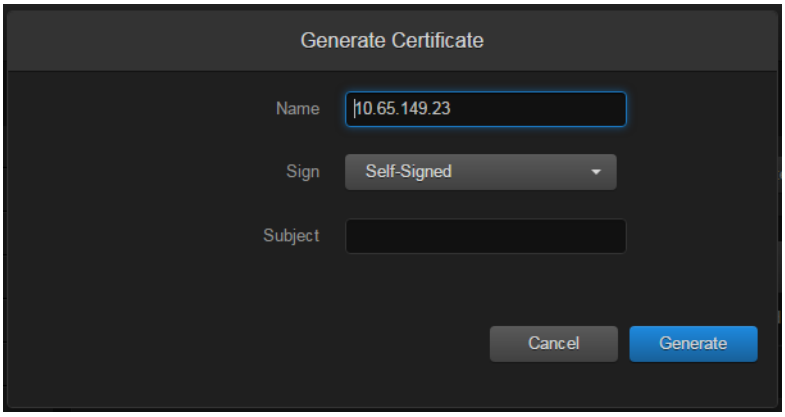
   The Certificates page opens as shown in the following example.



The default Identity Certificate is indicated with a blue check.

To generate a Certificate Signing Request:

1. On the Certificates page, click Generate.
2. (Optional) Type a name for certificate in the Generate Certificate dialog.



3. Select either Self-signed or Certificate Signing Request from the drop-down list.

   For more information, see "Sign" on page 149.

4. For the subject, type in information about the device that the Identity Certificate represents.

   For more information, see "Subject" on page 150.

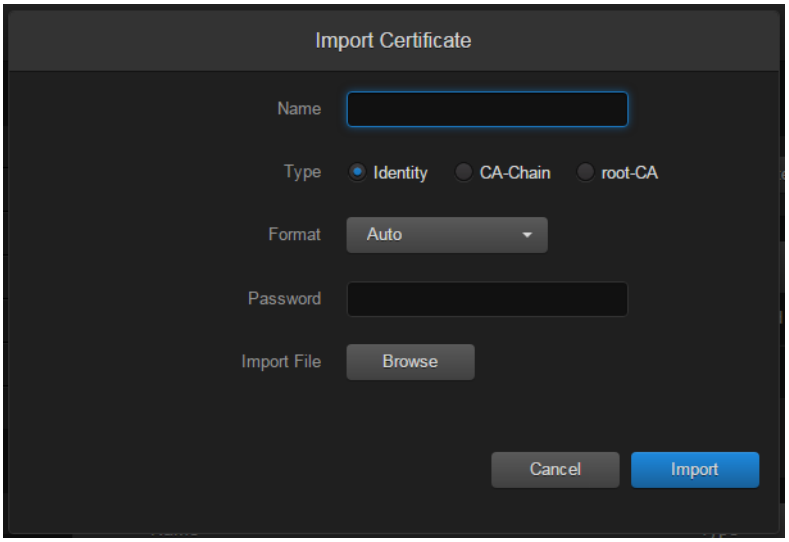
5. Click Generate.

   If the 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 it back later by clicking on the Import button (using the same name as the request).

TIP Keep in mind that there is a difference between importing a new certificate (that was generated externally) and importing a newly signed certificate whose request was previously generated on the Makito X and exported for signing. For details, see "Certificate Name" on page 150.

To manage Certificates:

1. To import a Certificate, click Import next to either the Identity Certificates or CA Certificates section.



   a. Type in the Certificate Name.

   b. Select or enter the new value(s) in the remaining field(s). See "Import Identity or CA Certificate dialog" on page 150.

   c. Click Import.

2. To view the details of a certificate, select the certificate name from either the list of Identity Certificates or CA Certificates. (See "Viewing Certificate Details".)

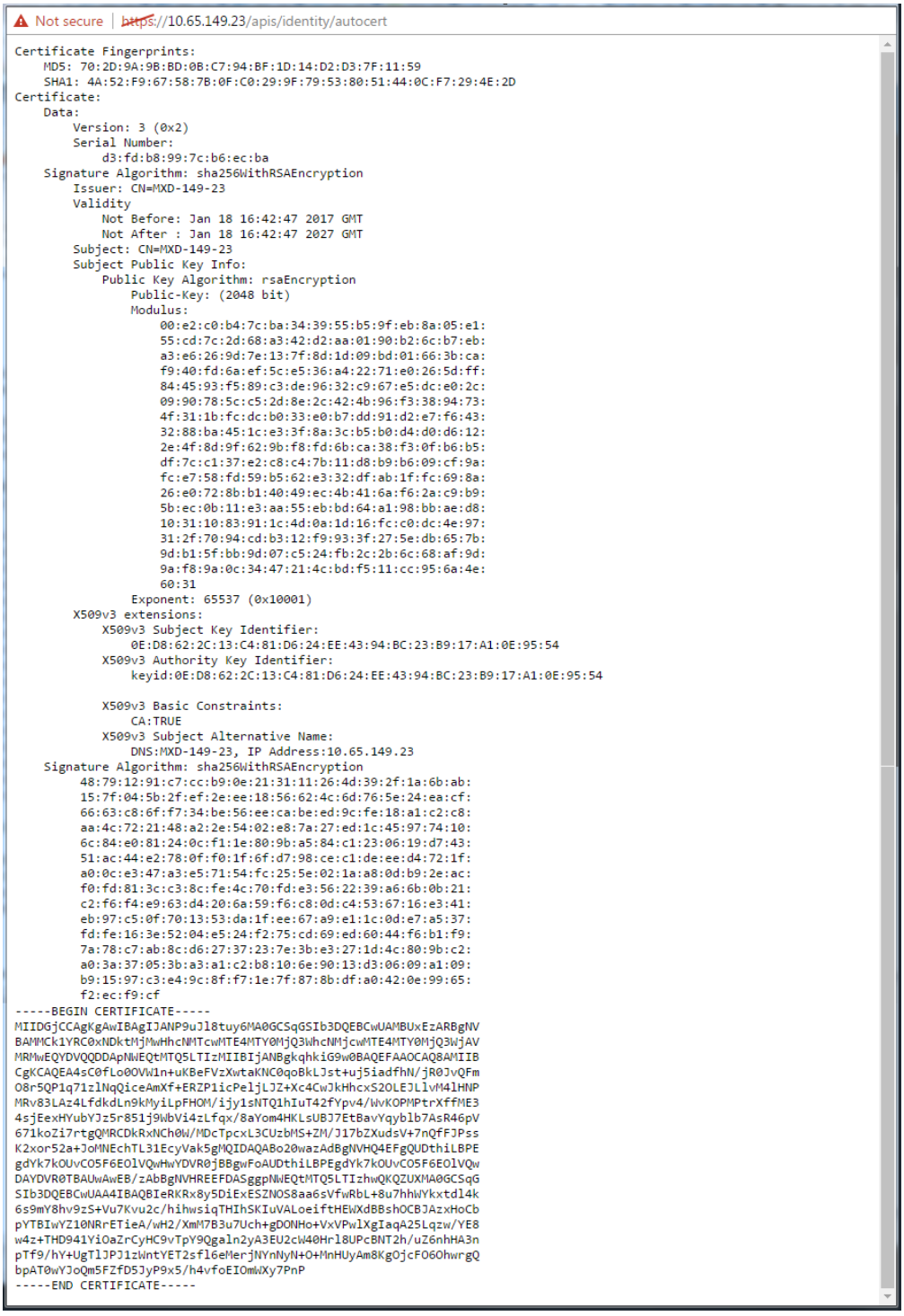
3. To delete a certificate file, select the certificate name from the list of Identity or CA Certificates and click Delete.

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 (greyed out) checkmark under Default.

   The selected certificate will be saved as the default certificate, and its effect will be directly applied to the Audit but does not apply to HTTP until the next service restart or system reboot.

Viewing Certificate Details

1. To view the details of a certificate file, select the certificate name from the list of Identity Certificates. (See following example.)



Certificate Settings

The following table lists the Certificates controls and settings:

Certificate Setting	Default	Description/Values
Generate...	n/a	Click to generate a Certificate Signing Request. See "To generate a Certificate Signing Request:" on page 145.
Import...	n/a	Click to import an Identity or CA Certificate. See "To manage Certificates:" on page 146.
Delete	n/a	Click to delete the selected Identity or CA Certificate. See "To manage Certificates:" on page 146.
Generate Identity Certificate dialog		
Certificate Name	n/a	Type in a unique name under which the certificate will be stored on the Makito X as well as listed on the Certificate page.
Sign	Self-signed	Select the Signature Type: • Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates. • Certificate Signing Request: A request will be generated, and its name will be added to the list of Identity Certificates. The request will be located in your home directory (accessible through the CLI), or you may export it by clicking on the View button and copying the content into a new file in a text editor. In its generated form, this certificate is still a request and cannot be used as an Identity Certificate before it is signed by a CA, and imported back.

Certificate Setting	Default	Description/Values (Cont.)
Subject		The Subject identifies the device being secured, in this case, the Makito X. The special value “auto” used with Generate sets the Subject Common Name to the device’s FQDN if DNS is set, or the IP address otherwise. Also, for self-signed certificates, the Subject Alternative Name extension is also set to FQDN, hostname, and IP Address of the device (there is no other method to set the Subject Alternative Name). Type in the subject in the form: "/C=US/ST=Maine..." where the most common attributes are: • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name TIP: For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device.
Import Identity or CA Certificate dialog		
Certificate 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 Makito X, 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.

Certificate Setting	Default	Description/Values (Cont.)
Type	Identity (Identity Certificates) ---------- root-CA (CA Certificates)	Select the type of the imported certificate: • Identity: If you are importing an identity certificate. • CA-Chain: If the import is a chain of certificate authorities leading to the root certificate authority. The imported CA-chain can contain one or more certificates linking its associated identity certificate to the root-CA and may or may not include the root-CA itself (that will only be trusted if imported as a root-CA). • root-CA: If you are importing a root CA certificate.These certificates are the anchor of trust of the certificate authorities you decide to trust and are generally publicly available from the CA Web sites. They are used by the device when validating the chain of trust of an identity certificate and its CA-chain. NOTE: Even though you can see the Type buttons, clicking Import in either the ID or CA sections may cause error messages to be displayed, i.e.: • If you select CA-root in the import from the ID. • If you select Identity or CA-chain in the import from the ca-root.
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 • pem: Privacy Enhanced Mail Base64 encoded DER certificate • der: Distinguish Encoding Rules • pkcs #7 • pkcs #12 • pfx

Certificate Setting	Default	Description/Values (Cont.)
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.
Import File	n/a	Click Choose File to select the file.

Managing Audits

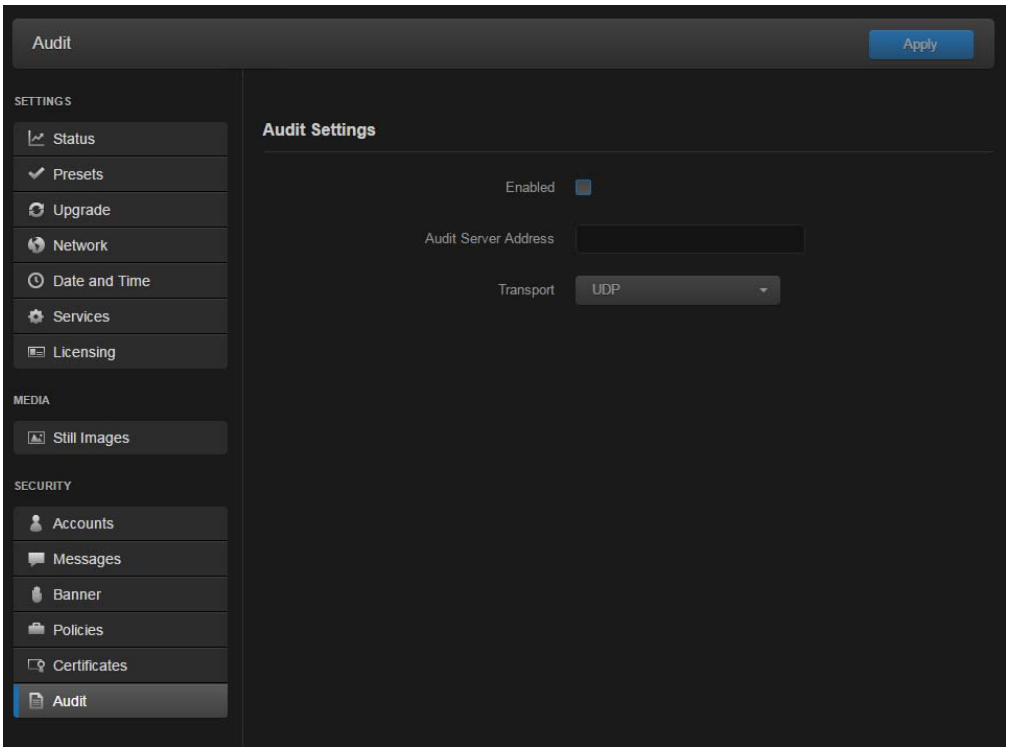
NOTE The Audits page is only accessible to administrators.

From the Audits page, administrators can set up logging to an Audit server for the Makito X.

To configure an Audit server:

1. Click the ADMINISTRATION icon on the toolbar, and then click AUDIT from the sidebar menu.

   The Audit page opens as shown in the following example.



2. Check the Enable Audit checkbox to start logging to the audit server.
3. Type the audit server address and port in the Audit Server Address field. See "Audit Settings" on page 154 for more details.

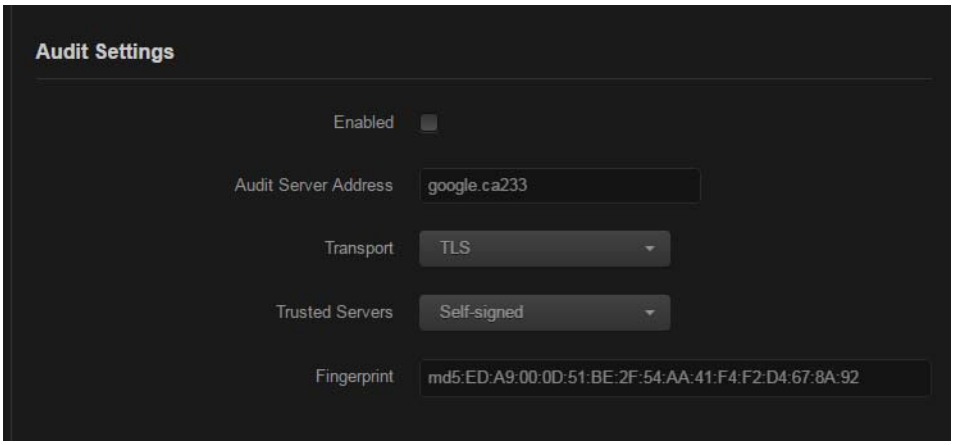
   The server address must be the Common Name or one of the Subject Alternative Names in the server's certificate for successful authentication if TLS and CA-signed trusted server is set.

4. Set the type of transport protocol that will be used to send the logs to the audit server. See details in "Audit Settings" on page 154.

5. If TLS is selected as Transport, choose the type of audit server to be accepted as a trusted server: either All (no server authentication), CA-signed, or Self-signed.

   If Trusted Servers is set to CA-signed, the root-CA certificate of the audit server certificate chain must be imported in the decoder (see "Managing Certificates" on page 144) for the TLS connection to succeed.

6. If Trusted Servers is set to Self-signed, fill in the Fingerprint field to identify the certificate trusted for this TLS connection.



   The fingerprint should be that of the certificate that belongs to the audit server which was set in "Audit Server Address".

7. To apply your changes, click Apply.

Audit Settings

The following table lists the Audit controls and settings:

Audit Setting	Default	Description/Values
Enable Audit	disabled	Check or clear this checkbox to enable or disable audits for the system.
Audit Server Address	n/a	Type in the address and port of the remote server, in one of the following formats: • fqdn[:port] • ipaddr[:port] • hostname[:port] If the port is not provided, the default port for the chosen transport will be used:

Audit Setting	Default	Description/Values (Cont.)
Transport	UDP	Select the Transport Type from the drop-down list: • UDP (default port: 514) • TLS (Transport Layer Security, default port: 6514)
Trusted Servers	ALL	(TLS must be selected for Transport). Select the type of certificate exchange: • All: Server authentication is disabled. Any server that is set in the Audit Server Address field will be accepted as a trusted server, and the authentication step is skipped. • CA-signed: Enables server authentication during the startup of audit. The decoder will only accept connection with the set server if its presented certificate is signed by a trusted Certificate Authority (i.e., The certificate of that certificate authority is present in the Makito X's CA Certificates list). • Self-signed: Enables server authentication. The set server will be accepted if its certificate is self-signed, but its fingerprint matches the one configured on the Makito X.
Fingerprint	n/a	(Only appears if Self-signed is selected for Trusted Servers) Enter the certificate fingerprint of the server certificate. The fingerprint should be the SHA-1 or MD5 fingerprint of the certificate that belongs to the audit server which was set in Audit Server Address.

CHAPTER 6: Configuring A/V Services Using SNMP

This chapter provides information required to manage the Makito X decoder through the Simple Network Management Protocol (SNMP). SNMP-based management uses Network Management Stations (NMSs) to collect data or configure devices (SNMP agents) across an IP network.

Audience

This chapter is intended for users who are familiar with SNMP-based management and who will be developing applications such as provisioning services, or creating and modifying existing network management systems to manage the Makito X decoder.

TIP To develop new SNMP applications, see the list of "Supported MIBs" on page 158.

Topics In This Chapter

Overview

To support management of the Makito X decoder by third party Network Management Stations (NMSs), the system includes an SNMP agent that may be used to configure and control the system's Audio/Video services and streams. This SNMP agent answers requests and issues traps (event notifications) to NMSs that are allowed to access the system.

NOTE The Makito X decoder uses Net-SNMP Version 5.5.2 and supports SNMP v1, v2c, and v3.

The Makito X decoder supports a number of SNMP commands used to set or get Management Information Base (MIB) objects on the local host or on other SNMP agents reachable over the IP networks. For details, see "SNMP Utilities" on page 165.

Supported MIBs

The Makito X decoder SNMP agent supports the MIB-II (RFC 1213) standard and its updates, SNMPv3 MIBs, as well as the Haivision proprietary Enterprise MIB. The following table lists the supported MIBs:

Supported MIBs	Standard	Description
RFC1213-MIB.txt SNMPv2-MIB.txt IP-MIB.txt IF-MIB.txt TCP-MIB.txt UDP-MIB.txt	MIB-II (RFC 1213)	Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the unit.
SNMP-USER-BASED-SM-MIB.txt SNMP-USM-AES-MIB.txt SNMP-VIEW-BASED-ACM-MIB.txt	SNMPv3	Supports SNMPv3 User-based Security Model (USM) and View-based Access Control (VACM).
HAI-VISION-MIB.txt HAI-AVT-STREAM-MIB.txt HAI-HDC-MIB.txt	Haivision Enterprise	Supports configuration, status, and statistics.
HAI-MAKITO-X-DEC-CAPS.txt	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X Series (decoder) SNMP AGENT. It specifies which object groups from the listed MIB files are implemented, and furthermore, it specifies implementation constraints and deviations from the MIB OBJECT specification such as differences in ranges.

SNMP Agent Components

This section provides key information for system administrators responsible for setting up SNMP management on the Makito X decoder.

snmpd

snmpd is an SNMP agent that binds to a port and listens for requests from SNMP management software. Upon receiving a request, it performs the requested operation, either retrieving information or configuring the system. When finished processing the request, the agent sends a response to the sender with the requested information or the status of the configuration operation.

When you start an SNMP agent on a Makito X decoder using the service snmp start command, it loads the management database with the MIB files in the directory /usr/share/snmp/mibs and configures the agent with the files /usr/share/snmp.

snmpd.conf

snmpd.conf is the configuration file that defines how the SNMP agent works. You may need to edit this file to specify the location of the Network Management System (NMS) and to set up traps. However, for most settings, it is preferable to use the nmcfg configuration script. On the Makito X decoder, the snmpd.conf file includes:

- access control setup (i.e., community and user privileges),
- system information setup (e.g., system location, services and contact),
- trap destinations (i.e., the trap sink community to use).

snmpd.conf is located in the directory /usr/share/snmp.

For a detailed description, see the snmpd.conf file.

TIP To edit the snmpd.conf file in order to enable SNMP traps, see "Editing snmpd.conf to Enable Traps" on page 168.

snmpd.local.conf

snmpd.local.conf is the configuration file that defines the VACM (View-based Access Control Model) views modeling the privilege levels of the Makito X decoder user groups: admins, operators, and users. These groups can be used for v1/v2c communities and v3 USM users.

This file cannot be modified. Access groups are used in place of the traditional ro (read-only) and rw (read-write) permissions when setting communities' and users' access with the nmcfg configuration script.

SNMP Community Names

Following are the default SNMP community names and their privileges for accessing the Makito X decoder MIBs.

SNMP Community Name	Access Rights
admin	Read and write permission from local network and local host
public	Read-only permission from local network

SNMP Traps

Traps are SNMP messages that the SNMP agent sends to management stations when events, alarms or faults occur in the system or on the network. The Makito X decoder generates trap messages and sends them to active management stations that are identified as the trapcommunity in the Trap Destinations section in the snmpd.conf file.

The following traps are generated by the Makito X decoder:

SNMP Trap	Description
coldStart	A coldStart trap indicates that the sending protocol entity (i.e., the Makito) has re-initialized itself and is ready to operate. The coldStart trap is generated when the Makito X decoder is powered on. It is developed in accordance with RFC 1215 - MIB.
linkDown or linkUp	A linkDown trap signifies that the sending protocol entity (i.e., the Makito) recognizes a failure in one of the communication links represented in the SNMP agent's configuration. A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the SNMP agent's configuration has come up. These traps are generated when the Ethernet interface goes down or up. These traps are developed in accordance with RFC 1215 - MIB.

TIP To get started, you may need to edit the snmpd.conf file in order to enable SNMP traps. See "Editing snmpd.conf to Enable Traps" on page 168.

nmcfg

nmcfg is the configuration script that helps the configuration of the SNMP agent. It is particularly useful for the creation and management of SNMPv3 users of the User-based Security Model (USM) and the assignment of VACM (View-based Access Control Model) access rights to communities and users. The script interacts with the /var/net-snmp/snmpd.conf persistent data file, which maintains the USM user database and other SNMP agent persistent information. The script also performs snmpget commands to display the list of USM users, which is not available in a human readable form in any configuration file.

The script also reads and modifies the snmpd.conf configuration file to manage system parameters (contact, location), community-based (v1/v2c) security, and user access control. Used without parameters, it displays a summary of the SNMP agent configuration: system parameters, access control, and SNMPv3 USM users.

Following is an example of the nmcfg configuration script output:

```
# nmcfg
system parameter             value
---------------------------- ------------------------------------------
engineid                     0x80001f88030050c2c611ad
contact                      "john doe <jdoe@example.net>"
location                     "QA lab"

model        perm/group   level        user/community      source
---------- ------------ -------------- --------------------- ------------
usm          users        auth         guest                -
usm          admins       priv         johndoe              -
v2c          admins       noauth       admin                localhost
v2c          admins       noauth       admin                localnet
v2c          users        noauth       public               localnet
v2c          rw           noauth       tech                 any

auth protocol        priv protocol        user
---------------- ---------------------- -------------
MD5                  DES                  admin
MD5                  nopriv               guest
SHA                  AES                  johndoe
# nmcfg help
usage: nmcfg
      nmcfg help
      nmcfg access help
      nmcfg access usm permit <uname> {<group>|ro|rw}
  [{noauth|auth|priv}]
      nmcfg access usm delete <uname>
      nmcfg community help
      nmcfg community permit <community> {<group>|ro|rw} [<host>]
      nmcfg community delete <community> [{<group>|ro|rw} [<host>]]
      nmcfg system help
      nmcfg system define <param> "<value>"
      nmcfg system delete <param>
```

```
nmcfg user help
nmcfg user define <uname> [{MD5|SHA} "<apwd>" [{DES|AES}
["<ppwd>"]]]
nmcfg user delete <uname>
```

Related Topics

- "nmcfg" on page 200 (in Appendix A: "CLI Command Reference")

SNMPv3

For SNMPv3, the definition of a user and its access permission are separate steps, whereas for v1/v2c community-based security, a single configuration line (e.g., rwcommunity admin) defines both.

The following command creates the user "johndoe" and defines its authentication protocol and password, and its privacy (encryption) protocol and password. (Note that you can type nmcfg user help to view the supported protocols and pass phrase restrictions.)

```
# nmcfg user define johndoe SHA "password" AES "pass phrase"
```

The new user has no permissions until a rouser or rwuser line is added in the snmpd.conf configuration file. The command below shows that read and write permission is granted if the user issues authenticated requests. Note that encryption (privacy) implies authentication.

```
# nmcfg access usm permit johndoe rw auth
```

The following line is added by the above command in the snmpd.conf configuration file:

```
rwuser johndoe auth
```

To assign Makito X decoder user group privileges instead of the read-only or read-write permissions (to the whole MIB), the ro or rw parameter of the nmcfg access command can be replaced by the access group admins, operators, or users. These groups provide to SNMP v1/v2c communities and SNMPv3 USM users access privileges modeled on the Makito X decoder CLI and Web interface privilege levels.

```
# nmcfg access usm permit johndoe operators auth
```

The following line is added by the above command in the snmpd.conf configuration file, using a VACM group defined in snmpd.local.conf:

```
group _operators_auth_ usm johndoe
```

Examples

The following examples show how the v3 parameters are used with the SNMP commands.

The following get command has the required security level (authentication) and succeeds.

```
# snmpget –v3 –u johndoe –a SHA –A "password" –l authNoPriv localhost
  sysName.0
SNMPv2-MIB::sysName.0 = STRING: razor
#
```

The following get command provides no security (no authentication, no privacy) and fails.

```
# snmpget -v3 -u johndoe -l noAuthNoPriv localhost sysName.0
Error in packet
Reason: authorizationError (access denied to that object)
#
```

The following set command provides the highest security level (authentication and privacy), even if access policy only required authentication, and succeeds.

```
# snmpset -v3 -u johndoe -a SHA -A "password" -x AES -X "pass phrase" -l
  authPriv localhost haiAvtStreamEncapsulation.1 i directRtp
HAI-AVT-STREAM-MIB::haiAvtStreamEncapsulation.1 = INTEGER:
  directRtp(1)
#
```

SNMP Utilities

The following table summarizes the SNMP commands which can be used to set values or request information from the MIB objects on the local host or on other SNMP agents reachable over the IP networks.

To do this...	Use this command...
To retrieve the value of an object from a network entity.	snmpget
To set information on a network entity.	snmpset
To retrieve management information from a network entity.	snmpstatus
To send an SNMP notification to a manager.	snmptrap
To retrieve the values of *all* objects under a particular location in the MIB object hierarchy tree. Use to obtain the values of all the objects under the system and interfaces nodes. NOTE: The retrieval of a complete subtree is referred to as "walking the MIB."	snmpwalk

The SNMP utilities are located in the directory /usr/bin.

For more information on an SNMP command, enter the command with the -h (or --help) argument.

SNMP Syntax for Setting Up Streams

The Haivision Audio/Video Transport Stream MIB (HAI-AVT-STREAM-MIB) is composed of multiple tables described below.

Table	Index	Description
haiAvtStreamNewID.0	none	Next available stream ID
haiAvtStreamInverseTable	IP address type IP address Port	Table to retrieve the stream ID from the IP address and port
haiAvtStreamTable	Stream ID	Stream configuration and status
haiAvtStreamStatsTable	Stream ID	Stream statistics

MIB object names and values are similar to their CLI parameter counterparts while following MIB syntax (for example, haiAvtStreamPort for port, directRtp for direct-RTP).

Streams are created and deleted using the SNMPv2 RowStatus object (haiAvtStreamRowStatus). All RowStatus values are supported (active, notInService, notReady, createAndGo, createAndWait, destroy). See the description in the SNMPv2-TC.txt file of the MIBs directory. Stream writable objects can only be set at creation time (RowStatus is createAndGo or createAndWait) or while the stream is not active (RowStatus is notInService or notReady).

The example below, using netsnmp CLI commands on the Makito X decoder, creates a streaming session with IP Multicast Address 233.252.0.106 on port 2000. The Stream ID 0 (haiAvtStreamTable index) is used to create a stream; this value will be set to the first available Stream ID (>=1) on createAndGo or when set to active after createAndWait:

```
snmpset -v2c -c admin localhost haiAvtStreamAddr.0 d 233.252.0.106
  haiAvtStreamPort.0 u 2000 haiAvtStreamRowStatus.0 i createAndGo
```

The example below shows the same command, using the prefix (-IS) and suffix (-Is) options to remove repetition:

```
snmpset -v2c -c admin –IS haiAvtStream –Is .0 localhost Addr d 233.252.0.106
  Port u 2000 RowStatus i createAndGo
```

To retrieve the Stream ID of the stream just created, the haiAvtStreamInverseTable is used:

```
snmpget -v2c -c admin localhost
haiAvtStreamInverseID.ipv4.4.233.252.0.106.2000
HAI-AVT-STREAM-MIB::haiAvtStreamInverseID.ipv4.”233.252.0.106”.2000 =
    HaiAvtStreamID: 5
```

To create a Stream with a known ID, the haiAvtStreamNewID.0 object reports the next available Stream ID. Note that createAndWait is used so the content table can be set after stream creation.

```
snmpget -v2c -c admin localhost haiAvtStreamNewID.0
HAI-AVT-STREAM-MIB::haiAvtStreamNewID.0 = HaiAvtStreamID: 5
snmpset -v2c -c admin –IS haiAvtStream –Is .5 localhost Addr d 233.252.0.106
Port u 2000 Encapsulation i tsUdp RowStatus i createAndWait
snmpset -v2c -c admin –IS haiAvtStreamRowStatus.5 i active
```

Editing snmpd.conf to Enable Traps

To enable the generation of SNMP traps, you may need to edit the file /usr/share/snmpd.conf to set the Trap receiving host. You must be logged in with administrative privileges to edit this file.

The file contains the syntax for v2c and v3 traps in a comment above the #trapsess line.

NOTE trapsess provides a generic mechanism for defining notification destinations. The option -Ci can be used (with -v2c or -v3) to generate an INFORM notification rather than an unacknowledged TRAP. This is the recommended directive for defining SNMPv3 trap receivers.

To edit the snmpd.conf file:

1. Open the /usr/share/snmp/snmpd.conf configuration file.
2. Uncomment the trapsess line (delete the leading #) and replace "trapreceiver" by the IP address of the "host" receiving SNMP traps.
3. Change the community (public) if needed and the port number (162) if your trap receiver is not using the well known SNMP trap port.

```
##############################################
# SECTION: Traps
#
# This section defines who is receiving traps from this snmp agent.
#
# trapsess: Send v2c or v3 TRAP or INFORM (-Ci)
# arguments: [-Ci] -v2c -c community-string host[:port]
# arguments: [-Ci] [-e engineID] -v3 -u user [-a {MD5|SHA} -A passwd] [-x
  {DES|AES} -X passwd] [-l level] host[:port]
#  example: trapsess -v3 -u joenet -a SHA -A secret -l authNoPriv mynms:162
#

#trapsess -Ci -v2c -c public trapreceiver:162
```

APPENDIX A: CLI Command Reference

This alphabetical command reference lists and describes the available Makito X decoder Command Line Interface (CLI) commands and their parameters.

Commands In This Appendix

Syntax Conventions

The following syntax conventions are used in this appendix:

Convention	Description
MS Sans Serif font	Indicates command names and options, filenames and code samples.
italic font	Indicates variables that you replace with a user-defined value or name.
< >	Same as italics. Variables are enclosed in angle brackets in contexts that do not allow italics.
[ ]	Square brackets indicate optional items or parameters.
x | y	A vertical bar separates items in a list of options from which you must select one. If options are not separated by |, you may use combinations.
{ x | y | z }	Items separated by vertical bars and enclosed in braces indicate a choice of required elements.
[x { y | z }]	Vertical bars and braces within square brackets indicate a required choice within an optional element.

TIP Parameter names and enumerated values are case-insensitive and can be abbreviated.

CLI Access Control

Below is a list of CLI commands and other functionalities supported by the system and the privileges for each group.

Command	Admins	Operators	Users
Web access	Yes	Yes	Yes
Telnet to/from decoder	Yes	Yes	Yes
Operation			
viddec	Yes	Yes	"get" only
auddec	Yes	Yes	"get" only
hdmi	Yes	Yes	"get" only
stream	Yes	Yes	"get" only
sap	Yes	Yes	"get" only
service	Yes	Yes	"status" only
talkback	Yes	Yes	"get" only
temperature	Yes	Yes	"get" only
mkstill	Yes	Yes	No
still	Yes	Yes	"list" only
Network and Management			
haiversion	Yes	Yes	Yes
package (for upgrade)	Yes	No	No
config	Yes	Yes	"list" only
ethercfg	Yes	No	No
ipconfig	Yes	No	No
license	Yes	No	No
service	Yes	No	No
passwd	Yes	"operator" password only	"user" password only
pubkey	Yes	Yes	Yes
reboot	Yes	No	No
iperf	Yes	Yes	Yes
ping	Yes	Yes	Yes
tcpdump	Yes	No	No

Command (Cont.)	Admins	Operators	Users
traceroute	Yes	Yes	Yes
Security Commands			
account	Yes	No	No
audit	Yes	No	No
banner	Yes	No	No
certificate	Yes	No	No
messages	Yes	No	No
policy	Yes	No	No

For an overview of system access control on the Makito X decoder, see "Role-based Authorization" on page 59.

account

SYNOPSIS

account uname create [role=admin]
account uname/all get
account uname/all list
account uname passwd
account uname pubkey add|remove keyfile
account uname pubkey list
account uname lock
account uname unlock
account uname delete

DESCRIPTION

The account command is used to create, delete and modify administrative user accounts for the Makito X decoder.

NOTE The account command can only be used by the Administrator.

ACTIONS

create	Creates a new user account. See account Parameters below for roles. You will be prompted to enter and confirm the initial password.
get	Displays the account information for the user or the Makito X decoder, including account name, role, state, password expiry status, and public key(s).
list	Lists the account information for the user or the Makito X decoder in table format.
passwd	Modifies the user account password. You will be prompted to enter and confirm the password (which the user will have to change upon first login). For the allowed characters, see "Password Requirements" on page 66.
pubkey add|remove keyfile	Adds or removes a public key to the user account. See "Managing Public Key Authentication" on page 133 for more information.

pubkey list	Lists any public key files that have been uploaded for this account.
lock	Locks the user account (if Enabled).
unlock	Unlocks the user account (if Locked).
delete	Deletes the user account.

ACCOUNT PARAMETERS

Parameter	Default	Description/Values
role		Use with account create command to specify the role for the user account, either: • Admin • Operator • Guest For details on roles, see "Role-based Authorization" on page 59.

ACCOUNT EXAMPLES

```
# account all list
```

```
name            role           state     pwd expiry   pubk
--------------- -------------- --------- ------------ ----
admin           Administrator  Enabled   never        No
fdfdf           Guest          Enabled   never        No
infodev         Operator       Enabled   by admin     No
operator        Operator       Locked    never        No
user            Guest          Enabled   never        No
```

Related Topics

- "Managing User Accounts" on page 128

auddec

SYNOPSIS

```
auddec set parameter=value [parameter=value ...]
auddec get
```

DESCRIPTION

The auddec command is used to manage audio decoding settings. This includes binding the analog audio output to either the SDI 1 or SDI 2 video decoder. You can also configure audio settings such as the Audio Level and view the Audio Sampling Rate.

On the dual channel decoder, two streams are received and can be displayed on either SDI video port. Analog audio can be selected from embedded channels on either stream. *Both* Analog Audio and Embedded Digital Audio are active.

NOTE When the decoder is licensed for one channel only, it mirrors the decoded stream to all interfaces and supports up to eight (8) channel pairs of AAL-LC audio decoding for a stream.

ACTIONS

set	Modifies decoder analog audio parameter(s). A series of one or more parameter=value pairs can be specified at once. See auddec Parameters below.
get	Displays decoder analog audio status information.

AUDDEC PARAMETERS

Parameter	Default	Description/Values
source	SDI1CH12	The input source for analog audio, either SDI 1 or SDI 2: • SDI1CH12, SDI1CH34, SDI1CH56, SDI1CH78 • SDI2CH12, SDI2CH34, SDI2CH56, SDI2CH78
level	6	The maximum analog audio output level in dBu (decibels unloaded), from +5dBu to +20dBu.

AUDDEC EXAMPLES

# auddec get all	Returns audio configuration information for the decoder, such as: Audio Analog Configuration: Output Source : SDI1Ch1+2 Output Level : 6 dBu
# auddec set level="6"	Sets the audio level to 6. You will receive the following confirmation: Decoder analog configured successfully.

Related Topics

- "Configuring the Analog Audio Output" on page 100

audit

SYNOPSIS

```
audit start
audit stop
audit set parameter=value [parameter=value ... ]
audit get [config|stats|all]
audit verify [debug]
```

DESCRIPTION

The audit command is used to enable remote logging of system events and configure the remote audit (syslog) server connection.

NOTE The audit command can only be used by the Administrator.

ACTIONS

start	Establishes a connection from the decoder to a remote audit server and enables logging to it.
stop	Disables the connection to the remote audit server.
set	Modifies the audit parameters. A series of one or more parameter=value pairs can be specified at once. See audit Parameters below.
get	Displays audit configuration and connection status information.
verify	Verifies the validity of the TLS connection parameters. TIP: Connect to the audit server in verbose mode to help diagnose connection or certificate problems.

AUDIT PARAMETERS

Parameter	Default	Description/Values
server	n/a	The server IP address. Enter an IP address in one of the following formats:
		• fqdn[:port]
		• ipaddr[:port]
		• hostname[:port]

Parameter	Default	Description/Values (Cont.)
transport	UDP	The transport protocol, either:
		• UDP (User Datagram Protocol): Default UDP port = 514
		• TLS (Transport Layer Security): Default TLS port = 6514
trusted	All	If transport is TLS, the type of server authentication:
		• All: No server authentication
		• CA-signed: Root-CA certificate imported
		• Self-signed: Fingerprint
fingerprint	n/a	If trusted is self-signed, specify the audit server certificate fingerprint (md5 or sha1):
		• md5-fingerprint:
		• sha1-fingerprint:

AUDIT EXAMPLE

# audit get	Configuration: Audit server address : syslog.example.com:10533 Transport : TLS Trusted servers : CA-signed

Related Topics

- "Managing Audits" on page 153

banner

SYNOPSIS

```
banner enable
banner disable
banner install <bannerfile>
banner get
banner delete
```

DESCRIPTION

The banner command is used to manage the Advisory Notice and Consent Banner. This is a single text file that will be displayed to users who log in for interactive sessions on the Makito X decoder.

NOTE The banner command can only be used by the Administrator.

In the current release, only ASCII file format is supported for the banner file; the maximum file size for the banner is 4KB.

ACTIONS

enable	Enables display of the installed Advisory and Consent Banner page at login (a banner must be installed).
disable	Disables display of the current Advisory and Consent Banner page at login.
install	Installs a text file as the Advisory and Consent Banner page. IMPORTANT: The text file must be downloaded to the decoder and locally stored in the current (administrative) user's directory before it can be installed from the CLI. The Makito X decoder supports FTP and TFTP client, as well as SCP client and server for downloading and uploading files.
get	Displays banner status information.
delete	Deletes the banner file from the system.

BANNER PARAMETERS

Parameter	Default	Description/Values
bannerfile	n/a	The name of the .txt file to display as the Advisory Notice and Consent Banner for the decoder.

BANNER EXAMPLES

# banner get	The Advisory Notice and Consent Banner is disabled. If enabled, the following banner is displayed upon user login: ------------------------------ ********** * WARNING * ********** THIS IS A PRIVATE COMPUTER SYSTEM. This computer system including all related equipment and network devices are provided only for authorized use. All computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. ********** * Haivision Systems - Makito X decoder #4 * **********

Related Topics

- "Managing Banners" on page 137

certificate

Synopsis

certificate name/all get
certificate name/all list
certificate name view
certificate name create [sign=self] [subject=query]
certificate name delete [type=id]
certificate name import infile=<certfile> [type=id] [fmt=auto]
certificate name select
certificate name verify

Description

The certificate command is used to manage the system's certificates that are used to establish TLS connections to the audit server as well as secure HTTPS sessions.

NOTE The certificate command can only be used by the Administrator.

The autocert file is a default certificate file, generated when the IP address is changed from factory settings, or when an audit or an HTTPS session starts with no selected certificate.

Actions

get	Displays the information for the specified certificate or all certificates, including certificate name, type, signature, subject, issuer, expiration, and fingerprint.
list	Lists the specified certificate or all certificates installed on the decoder, including the type and name.
view	Displays the content of the named certificate file.
create	Generates a Self-signed certificate or a Certificate Signing Request. The sign and subject can be specified. See certificate Parameters below.
delete	Deletes the selected certificate. The type can be specified. See certificate Parameters below. NOTE: The type specification may be added to specify the deletion of the Identity certificate, the chain associated with it, or the CA certificate with the given name.

import	Imports a certificate to be installed on the device. The infile, i.e., the file to import the certificate from, must be provided. The file's type and format can also be specified. See certificate Parameters below.
select	Selects the certificate used when establishing a TLS connection with the audit server or starting an HTTPS session.n.
verify	Verifies the validity of the specified certificate.

CERTIFICATE PARAMETERS

Parameter	Default	Description/Values
sign	self	The signature type for the certificate: • self: Creates a self-signed identity certificate. • Request: Creates an identity Certificate Signing Request (CSR)
subject	query	Sets the certificate's distinguished name parameters: • auto: Automatically gets the subject Common Name which is HOSTNAME.DOMAIN if DNS is configured, or IPADDR otherwise. The subject Alt Name is set to DNS:HOSTNAME.DOMAIN, DNS:HOSTNAME,IPAddress:IPADDR • query: Prompts the user for Distinguished Name (DN) attributes • DN: Distinguished Name 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

Parameter	Default	Description/Values (Cont.)
type	id	The type of certificate to either import or generate: NOTE: Only ID certificates can be generated. Chain and CA certificates can only be imported. • id: Identity certificate (for HTTPS service and audit) • chain: Identity certificate CA chain (Import only) • ca: Certificate Authority Certificate (for peer certificate validation, Import only)
fmt	auto	The format in which the certificate is encrypted: • auto: Detects the certificate format based on file extension when importing. • pem: Privacy Enhanced Mail Base64 encoded DER certificate • p7: PKCS#7 • p12: PKCS#12 • pfx: PKCS#12 • der: Distinguish Encoding Rules
infile	n/a	The name of the file to import. NOTE: The administrator has previously downloaded/uploaded the certificate file to import in its home directory (using SCP, for example).

Related Topics

- "Managing Certificates" on page 144

config

Synopsis

config save [cfgname] [startup=yes,no]

config load [cfgname]

config delete [cfgname/all]

config list

Description

The config command is used to manage configurations on the Makito X decoder. This includes saving the current configuration, loading a saved configuration, and specifying the configuration file to load at startup.

All configuration files are stored in /usr/share/haivision/config.

NOTE This is equivalent to saving and loading Presets in the Web interface. See Saving and Loading Presets on page 108.

Actions

save	Saves the current configuration. Saves every parameter in the system, including decoder settings and stream destination and status (excluding the system IP address). All configuration files are stored in /usr/share/haivision/config. See NOTE regarding cfgname.
load	Loads a previously saved configuration identified by <cfgname>. Reassigns every parameter in the system, including decoder settings and stream destination and status (excluding the system IP address).
delete	Deletes a previously saved configuration identified by <cfgname>. If no filename is specified, the system deletes the default configuration (haistartupcfg.ini).
list	Displays a list of the available configuration files.
help	Displays usage information for the config command.

CONFIG EXAMPLES

# config save Class200 startup= yes	Saves the current configuration under the name “Class200” and sets it to be the startup configuration.
# config load Class200	Loads a previously saved configuration identified by the name “Class200” (located in the active (local) directory).

NOTE The following special characters are *not* supported for use in the configuration name (cfgname) unless they are escaped using the backward slash (\) character before being used:

Single Quote `

Ampersand &

Parentheses ( )

Semicolon ;

Apostrophe ′

Double Quote ″

Left and Right Angle Brackets < >

Related Topics

- “Saving and Loading Presets” on page 108

date

SYNOPSIS

date

DESCRIPTION

The date command is used to view the current date.

DATE EXAMPLE

# date	Displays the current date, e.g.: Fri Jun 9 13:02:48 EDT 2017

Related Topics

- "Configuring Date and Time" on page 118

ethercfg

Synopsis

ethercfg [-a on|off] [-s 10|100|1000] [-d half|full] [-c bandwidth] [-w yes| no]

Description

The ethercfg command is used to view, manually control, and save the Ethernet configuration parameters.

When the Makito X decoder boots up, it automatically initializes and configures the Ethernet interface to match the settings on the Ethernet switch to which it is connecting. However, you may need to manually force settings such as the Ethernet interface line rate and duplex mode.

- You can change the Ethernet interface line rate while autonegotiation is enabled.
- However, in order to change the duplex mode, you must first disable autonegotiation.

If no options are specified, the system displays the current settings, as shown in the following example.

```
admin@haivision:~$ ethercfg
  Speed                 : 1000mbps
  Duplex                : Full
  Auto-Negociation      : On
  Advertised Mode       : All
  Link Detected         : Yes
  Ceiling               : 100Mbit
```

Options

-a	--autoneg	Enables or disables autonegotiation.
-s	--speed	If autonegotiation is disabled, sets the speed. If autonegotiation is enabled, this will be the only advertised supported speed.
-d	--duplex	If autonegotiation is disabled, sets the duplex mode. If autonegotiation is enabled, this will be the advertised duplex mode.
-c	--ceiling	Puts a “ceiling” (in kbps or Mbps) on the bandwidth available to the Ethernet port.
-w	--write	Skips the save settings prompt.

NOTE When the entire set of parameters is not specified, the system will try to combine the current Ethernet settings with the newly supplied ones. Therefore, you should carefully review the outputted configuration when the command completes to make sure it matches the desired Ethernet settings.

Always enable autonegotiation with Gigabit Ethernet (GigE) speed (1000 Mbps).

ETHERCFG EXAMPLE

# ethercfg -s 100	Sets the line speed to 100 Mbps (which modifies the advertised mode, see following example).

```
admin@haivision:~$ ethercfg -s 100
  Speed              : 100mbps
  Duplex             : Full
  Auto-Negociation   : On
  Advertised Mode    : 100mbps Full-Duplex
  Link Detected      : Yes
  Ceiling            : 100000kbps

Do you wish to save these settings ? (y,n): y
Settings saved successfully.
```

Related Topics

- "Configuring Network Settings" on page 114

haiversion

SYNOPSIS

haiversion

DESCRIPTION

The haiversion command is used to display the Firmware Build ID and Build Time on the Makito X decoder. It also displays the serial number for the unit.

HAIVERSION EXAMPLE

# haiversion	Displays the Serial Number, Firmware Version and Date for the unit, such as. Card Type : "Makito2 Decoder" Part Number : B-292D-HD2 Serial Number : HAI-031325030002 MAC Address : 5c:77:57:00:42:b2 Firmware Version : 2.0.0-85 Firmware Date : "Jun 8 2017" Firmware Time : "14:42:19" Firmware Options : "SRT" Hardware Version : -- Hardware Compatibility : -001G CPLD Version : 5 (Official, Internal flash) Boot Version : "U-Boot 2010.06 (Mar 19 2014 - 10:37:19)-MakitoXD 0.9.14"

Related Topics

- "Viewing System Status Information" on page 104

hdmi

SYNOPSIS

```
hdmi set parameter=value [parameter=value ...]
hdmi get
```

DESCRIPTION

The hdmi command is used to manage decoder HDMI settings.

NOTE The HDMI port can be configured to mirror the same content that is seen on either Decoder 1 or Decoder 2. If the stream contains computer graphics content, that content can only be displayed on the HDMI interface. By default, HDMI displays the SDI 1 content, so you only need to change the HDMI setting to monitor the SDI 2 channel.

ACTIONS

set	Configures HDMI settings. A series of one or more parameter=value pairs can be specified at once. See hdmi Parameters below.
get	Displays HDMI status information.

HDMI PARAMETERS

Parameter	Default	Description/Values
videoSource	Decoder1	None, Decoder1, Decoder2.
audioSource	Chan12	Chan12, Chan34, Chan56, Chan78
surroundSound	no	yes, no

HDMI EXAMPLE

# hdmi get	Displays the current HDMI configuration and status. Decoder Hdmi Infomation: Video Source : Decoder1 Audio Source : Chan1+2 Surround Sound : No Decoder 1 State : Running Current Resolution : 1280x720 Progressive Current FrameRate : 60

Related Topics

- "Configuring the HDMI Display" on page 98

ipconfig

Synopsis

```
ipconfig display
ipconfig configure
ipconfig renew
ipconfig release
```

Description

The ipconfig command is used to set and view the parameters that specify the networking context for the Makito X decoder, including the IP settings, hostname, and DNS.

The ipconfig command is also used to:

- Configure the display of the decoder IP address during the boot sequence, so users can determine the IP address simply by examining the HDMI or SDI outputs on a display.
- Enable the Multicast DNS (mDNS) protocol to allow the Safari Web browser (or other mDNS application) to automatically find the decoder. In Safari, navigate to Bookmarks and then select Bonjour to see the Makito X listed.
- Set the Network Time Protocol (NTP) server address and Time Zone.

When DHCP is enabled, you can configure the DHCP Vendor Class ID (option 60), which is set by default to “Haivision Makito X Decoder”. This allows IT departments to identify Makito X devices on their networks. You must reboot for any changes to take effect.

As shown in the following example, when you enter the ipconfig configure command, the system displays the current IP settings and takes you through a series of prompts enabling you to change the IP settings, optionally enable DHCP, and change the hostname, DNS settings, NTP settings, and/or Time Zone setting.

The ipconfig display command returns the current IP settings.

Actions

display	Displays the current IP configuration.
configure	Configures IP settings.
renew	Renews DHCP address lease.
release	Releases current DHCP address lease.

IPCONFIG EXAMPLES

# ipconfig display	Returns current IP settings for the decoder, when configured to use DHCP: Current IP Settings (Obtained via DHCP): IP Address : 10.65.133.135 Network Mask : 255.255.255.0 Gateway : 10.65.133.1 Link-Local Address : (Auto-assigned when DHCP is unavailable) Hostname : MXD-133-22 DHCP Vendor Class ID: "Haivision Makito X Decoder" Current IP On Screen Display Settings: Startup Display : On Display Duration : 15 seconds Display Format : 1080p60 Current DNS Settings: Domain : haivision.com Primary Server : 10.65.0.10 Alternate Server : (None) Current Multicast DNS (mDNS) Settings: Responder : Disabled Current NTP Settings: Server : 10.5.0.1 Timezone : "America/Montreal"
# ipconfig display	Returns current IP settings for a decoder that does not use DHCP: Current IP Settings: IP Address : 10.5.1.2 Network Mask : 255.255.255.0 Gateway : 10.5.0.1 Hostname : MakitoX_Dec2 Current IP On Screen Display Settings: Startup Display : On Display Duration : 60 seconds Display Format : 1080i30 Current DNS Settings: Domain : haivision.com Primary Server : 10.65.0.10 Alternate Server : (None) Current Multicast DNS (mDNS) Settings: Responder : Disabled Current NTP Settings: Server : pool.ntp.org Timezone : "America/Montreal"

#ipconfig configure	Prompts you as follows to modify current settings: Current IP Settings: IP Address : 10.5.1.2 Network Mask : 255.255.255.0 Gateway : 10.5.0.1 Change IP settings? (y,N): y Use DHCP to obtain IP address automatically? (y,N): n Enter IP address (10.5.1.2) : 10.65.131.31 Enter netmask (255.255.255.0): 255.255.255.0 Enter default gateway (10.5.0.1): 10.65.131.1 Current IP On Screen Display Settings: Startup Display : Off Display Duration : 60 seconds Display Format : 1080i30 Change OSD settings? (y,N): y Display IP address on screen at startup? (Y,n): On Current Hostname : MakitoX_Dec2 Change hostname? (y,N): y Enter hostname (MakitoX_Dec2): MXD-31 Current DNS Settings: Domain : eqa.haivision.com Primary Server : 10.65.158.10 Alternate Server : (None) Change DNS settings? (y,N): n Current Multicast DNS (mDNS) Settings: Responder : Disabled Change Multicast DNS Settings? (Y,n): y Enable mDNS responder? (y,N): y Current NTP Settings: Server : 206.186.255.228 Timezone : "America/Montreal" Change NTP server? (y,N): n Change Timezone? (y,N): n Network settings updated successfully. Host name updated successfully. Multicast DNS settings updated successfully. You must REBOOT for any changes to take effect!

Related Topics

- "Configuring Network Settings" on page 114

license

SYNOPSIS

```
license list
license view <features.lic>
license install <features.lic>
license verify <features.lic>
license delete <features.lic>
```

DESCRIPTION

The license command is used to manage licensed features.

The license is delivered as a plain-text ASCII license file with the extension .lic to be installed on your Makito X decoder.

For more information, see "Managing Licenses" on page 123.

NOTE Multiple licenses may be installed on the same device at the same time.

ACTIONS

list	Displays a list of installed licenses. Licenses are stored on the Makito X decoder file system in the folder /usr/share/haivision/licenses.
view	Displays the content of the specified license file.
install	Installs the specified (uploaded) license. IMPORTANT: The license file must be uploaded to the decoder and locally stored in the current (administrative) user's folder before it can be installed. The Makito X decoder supports FTP and TFTP client, as well as SCP client and server for downloading and uploading files.
verify	Verifies the specified license (either installed or uploaded).
delete	Deletes a previously installed license file from the system.

LICENSE EXAMPLES

$ license list	Displays a list of licenses currently installed on the system: License Files (in /usr/share/haivision/licenses): metadata-PO123456.lic

Related Topics

- "Managing Licenses" on page 123

messages

SYNOPSIS

```
messages add <msgtext>
messages get
messages delete
```

DESCRIPTION

The messages command is used to manage administrative login messages. This is a log of a limited number of important events recorded such as installation of a software package, failure to establish or maintain connectivity with a remote audit server, Power-On Self Test (POST) errors, and other noteworthy events that require the administrator's attention.

These events will result in a message being sent directly to all logged-in administrators and will appear on their terminals. The message will also be displayed at the next administrative Web interface or CLI login.

NOTE The messages command can only be used by the Administrator.

Messages starting with "POST" are Power-On Self Test events. If you repeatedly get POST errors, the cryptographic module of the decoder may be compromised, and it is recommended to re-installed the firmware.

ACTIONS

add <msgtext>	Adds the message text to the log. This could be used to send messages to other administrators.
get	Displays messages.
delete	Deletes the messages.

Related Topics

- "Managing Messages" on page 135

mkstill

SYNOPSIS

mkstill <infile> resolution [-f]

where:

infile is the name of the image file to convert into a still image.

DESCRIPTION

The mkstill command is used to generate still images from a picture. The static image will be displayed when the decoder is not receiving a video stream.

The supported source formats for the static image are JPEG and PNG.

NOTE The maximum size of the source image is 2048x2048 pixels.

The resulting still image files are stored on the Makito X file system under /usr/share/haivision/still_images.

MKSTILL PARAMETER

Parameter	Default	Description/Values
resolution	n/a	Specifies the desired resolution of the still image. Supported values include: • 1080 for 1920x1080 • 720 for 1280x720 • 480, NTSC for 720x480 • 576, PAL for 720x576 • VGA for 640x480 • SVGA for 800x600 • XGA for 1024x768 • XGA+ for 1152x864 • WXGA for 1280x768 • WXGA2 for 1280x800 • SXGA for 1280x1024

Parameter	Default	Description/Values (Cont.)
resolution	n/a	• WXGA3 for 1360x768 • WXGA4 for 1366x768 • WXGA+ for 1440x900 • SXGA+ for 1400x1050 • HD+ for 1600x900 • UXGA for 1600x1200 • WSXGA+ for 1680x1050 • WUXGA for 1920x1200
-f		Forces overwrite of the still image at the destination.

MKSTILL EXAMPLE

```
# mkstill myimage.jpg resolution=1080
```

Converts the image file myimage.jpg into a 1920x1080 still image.

Related Topics

- "still" on page 218
- "Configuring Still Image Streaming" on page 126

nmcfg

NOTE You must be logged in with administrative privileges to enter nmcfg commands.

SYNOPSIS

```
nmcfg help
nmcfg access help
nmcfg access usm permit <uname> {<group>|ro|rw} [{noauth|auth|priv}]
nmcfg access usm delete <uname>

nmcfg community help
nmcfg community permit <community> {<group>|ro|rw} [<host>]
nmcfg community delete <community> [{<group>|ro|rw} [<host>]]

nmcfg system help
nmcfg system define <param> "<value>"
nmcfg system delete <param>

nmcfg user help
nmcfg user define <uname> [{MD5|SHA} "<pwd>" [{DES|AES} ["<pwd>"]]]
nmcfg user delete <uname>
```

DESCRIPTION

The nmcfg (Network Management Configuration) command is used by system administrators or GUI/Web Interface applications in the configuration of SNMP for the Makito X decoder. The nmcfg script reads and edits the standard SNMP configuration files, and then restarts the SNMP agent (snmpd) to apply the new settings.

The nmcfg script supports the configuration of v1/v2c community-based security model and v3 USM (User-based Security Model). The script supports the traditional access permissions (read-only, read-write) and VACM (View-based Access Control Model) views modeling the Makito X decoder user groups (admins, operators, and users).

Note that traps are not supported by the nmcfg script.

A detailed help, describing the options is available for each command option (for example, nmcfg access help or nmcfg user help).

For more information, see "nmcfg" on page 161 (in "SNMP Agent Components").

Options

access	Defines the access permissions granted to the v1/v2c communities and USM (v3) users. Only the USM security model option is shown in the summary help. The v2c security model, a different format for community configuration, is only displayed in the access detailed help. Note that the v2c security model also applies to SNMP v1.
community	Defines community-based (v1v/2c) security configuration for the Makito X decoder.
system	Defines contact and location system parameters.
user	Defines user-based (v3) security configuration for the Makito X decoder.

Actions

define	Acts as both create and update. If an object does not exist, it is added. If it exists, it is replaced or updated with the new settings. It is then not necessary to delete an existing object to change its settings. All required settings of an object are specified when defining/changing an object. It is not possible to set settings individually.
permit	Defines the access permissions for the community or the user. NOTE: Access permissions may be additive. For example, permitting a new source for an existing community adds to the existing one if it complements it.
delete	Deletes the specified object.
help	Displays usage information for the command, or if specified, the option.

NOTE nmcfg settings persist after reboots, unlike other Makito X decoder settings which are lost when the unit is rebooted unless saved as a configuration.

Example #1: Initialize a community-based (v1/v2c) system

In the example below, a system with default settings is configured to add a distant host access (198.51.100.122) to the existing localhost and localnet accesses of the admin community. Note that the localnet source is a special keyword that translates at runtime to the network settings of the LAN interface. System parameters are also defined.

```
# nmcfg
parameter value
-------------- ----------------------------------
contact<undefined>
location<undefined>

perm/groupcommunity       source
------------- ------------------- ---------------------
rw      admin               localhost
rw      admin               localnet
ro      public              localnet
# nmcfg system define contact "myname <myname@example.org>"
# nmcfg system define location "Media Lab"
# nmcfg community permit admin rw 198.51.100.122
#
```

Example #2: Create an SNMPv3 user

Two commands are required to create a USM (v3) user and define its access:

```
# nmcfg user define johnsmith SHA "arfds23dsjs" AES "2394urscxkvn"
# nmcfg access usm johnsmith operators
```

EXAMPLE #3: INITIALIZE A USM-ONLY (SNMPV3) SYSTEM

In the example below, system security is enforced by completely disabling SNMPv1/v2c access, and by requiring v3 USM authentication only for users group-based access, and encryption for admins and operators group-based access.

```
# nmcfg
system parameter value
---------------------- ----------------------------------
contact<undefined>
location<undefined>

perm/groupcommunity          source
------------------ -------------------- ----------------------
rw      admin                localhost
rw      admin                localnet
ro      public               localnet

# nmcfg agent stop
# nmcfg system define contact "joe net <jnet@example.org>"
# nmcfg system define location "Media Lab"
# nmcfg community delete admin
# nmcfg community delete public
# nmcfg user define joenet SHA "arfds23dsjs" AES "2394urscxkvn"
nmcfg: snmp agent is not running, user settings will apply when started
# nmcfg user define johnsmith SHA "89ss5dkj" AES "jfdsf78998sd"
nmcfg: snmp agent is not running, user settings will apply when started
# nmcfg user define guest MD5 "nososecret"
nmcfg: snmp agent is not running, user settings will apply when started
# nmcfg access usm permit joenet admins priv
# nmcfg access usm permit johnsmith operators priv
# nmcfg access usm permit guest users
# nmcfg agent start
# nmcfg

system parameter      value
----------------  ----------------------------------
engineid        0x80001f88802054a68b4b75388e
contact         "joe net <jnet@example.org>"
location        "Media Lab"

model perm/groupleveluser/community      source
--------------  -------------  ------  ----------------------  ---------
usm users     auth    guest                 -
usm admins    priv    joenet                -
usm operatorspriv     johnsmith             -
```

```
auth protocol priv protocol user
--------------------  --------------  -----------
MD5    nopriv         guest
SHA    AES            joenet
SHA    AES            johnsmith
#
```

Related Topics

- "nmcfg" on page 161 (in "SNMP Agent Components")

package

SYNOPSIS

```
package list
package info [<pkgfile>.hai]
package verify <pkgfile>.hai
package install <pkgfile>.hai
package download <pkgfile>.hai <tftpipaddr>
package delete <pkgfile>.hai | all
package cancel <pkgfile>.hai
```

DESCRIPTION

The package command is used to view and manage software packages.

NOTE The package command can only be used by the Administrator.

When package is entered without any actions or parameters, the system displays usage information for the command.

Package files are digitally signed to ensure integrity and authenticity. Package component signatures and their certificate validity are verified when downloading, manually with the verify action, and when actually performing the installation upon reboot.

If the verification fails after downloading, an error message is reported by the download command and the downloaded package is discarded. If verification fails while actually installing upon reboot, installation is canceled and a package install failure notice is added to the messages displayed to the Administrators (see messages CLI command). A successful package installation notice is added to the messages upon successful installation.

Example #1: Package Download and Installation

```
$ package download makitox_dec_v1.0.0-39.hai mytftp.example.com
1/5) Temporarly pausing decoder(s)...
2/5) Downloading package makitox_dec_v1.0.0-39.hai from
  mytftp.example.com...
3/5) Verifying integrity of downloaded package... Package verified
  successfully.
4/5) Synching file system...
5/5) Resuming decoder(s)...
Package downloaded successfully.
$ package install makitox_dec_v1.0.0-39.hai
Package makitox_dec_v1.0.0-39.hai will be installed on next boot sequence.
You must REBOOT to complete the update process!
$
```

Example #2: Package Download Verification Failure

```
$ package download makitox_dec_v1.0.0-39.hai mytftp.example.com
1/5) Temporarly pausing decoder(s)...
2/5) Downloading package makitox_dec_v1.0.0-39.hai from
  mytftp.example.com...
3/5) Verifying integrity of downloaded package... Package verification failed!
Try downloading the package again.
$
```

Actions

list	Displays a list of downloaded packages.
info	Displays information about the currently installed package. If a filename is specified, displays information about the package.
verify	Verifies the authenticity and integrity of the specified package.
install	Installs the specified package. The package will be automatically verified before installation.
download	Downloads the specified package file using TFTP and then verifies it.
delete	Deletes a previously downloaded package file. You can specify the package file or all.
cancel	Cancels installation of a package scheduled for the next reboot.

PACKAGE EXAMPLES

package list	Displays the list of downloaded packages: Package Files (in /usr/share/haivision/packages/): makitox_dec_v1.0.0-51.hai makitox_dec_v1.0.0-52.hai makitox_dec_v1.0.0-53.hai makitox_dec_v1.0.0-54.hai There are no packages pending installation on this system.
# package info makitox_dec_v1.0.0-54.hai	Displays information about the package
# package install makitox_dec_v1.0.0-54.hai	Installs the package

passwd

SYNOPSIS

passwd [<name>]

DESCRIPTION

The passwd command is used to change the password for the current user account.

NOTE Use the account command to reset the password of other users.

PASSWD EXAMPLE

# passwd	Changes the password for the current user account. The system prompts you to enter the old password and then the new password.

Related Topics

- "Role-based Authorization" on page 59

policy

SYNOPSIS

```
policy password  set [quality=basic] [minlen=6] [minuppers=0] [mindigits=0]
   [minsymbols=0] [expiry=yes] [lifetime=90]
policy session   set [autologout=yes] [idletimeout=15]
policy crypto    set [compliance=None]
policy pname/all get
```

DESCRIPTION

The policy command is used to configure and manage security policy settings. Policies are needed to define security criteria such as the required quality, length and composition of passwords. The security policies are: Password, Session, and Cryptographic Strength.

Security policies may be applied to bring the decoder to its CC evaluated configuration. During the hardening procedure, it is important for the administrator to set the policies before creating accounts.

NOTE The policy command can only be used by the Administrator.

ACTIONS

policy password set	Modifies the password policy parameters. A series of one or more parameter=value pairs can be specified at once. See password under policy Parameters below.
policy session set	Modifies the session policy parameters. A series of one or more parameter=value pairs can be specified at once. See session under policy Parameters below.
policy crypto set	Specifies the cryptographic policy. The complianceparameter can be specified. See crypto under policy Parameters below.
policy pname/all get	Displays the policy information for either the policy (i.e., password, session, or crypto) or the decoder.

POLICY PARAMETERS

Parameter	Default	Description/Values
	crypto	
compliance	None	Specifies the required cryptographic compliance, either: • None • FIPS140: All management cryptography is operated in the FIPS 140-2 mode. • NDPP11: Activates cryptographic security to a level compliant with the Network Device Protection Profile v1.1. • SP800-52 Revision 1: Applies cryptographic modules accredited under the National Institute of Standards and Technology (NIST) Special Publication 800-52, Revision 1. NOTE: Either selection will reinforce security for all management functions of the decoder in terms of cryptography. This setting will take effect upon the next reboot.
	password	
quality	Basic	The required password strength, either: • Basic • Strong
minlen	6	The minimum password length: • 6..40
minuppers	n/a if Basic --- 0 if Strong	(Password quality must be Strong) The minimum number of uppercase letters: • 0..40
mindigits	n/a if Basic --- 0 if Strong	(Password quality must be Strong) The minimum number of digits: • 0..40
minsymbols	n/a if Basic --- 0 if Strong	(Password quality must be Strong) The minimum number of symbols: • 0..40
expiry	No	Enables or disables password expiration: • Yes, No

Parameter	Default	Description/Values (Cont.)
lifetime	90 days	(Password expiry must be Yes) The number of days after which users must change their passwords: • 1..180 days (password expiration)
remember	0	The number of stored passwords. 5..400 passwords
session		
autologout	No	Enables or disables Auto Logout: • Yes, No
idletimeout	15 minutes	(autologout must be Yes) The maximum length of time the system may be idle before the user will be logged out: • 1..1440 minutes (inactivity timeout)

POLICY EXAMPLES

# policy crypto set compliance= NDPP11	
# policy password set quality= strong minlen=10 minuppers=1 minsymbols=1 expiry=yes lifetime=30	Sets the password policy for the decoder to be Strong, requiring passwords to be at least 10 characters in length, with one uppercase letter, one symbol. Passwords will expire in 30 days.

Related Topics

- "Managing Password Policies" on page 140

pubkey

SYNOPSIS

```
pubkey add <KEYFILE.pub>
pubkey remove <KEYFILE.pub>
pubkey list
```

DESCRIPTION

The pubkey command is used to manage your account's authorized SSH public keys.

You must first get the public key of your SSH client. Note that in the current release, this only applies to SSH CLI access to the decoder.

NOTE The pubkey command can only be used by the Administrator.

ACTIONS

pubkey add	Uploads a new public key file (.pub extension) to the decoder.
pubkey remove	Removes the specified public key file from the decoder.
pubkey list	Lists the public key files currently loaded on the decoder.

PUBKEY EXAMPLES

# pubkey add makito.pub	Uploads the public key file makito.pub to the decoder.
# pubkey list	Lists all public key files currently loaded on the decoder along with their fingerprints. In this example, there is one public key file: makito.pub : rsa[2048] b7:ae:79:92:0d:86:f9:8d:2d:ee:99:fc:ff:24:95:87:ee:78:1d:fd

Related Topics

- "Managing User Accounts" in Chapter

reboot

SYNOPSIS

reboot

DESCRIPTION

The reboot command is used to is used to halt and restart the Makito X decoder. Any unsaved configurations will be lost. The decoder will restart with the saved startup configuration.

REBOOT EXAMPLE

# reboot	Reboots the Makito X decoder. NOTE: While the unit is rebooting, you will lose your connection to the CLI. This will take approximately two minutes. Once the unit has rebooted, you can reconnect to the unit and log in again.

Related Topics

- "Rebooting the Decoder" on page 106

sap

Synopsis

```
sap get
sap enable
sap disable
sap start
sap stop
sap set
```

Description

The sap command is used to manage SAP settings.

NOTE To display the list of advertised sessions, use the stream get all command. See "stream" on page 219.

Actions

get	Displays SAP configuration information.
enable	Enables the SAP service and starts listening for session advertisements.
disable	Disables the SAP service, stopping the listening for session advertisements and deleting any discovered streams.
start	Starts listening for SAP advertisements; service must be enabled.
stop	Stops listening for SAP advertisements and deletes any discovered streams.
set	Configures SAP settings. A series of one or more parameter=value pairs can be specified at once.

SAP Parameters

Parameter	Default	Description/Values
address	n/a	The multicast address to listen on for SAP messages.
port	n/a	The UDP port to listen on for SAP messages.

SAP EXAMPLE

# sap get	Returns sap configuration information for the decoder, such as: Configuration: Address : 224.2.127.254 UDP Port : 9875

Related Topics

- "Enabling and Disabling Network Services" on page 120
- "Configuring the SDI Decoder Output" on page 86

service

SYNOPSIS

service svcname action [svcname action] [...]

where:

svcname can be: all, http, sap, snmp, ssh, talkback, telnet

DESCRIPTION

For security purposes, you may need to stop one or more network services from accessing the Makito X decoder. The service command is used to enable and disable the following network services: HTTP, SAP, SNMP, SSH, Talkback, and Telnet.

NOTE To specify SAP Source Address and Port, use the sap command. See "sap" on page 214.

ACTIONS

start	Activates the service immediately and configures the unit so that the service will be started automatically when the unit is rebooted.
stop	De-activates the service immediately and configures the unit so that the service will be disabled when the unit is rebooted.
restart	Restarts the service and configures the unit so that the service will be started automatically when the unit is rebooted.
status	Displays the current status of the service, i.e., if it has been started or stopped.

SERVICE EXAMPLES

# service all status	Displays information about all services, such as: http service is currently enabled http service is enabled at system startup sap service is currently enabled sap service is enabled at system startup snmp service is currently enabled snmp service is enabled at system startup ssh service is currently enabled ssh service is enabled at system startup talkback service is currently disabled talkback service is disabled at system startup telnet service is currently enabled telnet service is enabled at system startup
# service telnet stop	Stops telnet connection to the Makito X decoder.
# service all stop	Stops all network connections to the Makito X decoder.

Related Topics

- "Enabling and Disabling Network Services" on page 120
- "Audio Talkback" on page 32

still

SYNOPSIS

```
still list
still delete <filename>
still delete all
```

DESCRIPTION

The still command is used to manage available still image files on the Makito X file system.

Static image files must already have been generated (see following NOTE) and be located the folder /usr/share/haivision/still_images on the Makito X file system.

NOTE You can generate the image file either using the mkstill command, or from the Web interface (STILL IMAGES page, see "Configuring Still Image Streaming" on page 126).

Static images may be used to replace the "real" video stream when streaming is paused. You can then configure a Makito X stream with a static image using the viddec set command with the parameters [stillimage=custom] and [stillFile=<fname>].

ACTIONS

list	Lists the available still image files in /usr/share/haivision/still_images
delete	Deletes the specified still image file or all still image files.

STILL EXAMPLE

```
# still delete myimage.png
```

Deletes the image file myimage.png

Related Topics

- "mkstill" on page 198
- "stillImage" on page 230

stream

Synopsis

stream create port=udpport [addr=ipaddr] [id=number] [name=text]
[encapsulation=ts-udp | ts-rtp | ts-srt]
[sourceaddr=mcastsenderaddr]
stream id/name delete
stream id/name/all get [config | stats | all]
stream all get table
stream id/name clear

Possible Encapsulation Formats

ts-rtp: MPEG2 transport stream over RTP
[fec=yes,no]
ts-udp: MPEG2 transport stream over UDP (no RTP header)
[fec=yes,no]
ts-srt: MPEG2 transport stream over SRT (Secure Reliable Transport)
[latency=number] [passphrase=text]
[mode=listener | caller | rendezvous] [sourceport=udpport]
[flipaddr=ipaddr] [flipport=udpport] [flipttl=ipttl]
[fliptos=iptos]

Description

The stream command is used to create and manage streams to map the decoder inputs to output interfaces.

When creating a stream you can specify a unique id to assign to it or let the system assign one for you. You can also specify a name for the stream if needed.

The IP Address (addr field) is only required for multicast, but not for unicast streams.

Most commands will accept the stream id or name in order select the proper stream to manage.

Actions

create	Creates a decoder streaming session. A series of one or more parameter=value pairs can be specified at once.
delete	Deletes the specified stream.

get	Displays stream information. See stream Parameters below. You can specify to display the stream configuration, statistics, or all. stream all get table displays a summary of all the streams in a table format. NOTE: If sap is enabled, stream get all displays the list of advertised sessions. See "sap" on page 214.
clear	Clears the stream's statistics.
help	Displays usage information for the stream command.

STREAM PARAMETERS

Parameter	Default	Description/Values
port	n/a	The UDP port for the Decoder. Enter a number in the range 1025..65,535. Note that RTP streams use *even numbers only* within this range.
addr	n/a	(Optional, only required for multicast) Enter a Multicast IP address in dotted-decimal format. For multicast addresses, see IMPORTANT on page 222.
Optional stream Parameters		
id	n/a	A unique number assigned to the stream. NOTE: When creating a stream, you can specify a unique id to assign to it or let the system assign one (a sequential number) for you. Most commands will accept the stream id or name (see below) in order to select the proper stream to manage. TIP: The active stream ID may change due to a stream failover event.
name	n/a	(Optional) When creating a stream, you can also specify a name for the stream. 1 to 32 characters
encapsulation	ts-rtp	(Optional) The Encapsulation Type for the stream.
		• ts-rtp - MPEG2 transport stream over RTP
		• ts-udp - MPEG2 transport stream over UDP (no RTP header)

Parameter	Default	Description/Values (Cont.)
		• ts-srt - MPEG2 transport stream over SRT (Secure Reliable Transport)
		• rtsp - Real Time Streaming Protocol (RFC2326) with control over RTSP. For RTSP streams, you can specify the address as addr= rtsp://user:password@ip.add.re.ss/ path?var=value& var2=value2...
sourceaddr	n/a	(Multicast streams only) Enter the multicast sender IP address in dotted-decimal format (i.e., what address is broadcasting). See "Source Address" on page 78.
ts-rtp and ts-udp only		
FEC	None	(Optional) To enable Forward Error Correction (FEC), specify fec=yes. FEC varies with the protocol (encapsulation): • TS over UDP = VF FEC • TS over RTP = Pro-MPEG FEC NOTE: VF FEC is a proprietary FEC and is not interoperable with devices outside of the Haivision family. The FEC level is read from the encoded stream.
ts-srt only		
latency	125	Specifies how long the decoder will buffer received packets, from 20-8000 ms. See "Latency" on page 80.
passphrase	n/a	(Optional) A sequence of words or other text used to control access to the stream. Similar to a password in usage, but is generally longer for added security. This parameter is required if the stream is encrypted and is used to retrieve the cryptographic key protecting the stream. From 10-79 characters.

Parameter	Default	Description/Values (Cont.)
mode	listener	Specifies the SRT Connection Mode (to simplify firewall traversal): • caller: The SRT stream acts like a client and connects to a server listening and waiting for an incoming call. • listener: The SRT stream acts like a server and listens and waits for clients to connect to it. • rendezvous: Allows calling and listening at the same time.Also, to simplify firewall traversal, Rendezvous Mode allows the encoder and decoder to traverse a firewall without the need for IT to open a port.
SRT to UDP Stream Conversion (ts-srt only)		
flipaddr	n/a	Specifies the destination IP address for the stream. See "SRT to UDP Stream Conversion (TS over SRT only)" on page 80.
flipport	n/a	Specifies the UDP source port for the stream.
flipttl	64	(Time-to Live for stream packets) Specifies the number of router hops the stream packet is allowed to travel/pass before it must be discarded. 1..255
fliptos	184 or 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 The Multicast address range is from 224.0.0.0 to 239.255.255.255. Multicast addresses from 224.0.0.0 to 224.0.0.255 are reserved for multicast maintenance protocols and should not be used by streaming sessions. We recommend that you use a multicast address from the Organization-Local scope (239.192.0.0/14).

STREAM EXAMPLES

# stream create addr= 10.6.230.106 port=2000	Creates a streaming session from IP Address 10.6.230.106 at port 2000.
# stream 1 get all	Returns configuration information for decoder stream #1, such as: Stream ID : 1 Name : (None) Configuration: Address : 236.65.140.44 UDP Port : 4440 Encapsulation : TS-UDP Statistics: State : Streaming Output : DECODER-1 Bitrate : 6,781 kbps Received Packets : 20,135,282 Received Bytes : 1,745,649,664 Lost Packets : 0
# stream 10 get all # stream 10 get all [cont]	Returns configuration information for decoder stream #10, where it is an SAP Discovered stream: Stream ID : 10 Name : "DVI42" Configuration: Address : 239.146.42.101 (SAP Discovered) UDP Port : 4900 Encapsulation : TS-UDP Statistics: State : STOPPED Output : Not Configured Bitrate : 0 kbps Received Packets : 0 Received Bytes : 0 Received Errors : 0

# stream 1 get stats	Returns status information for decoder stream #1, such as: Stream ID : 1 Name : (None) Statistics: State : Streaming Output : DECODER-1 Bitrate : 6,543 kbps Received Packets : 20,231,121 Received Bytes : 1,973,649,408 Lost Packets : 0
# stream 1 delete	Deletes Stream #1.

Related Topics

- "Setting Up Decoder Streams" in Chapter
- "Stream Statistics" on page 81

talkback

Synopsis

talkback ID start [timeout=X(in secs)]

talkback stop

talkback set

talkback get

talkback clear

Description

The talkback command is used to start and stop transmission of audio talkback and manage audio talkback settings.

Actions

start	Starts transmission of talkback audio for the specified decoder (1 or 2). Time is specified in seconds (default is 30 seconds). timeout=0 means infinity.
stop	Stops transmission of talkback audio.
set	Configures talkback settings. A series of one or more parameter=value pairs can be specified at once.
get	Displays talkback information (i.e., the UDP port). You can specify configuration, stats, or all talkback information.
clear	Clears talkback statistics

Talkback Parameter

Parameter	Default	Description/Values
port	9177	UDP port on which to send for talkback audio packets. Should match the encoder's output port.

Talkback Examples

```
# talkback 1 start
```

Starts transmission of audio talkback on decoder #1. If not specified, the duration is 30 seconds (default).

Returns the following:

```
Talkback started successfully.
```

```
# talkback get
```

Returns the following audio talkback configuration:

```
  UDP Port                  : 9233
```

```
# talkback get all
```

Returns talkback configuration and statistics, such as:

```
Configuration:
  UDP Port                  : 9233
Statistics:
  State                     : STOPPED
  Transmitted Packets       : 2,823
  Transmitted Bytes         : 2,484,240
  Last Transmitted          : 1s ago
  Last Decoder ID           : 1
  Destination Address       : 10.65.10.124
  Last Tx Time Length       : 30 (Secs)
  Received Packets          : 2,823
  Received Bytes            : 2,484,240
```

```
# talkback 1 start timeout=60
```

Starts transmission of audio talkback on decoder #1 for 60 seconds.

Returns the following:

```
Property "timeout=60" set successfully.
Talkback started successfully.
```

```
# talkback 2 start timeout=0
```

Starts transmission of audio talkback on decoder #2 with no auto shut-off.

```
# talkback get all
```

Returns talkback configuration and statistics, such as:

```
Configuration:
  UDP Port                  : 9233
Statistics:
  State                     : TRANSMITTING
  Transmitted Packets       : 3,027
  Transmitted Bytes         : 2,663,760
  Last Transmitted          : 0s ago
  Last Decoder ID           : 1
  Destination Address       : 10.65.10.124
  Last Tx Time Length       : 60 (Secs)
  Received Packets          : 3,027
  Received Bytes            : 2,663,760
```

```
# talkback set port=9233
```

Sets the UDP port to 9233.

Related Topics

- "Audio Talkback" on page 32
- "service" on page 216
- For "Talkback Audio Format Specifications", please refer to the Makito X User's Guide

temperature

SYNOPSIS

temperature get

DESCRIPTION

The temperature command is used to display the current temperature of the unit.

ACTIONS

get	Displays the current temperature status of the unit.

TEMPERATURE EXAMPLE

# temperature get	Displays the current temperature for the unit, see example below: Temperature Status: Current Temperature : 35 Celsius measured 2s ago Maximum Temperature : 36 Celsius measured 5d2h9m2s ago Minimum Temperature : 32 Celsius measured 5d5h34m2s ago

viddec

Synopsis

viddec ID start

viddec ID stop

viddec ID set parameter=value [parameter=value ...]

viddec ID get [config, stats, all]

viddec ID clear

Description

The viddec command is used to manage video decoding for the SDI 1 and SDI 2 ports. This includes binding the video outputs to the streams and configuring properties such as the Output Resolution and Frame Rate.

Each decoder channel can support an alternate (secondary) stream as input which is switched to if the primary fails in order to minimize down-time.You can also select a Still Image such as a black screen that the decoder will display if it is no longer receiving video (for example, if the encoder stream has stopped or the network connection is lost).

Actions

start	Activates decoding of the video input.
stop	Stops (mutes) decoding of the video input.
set	Modifies decoder video parameter(s). A series of one or more parameter=value pairs can be specified at once. See viddec Parameters below.
get	Displays decoder video status information. You can specify to display the configuration (config), stats, or all.
clear	Clears the decoder's statistics.
help	Displays usage information for the viddec command.

viddec Parameters

Parameter	Default	Description/Values
streamId	n/a	Specifies the primary stream to bind to the video output. Positive stream index. See "Configuring Decoder Outputs" on page 86.
altStreamId	n/a	Specifies the alternative stream to bind to the video output. Positive stream index. See "Configuring Decoder Outputs" on page 86.

Parameter	Default	Description/Values (Cont.)
frameRate	Auto	The output frame rate for the displays. Auto, 23, 24, 25, 29, 30, 50, 59, 60, 75 If Auto is selected, the actual frame rate generated will be the next highest valid frame rate supported by the SDI interface, plus the one that gives the best decimation factor. For example, 30Hz could be chosen instead of 29.970 Hz. Values set which are impossible to implement will be treated as Auto. Reasons for not supporting the selection can range from "Display does not support the frame rate" or "Frame rate is undefined for the detected input resolution".
stillImage	freeze	The type of static image to display when the decoder is not receiving a video stream.
		• freeze: continues to display the last decoded video frame.
		• black: displays a black screen.
		• blue: displays a blue screen.
		• bars: displays a series of vertical color bars across the width of the display.
		• mute: disables the video output.
		• custom: displays a custom static image. See "mkstill" on page 198. NOTE: When the still image is substituted on the display outputs, the video frame rate and resolution will be maintained. When the video decoder receives a new video stream, it will wait until it receives a new IDR frame and will re-start the display with that IDR frame.
stillDelay	3	The delay in seconds before the still image is displayed. 1...1000
stillFile	n/a	File name of custom still image.

Parameter	Default	Description/Values (Cont.)
resolution	n/a	The output resolution: • Auto: The decoder will select an output resolution that attempts to closely match the coded picture resolution, taking into account the capabilities of any displays connected to the HDMI interface. • Native: The output resolution will be exactly the same as the coded picture resolution. If the coded picture resolution is not compatible with the output interfaces, nothing will be displayed. See "Output Resolution" on page 93. • 1080p, 720p, 1080i, 480i, 576i, 480p, 576p, Xga, Sxga, Vga, Svga, 1152x864p, 1280x768p, 1280x800p, 1360x768p, 1366x768p, 1400x1050p, 1440x900p, 1600x900p, 1600x1200p, 1680x1050p, 1920x1200p
syncmode	stc	The mode of synchronization of sound and picture for the decoded stream: • stc: Synchronizes with the encoder system clock by comparing the packet timestamp with the reference clock. • passthrough: Decodes packets without comparing the packet timestamp to synchronize video and audio. This may result in A/V sync issues, but may be required in circumstances where network performance hinders synchronization. See "Video Decoder Buffering Passthrough" on page 235.

Parameter	Default	Description/Values (Cont.)
buffering	automatic	(syncmode must be stc) The type of buffering to use. A jitter buffer temporarily stores arriving packets in order to remove the effects of jitter from the decoded stream. • Automatic: Automatic mode favors smooth playing content with good synchronization between audio and video. The incoming stream is monitored and the optimal required delay is determined so that stream packet and video picture jitter is absorbed. The calculated delay may change slowly as network and video conditions change. See "Mode" on page 92. • Fixed: Fixed mode allows users to specify a delay to be added to the decode pipeline after the content is decoded. The amount of delay does not vary and artifacts may result if a too low value is used. NOTE: The decoder has a minimum buffer set based on the resolution and frame-rate of the stream content. In addition, users can add more delay if desired: (1) to achieve a specific decoding latency for inter-channel synchronization purposes; (2) to deal with unusually large amounts of jitter in the stream; or (3) to allow A/V sync to occur when the stream content is highly out of sync. (See delay below.) Adaptive (Low-Latency): The decoder measures the stream packet and video picture jitter and adds in a delay so that artifacts are minimized while also minimizing video latency. Provides backward compatibility with older decoder versions. NOTE: Audio artifacts may occur if audio is streamed after video when using Adaptive Low Latency.
delay	0	The delay in ms when using stc syncmode with fixed buffering. 0..2000ms (Interlace) 0..33ms (Progressive)

VIDDEC EXAMPLES

# viddec 1 get all	Returns video configuration information and statistics for decoder #1, such as: Decoder ID : 1 Configuration: Stream ID : 1 State : STARTED Resolution : Auto Frame Rate : Auto Still Image : Freeze Still Delay : 3 (s) Sync Mode : Stc Buffering : Fixed Delay : 0 (ms) Statistics: State : Running Hdmi Output : Yes Up Time : 0 days 16 hours 11 minutes 31 seconds Number of Restarts : 0 Video: State : Invalid Input Format : 1920x1080 Interlaced Output Format : 1080i30 Bitrate : 9964 kbps Framerate : 30 Decoded Frames : 128870 Displayed Frames : 128448 Skipped Frames : 218 Replayed Frames : 0 Displayed Errors : 0 Audio: State : Running Bitrate : 128 kbps Sample Rate : 48 Hz Algorithm : AACLC/LATM Number of Pairs : 1 Decoded Frames : 201357 Output Frames : 201350 Output Errors : 0 KLV : Not Present CC : Not Present TC : Not Present AFD : Not Present

# viddec 1 set stillimage=blue	Sets the static image to blue. You will receive the following confirmation: Decoder configured successfully.
# viddec 1 get stats	Returns video configuration statistics for decoder #1, such as: Decoder ID : 1 Statistics: State : Running Active Stream ID : 1 Hdmi Output : Yes Up Time : 0 days 20 hours 20 minutes 53 seconds Number of Restarts: 0 Audio vs Video delay: ~ 35 ms (Video late) Add A/V latency : 0 ms (Added Video and Audio delay due to important video frame jitter) Est Video jitter : 5 ms Video: Algorithm : H.264 State : Running Input Format : 1280x720 Progressive Output Format : 720p60 Still Image : Freeze (Not Active) [Count=0] Bitrate : 10,022 kbps Framerate : 60 Decoded Frames : 4,395,049 Displayed Frames : 4,394,707 Skipped Frames : 128 Replayed Frames : 95 Audio: Algorithm : AACLC/ADTS State : Running Bitrate : 127 kbps Sample Rate : 48 kHz Number of Pairs : 1 Decoded Frames : 3,433,632 Output Frames : 3,433,630

TIP The stream type is automatically determined on decoder startup. The viddec Video Algorithm statistic shows which codec algorithm (H.264 or HEVC) is in use for a decode channel.

VIDEO DECODER BUFFERING PASSTHROUGH

Passthrough is a special mode that instructs the decoder to bypass its internal jitter buffer and output video/audio as data becomes available to play (while maintaining AV sync). Normally, the decoder will adapt to the detected network jitter to preserve smooth play of the video. Passthrough mode is intended for use within QoS-enabled enterprise class networks that have well controlled network jitter.

The advantage of this mode is a perceptible reduced latency

The side effect of passthrough is that, occasionally, even the most pristine networks may have issues that, when passthrough mode is enabled, are more likely to cause the decoder to drop or replay a video frame.

Related Topics

- "Configuring Decoder Outputs" on page 86
- "Video Decoder Statistics" on page 95

APPENDIX B: Technical Specifications

This appendix lists the technical specifications for the Makito X decoder.

Topics In This Appendix

Audio/Video Interfaces

Video Outputs:	
HDMI 1.4	
SD-SDI	SMPTE 259M-C
HD-SDI	SMPTE 292M & 296M & 274M
3G-SDI	SMPTE 424M (Level A only) & 425M

Audio Outputs:
Two analog audio channels per blade
Up to 8 channels of embedded audio per blade, in channel pair groups. The channel pair sources are: • SDI1ch1&2, SDI1ch3&4, SDI1ch5&6, SDI1ch7&8 • SDI2ch1&2, SDI2ch3&4, SDI2ch5&6, SDI2ch7&8
Available through a mini-DIN-8 locking connector: • Balanced / Unbalanced stereo analog audio

Digital Embedded Audio	
SD-SDI	SMPTE 272M
HD/3G-SDI	SMPTE 299M
HDMI 1.4	

Talkback:
Analog Audio Input • Level: 2.2 dBu (1Vrms) • Impedance: 100 Ohms

Video Decoding

Video Output (TV) Resolutions:	
Supported by SDI	
1920x1080p	60/59.94/50/30/29.97/25/24/23.98 Hz
1920x1080i	60/59.94/50 Hz
1280x720p	60/59.94/50/30/29.97/25 Hz
720x576i	50 Hz
720x480i	60/59.94 Hz
(interlaced shown in fields per second)	
See "Supported Decoding TV/Computer Resolutions" on page 239.	
Supported by HDMI	
1920x1080p	60/59.94/50/30/29.97/25/24/23.98 Hz
1920x1080i	60/59.94/50 Hz
1280x720p	60/59.94/50 Hz
720x576p	50 Hz
720x576i	50 Hz
720x480p	60/59.94 Hz
720x480i	60/59.94 Hz
(interlaced shown in fields per second)	
Computer Output Resolutions: (supported only by HDMI)	
1920x1200	60 Hz
1680x1050	60 Hz
1600x1200	60 Hz
1600x900	60 Hz
1440x900	60 Hz
1400x1050	60 Hz
1366x768	60 Hz
1360x768	60 Hz
1280x1024	60 Hz
1280x800	60 Hz
1280x768	60 Hz
1152x864	75 Hz
1024x768	60 Hz
800x600	60 Hz
640x480	60 Hz
NOTE: All computer output resolutions are progressive.	
See "Supported Decoding TV/Computer Resolutions" on page 239.	

Video Bit Rates:
SD/HD from 32 kbps to 25 Mbps (Single Channel H.264 video)
SD/HD from 32 kbps to 14 Mbps (Single Channel HEVC video))
Compression Standards:
H.264 (MPEG-4 AVC part 10) ISO/IEC 14496-10 Baseline, Main, and High Profiles Up to Level 4.2 (1080p60) and lower intermediate levels I, IP, IBP, IBBP framing
H.265/HEVC ISO/IEC 23008-2 Main Profile Up to Level 4 (1080p60) IP framing

Supported Decoding TV/Computer Resolutions

The Makito X decoder accepts many input resolutions and frame rates and will scale as appropriate to a supported resolution as listed in the "Video Decoding" table on page 238, with the following limitations:

- A received stream with progressive video cannot be output as interlaced. If the input stream is progressive, the decoder will display progressive.
- Users may manually select a specific output resolution if the automatic choice does not produce the desired results.

Audio Decoding

Audio Decoding	
Audio Channels	• 2 Analog audio per blade • SDI Embedded audio (4 or 8 audio pairs) per output port • HDMI Embedded audio pairs per blade) NOTE: When the decoder is licensed for one channel only, it mirrors the decoded stream to all interfaces and supports up to eight (8) channel pairs of AAL-LC audio decoding for a stream. See "Audio Channel Details/Breakout" below.
Audio Bit Rates	• Mono: From 56 to 160 kbps per audio pair • Stereo: From 80 to 320 kbps per audio pair
Frequency Response	From 20 Hz to 22 kHz
Sampling Rate	48kHz
Maximum Analog Audio Output Level	From +5dBu to +20dBu (balanced or unbalanced) (+6dBu = default)
Compression Standards	• MPEG-2 AAC-LC ISO/IEC 13818-7 • MPEG-4 AAC-LC ISO/IEC 14496-3

Audio Channel Details/Breakout	
Analog Audio	
Single Channel	Analog audio can select any channel pair in a stream up to the eighth pair: • SDI1ch1&2, SDI1ch3&4, SDI1ch5&6, SDI1ch7&8, SDI1ch9&10, SDI1ch11&12, SDI1ch13&14, SDI1ch15&16
Dual Channel	Analog audio can select from the first 4 channel pairs of either SDI interface: • SDI1ch1&2, SDI1ch3&4, SDI1ch5&6, SDI1ch7&8 • SDI2ch1&2, SDI2ch3&4, SDI2ch5&6, SDI2ch7&8

Audio Channel Details/Breakout	
HDMI Embedded Audio	
Single Channel	HDMI embedded audio can select either a single channel pair or a set of four channel pairs when in surround sound: Single Pair: • SDI1ch1&2, SDI1ch3&4, … SDI2ch15&16 Surround Sound uses up to 4 channel pairs from: • SDI1
Dual Channel	Single Pair: • SDI1ch1&2, SDI1ch3&4, … SDI1ch7&8 • SDI2ch1&2, SDI2ch3&4, … SDI2ch7&8 Surround Sound uses up to 4 channel pairs from: • SDI1 or SDI2
SDI Embedded Audio	
Single Channel	Supports up to 16 channels (8 channel pairs) of embedded audio on the SDI interface: • SDI1ch1&2, SDI1ch3&4, … SDI2ch15&16
Dual Channel	Supports up to 8 channels (4 channel pairs) of embedded audio per SDI interface: • SDI1ch1&2, SDI1ch3&4, SDI1ch5&6, SDI1ch7&8 • SDI2ch1&2, SDI2ch3&4, SDI2ch5&6, SDI2ch7&8

Advanced Features

Advanced Features
HD/SD de-interlacing
Built-in downscaling
EIA-708-B/SDI closed captioning
Forward Error Correction (FEC)
AES decryption 128-bit or 256-bit with Furnace & SRT
Active Format Description (AFD)
Advanced buffering control
Still image insertion on loss of input stream

Metadata (Optional)

Output Metadata Features
KLV over SD-SDI/HD-SDI/3G-SDI
Metadata Processing:
SMPTE 336M compliant
CC 608/708 pass-through
MISB 0601.11 Compliant
MISB 0604.2 Compliant, supporting Synchronous and Asynchronous formats
SMPTE 12M Timecode
SMTPE 2016 AFD

NOTE KLV Metadata may be de-encapsulated from a supported format and provided to an SDI output interface. KLV metadata is inserted into the VANC of the video frame whose PTS most closely matches the PTS associated with the KLV AU.

Network and Management Interfaces

IP Network and Management Interfaces	
Networking Standards	Ethernet 10/100/1000 Base-T, Auto-detect, Half/full-Duplex
	IPv4 (Internet Protocol Version 4)
	DHCP (Dynamic Host Configuration Protocol)
	IGMPv3 (Internet Group Management Protocol) for IP Multicast
	DNS (Domain Name System)
Connector	RJ45 (TIA/EIA-568)
Streaming Protocols	Unicast Streaming
	Multicast Streaming
	MPEG Transport Stream over UDP / RTP
	Secure Reliable Transport (SRT)
	MPEG2 Transport Stream as per ITU-T Rec. H.222.0 | ISO/IEC 13818-1 and RFC 2250
	SAP (RFC 2974)
Management Protocols	HTTPS (Web browser)
	Command line over SSH / Telnet / RS-232
	SFTP / TFTP / SCP
	SNMP v3

Chassis Options

Single-Height Appliance

Single Height Appliance (#S/B-292D-HD2)	
Dimensions (H x W x D)	24mm H x 149mm W x 202mm D (0.92” H x 5.85” W x 8.0” D)
Weight	Approximately 1.13 kg (2.5 lbs.)
Power Requirements	12VDC, 20W (each single-height blade) 100-240VAC 30W external power supply NOTE: IEC 60601-1 Class I and II power supplies are available from Haivision.
Temperature	Operating: 0° to 40°C (32° to 104°F) Non-operating*: -30° to 70°C (-22° to 158° F) *Limited by the power supply storage: -30°C
Relative Humidity	Up to 95% without condensation
Heat	20 Watts or 68 BTU/hr
Sound Emission	41.2 dB(A) L’p(AVG)

Dual-Height Appliance (HEVC Mezzanine)

Dual Height Appliance (#S/B-292D-HD1-HEVC OR S/B-292D-HD2-HEVC)	
Dimensions (H x W x D)	44mm H x 149mm W x 202mm D (1.74” H x 5.85” W x 8.0” D)
Weight	Approximately 1.36 kg (3 lbs.)
Power Requirements	12VDC, 25W (each double-height blade) 100-240VAC 60W external locking power supply NOTE: IEC 60601-1 Class I and II power supplies are available from Haivision.
Temperature	Operating: 0° to 40°C (32° to 104°F) Non-operating*: -30° to 70°C (-22° to 158° F) *Limited by the power supply storage: -30°C
Relative Humidity	Up to 95% without condensation
Heat	~20 Watts or 68.3 BTU/hr
Sound Emission	41.2 dB(A) L’p(AVG)

MB6X - 6 Blade Chassis

MB6X - 6 Blade Chassis (#F-MB6X-RAC, F-MB6X-MED or F-MB6X-DC)	
Dimensions (H x W x D)	19” rack mountable, 1 RU 43.69mm H x 434.98mm W x 420.37mm D (1.72” H x 17.125” W x 16.55” D)
Weight	6 slot empty chassis: 7.94 kg. (17.5 lbs.) Single decoder blade: 230 g. (0.5 lbs.)
Power Requirements	Single Internal Power Supply: • Redundant AC type: 90-264VAC 47Hz-63Hz 300 Watt max. • Medical Grade: 90-264VAC 47Hz-63Hz 300 Watt max. • DC type: 20-36 VDC 300 Watt max.
Temperature	Operating: 0° to 50°C (32° to 122°F) Non-operating: -40° to 70°C [-40° to 158° F)
Relative Humidity	Up to 95% without condensation
Heat	155 Watts or 530 BTU/hr
Sound Emission	• Room temperature: 57.0 dB(A) L’p(AVG) • 50°C Ambient: 65.9 dB(A) L’p(AVG)

MB21B (#F-MB21B-R)

MB21 - 21 Blade Chassis (#F-MB21B-R)	
Dimensions (H x W x D)	19-inch rack mountable, 4RU 178 mm H x 439.98 mm W x 460 mm D (7.00 inches H x 17.125 inches W x 18.00 inches D)
Weight	Empty 21-slot chassis: 38 pounds Each blade: 0.5 pounds
Power (internal power supply)	Quad redundant power supplies: • 90-132V and 180-240VAC 47Hz-63Hz • 400 watt maximum per PSU
Temperature	Operating: 0°C to 40°C (32°F to 104°F) Non-operating: -40°C to 70°C (-40°F to 158°F)
Relative Humidity	Up to 95% without condensation
Heat	560 Watts or 1910 BTU/hr *assumes chassis full of Makito X or other Haivision blades;
Sound Emission	• Room temperature: 56.4 dB(A) L'p(AVG) • 50°C Ambient: 63.3 dB(A) L'p(AVG)

MB21X (#F-MB21X-R)

MB21 - 21 Blade Chassis (#F-MB21X-R)[1]	
Dimensions (H x W x D)	19-inch rack mountable, 4RU *178 mm H x †441.35 mm W x 462 mm D (7.00 inches H x 17.38 inches W x 18.19 inches D) *187 mm / 7.35 inches H with rubber feet installed †482.6 mm / 19 inches W including mounting flanges
Weight	Empty 21-slot chassis: 32.5 pounds Each blade: 0.5 pounds
Power (internal power supply)	Dual redundant power supplies: • 100-240VAC 47Hz-63Hz • 600 watt maximum per PSU
Temperature	Operating: 0°C to 50°C (32°F to 122°F) Non-operating: -40°C to 70°C (-40°F to 158°F)
Relative Humidity	Up to 95% without condensation
Heat	560 Watts or 1910 BTU/hr *assumes chassis full of Makito X blades
Sound Emission	• Room temperature: 56.4 dB(A) L'p(AVG) • 50°C Ambient: 63.3 dB(A) L'p(AVG)
Advanced Features	• Removable fan trays • Station Alarm Interface

1. Supports Makito X products *only*; excludes classic Makito encoder/decoder or Torpedo blades

Makito X Harsh Decoder Environment Chassis Option

Makito X Harsh Decoder Environment Chassis Option (#S-292D-X2H)	
Fanless operation for high temperature applications	
Dimensions	44mm H x 137mm W x 202mm D (1.73” H x 5.4” W x 8.0” D)
Weight	1.8 kg (4lbs.)
Power	12VDC, 20W 100-240VAC 30W external locking power supply
Temperature	Operating: -20º to 70ºC (32º to 158ºF) Non-operating: -40º to 85ºC (-40º to 185ºF)
Relative Humidity	0-95% condensing
IP rating	IP42

Regulatory/Compliance

Regulatory/compliance	
Certification	UL / CSA / CE
Compliance	Electromagnetic Compatibility: EN 55022 (Emissions) / 55024 (Immunity) / EN 61000-3-2 / EN 61000-3-3
	Safety (Low Voltage Directives): EN 60950-1 (CSA C/US) / IEC/EN 60950-1 (International /CB Scheme)
	Industry Canada Warnings: Canadian ICES-003, “Electromagnetic Compatibility” / Avis d’Industrie Canada: la norme NMB-003 du Canada, “La Compatibilité électromagnétique”
	FCC Part 15, Subpart B, Class A
Compliance with Environmental Regulations	RoHS2, European Union Directive 2011/65/EU
	RoHS, Marking Control for China, Regulation SJ/T 11364-2006
Sound Emission	Telcordia GR-63 Section 4.6

NOTE Please refer to the product Declaration of Conformity (DoC) for complete details.

APPENDIX C: Open Source Software Credits

This appendix lists the Open Source software packages currently deployed on the Makito X decoder platform. For more details, please consult the provider of the package.

References

GNU General Public License v2: GPL-2.0

GNU General Public License v3: GPL-3.0

GNU Lesser General Public License v2: LGPL-2.1

BSD type licenses, or those describe by Regents of the University of California identifier are typically described by the following: BSD-2-Clause and BSD-3-Clause (revised BSD license).

Permissive Free Software License: Rights are owned by an individual, group of individuals, institution or consortium but is generally free provided minimal conditions are met. See: Permissive free software licence wikipedia entry for more information.

Open Source Software Credits

Package	Version	Description	License
Linux kernel	2.6.37	Linux Kernel	GPL v2, June 1991
Linux-PAM	1.1.3	Linux Pluggable Authentication Module	permissive free software license or GPL V2
bash	4.3.30	Bourne Again Shell - Posix.2 Shell	GPL v3, June 2007
beecrypt	4.2.1	Cryptography Library	LGPL v2.1
busybox	1.17.3	Common UNIX utilities.	GPL v2, June 1991.
chkconfig	1.3.30c	Service run level configuration	GPL v2, June 1991

Package	Version	Description	License
coreutils	8.9	Basic shell, file and text manipulation	GPL v3, June 2007
cracklib	2.8.18	Password checking library	LGPL v2.1 - June 1999
cron	3.0p11	Time base job scheduler	permissive free software license
db	5.1.19	Berkeley Relational Database Library	Oracle 2010 (redistribute as-is) + Berkeley type license
dpkg	1.16.0	Debian Package Manager System	GPL v2 - June 1991
ethtool	2.6.38	Network interface controller configuration	GPL v2 - June 1991
ffmpeg	3.0.0	Multimedia framework	LGPL v2.1
gawk	3.1.8	GNU AWK - Pattern scanning and processing.	GPL v3 - June 2007
ifupdown	0.6.10	Network Interface Configuration	GPL v2 - June 1991
initscripts	9.22	Run level scripts and assoc processing	GPL v2 - June 1991
iperf	2.0.5	Internet Bandwidth Measurement Tool	University of Illinois - permissive free software license
iproute2	2.6.38	Linux TCP/IP traffic control	GPL v2 - June 1991
ipv4ll	1.5	Simple IPv4 Link-Local addressing	LGPL v2.1
jpeg	8b	JPEG Software Tools	Lane & Vollbeding - permissive free software license
libevent	2.0.17	Event notification library	3-clause (“modified”) BSD License
lighttpd	1.4.41	Lightweight open-source Web server	Jan Kneschke, 2004 - permissive free software license

Package	Version	Description	License
mDNS responder	320.10.80	Multicast Domain Name System	Apache License 2.0
mtd-utils	2.0	Memory Technology Device (MTD) utilities for nor, nand access and UBI & JFFS2 tools.	GPL v2 - June 1991
mtr	0.92	MyTraceroute: ping and traceroute combination in a single utility	BSD styled
ncurses	5.5	Text-base UI library	Permissive free software license
net-tools	1.60	Network tools.	GPL v2 - June 1991
netkit-ftp	0.17	File Transfer Protocol	Regents of the University of California
netkit-telnet	0.17	Telnet	Regents of the University of California
net-snmp	5.5.2	Simple Network Management Protocol	Multiple BSD Licenses
nsyslog	1.84	syslog for NetBSD	BSD License
ntp	4.2.8p10	Network Time Protocol	University of Delaware - Permissive free software license
openssh	7.3p1	Open SSH	Multiple BSD style licenses.
openssl	1.0.2k	Open Secure Socket Layer	Dual OpenSSL / SSLeahy
openssl-fips-algvs	2.0	FIPS Algorithms	Multiple Licenses.
pcre	8.21	Perl Compatible Regular Expression Library	BSD License
popt	1.16	Command Line Parsing Library	Permissive free software license

Package	Version	Description	License
postgresql	7.4.1	Postgresql database (support library)	Permissive free software license - (PostgreSQL Development Group and Regents of the University of California)
procps	3.2.8	Process reporting utilities.	GPL v2 - June 1991
readline	6.1	Command Line Editing Library	GPL v3 - June 2007
rng-tools	4	Random Number Generator tools	GPL v2, June 1991
rpm	4.4.2.3	RPM Package Manager	Dual GPL v2 - June 1991 and LGPL v2 - June 1991
sed	4.2	Stream Editor	GPL v3 - June 2007
shadow	4.1.4.2	Shadow Passwords	Permissive free software license.
sudo	1.8.4p5	Privilege modification	Free Software Foundation - Permissive free software license
sysstat	10.0.0	Performance monitoring tools for Linux	GPL v2 - June 1991
sysvinit	2.88dsf	Init process	GPL v2 - June 1991
tcp_wrappers	7.6	Host base networking Access Control System	Permissive free software license.
tcpdump	4.3.0	Network monitoring and acquisition	BSD
tftp-hpa	0.43	tftp server	Permissive free software license.
u-boot	2010.06	U-Boot boot loader	GPL v2 - June 1991
UDT4	4.11	UDP-based Data Transfer	Permissive free software license
zlib	1.2.5	Compression library	Jean-Loup Gailly - Permissive free software license.

Open Source Software Credits

Please refer to the URLs listed above for details of each Open Source licensing agreement. Code for GPL-related components is available upon request.

APPENDIX D: Warranty Information

Haivision One (1) Year Limited Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

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

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

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

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

4.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 available on our Download Center at https://support.haivision.com. If the product is still not functioning properly after making use of these resources, please contact your Authorized Reseller or Haivision at http://support.haivision.com using the information provided in the documentation. The Authorized Reseller or Haivision 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.

Software End User License Agreement

READ BEFORE USING

THIS SOFTWARE END USER LICENSE AGREEMENT ("AGREEMENT") IS FOR ANY OR ALL OF THE HAIVISION SOFTWARE PRODUCT(S) LICENSED, DOWNLOADED, INSTALLED AND/OR ACTIVATED BY YOU ("PRODUCT"). THE PRODUCT IS PROTECTED BY NATIONAL AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES.

READ THE TERMS OF THE FOLLOWING AGREEMENT CAREFULLY. BY CLICKING THE ACCEPT BUTTON ON THIS AGREEMENT, OPENING THE SHRINKWRAP AROUND OR USING THE PRODUCT OR ANY PORTION THEREOF, OR BY USING OR DISTRIBUTING ANY VIDEO INFORMATION ENCODED BY, DECODED BY OR OTHERWISE MANIPULATED OR PASSED THROUGH THE PRODUCT, YOU CONFIRM YOUR ACCEPTANCE OF THIS AGREEMENT.

THIS AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (A SINGLE CORPORATE ENTITY) AND HAIVISION. IF YOU DO NOT AGREE TO THESE TERMS, HAIVISION IS UNWILLING TO LICENSE THE PRODUCT TO YOU AND YOU ARE NOT AUTHORIZED TO INSTALL OR USE THE PRODUCT.

NOTWITHSTANDING SECTION 6.5 BELOW, THIS AGREEMENT ONLY GOVERNS THE PRODUCT(S) IF A SEPARATE SOFTWARE END USER LICENSE AGREEMENT HAS NOT BEEN SIGNED PRIOR TO THIS AGREEMENT FOR THE PRODUCT OR THE AGREEMENT IS NOT SUPERCEDED BY A SEPARATE SOFTWARE END USER LICENSE AGREEMENT FOR THE PRODUCT AT A LATER DATE.

1. DEFINITIONS

1.1. Entitlement. The collective set of applicable documents (e.g., warranty, support and maintenance documents, data sheets, etc.) authorized by Haivision Network Video or its affiliate Haivision (collectively, "Haivision") evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Product under this Agreement.

1.2. License Fee. License Fee shall mean the consideration paid to Haivision for use of the Product. The License Fee is part or all of the price paid for the relevant Product.

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

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

1.5. Third-Party Content. Services or materials, which are not proprietary to Haivision or may not be part of the materials of the company, entity or individual using the Product.

1.6. Updates. Updates shall mean any periodic software releases, additions, fixes, and enhancements thereto, release notes for the Product and related Reference Manuals, (other than those defined elsewhere in this section as Upgrades) which have no value apart from their operation as part of the Product and which add minor new functions to the Product, but none so significant as to warrant classification as an Upgrade, which may be provided by Haivision to fix critical or non-critical problems in the Product on a scheduled, general release basis. Updates to the Product ("Version") are denoted by number changes to the right of the decimal point for a version and revision number (for example, going from 2.0.0 to 2.1.0).

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

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

2. RIGHTS AND RESTRICTIONS

2.1. License to Use. Subject to the terms and conditions set forth herein and subject to the terms of your Entitlement, Haivision hereby grants to You a non-exclusive, personal, limited and nontransferable right and license to use the Product in accordance with the terms of this Agreement. This license is granted to You and not, by implication or otherwise, to any parent, subsidiary or affiliate of Yours without Haivision's specific prior written consent. This license is for the limited use of the Product by You for the purpose of creating, managing, distributing and viewing IP Video assets. This license does not grant any license for content whatsoever. All rights not expressly granted to You by this Agreement are reserved by Haivision.

2.2. Restrictions.

(a) Reproduction. You shall not copy, modify, distribute, use or allow access to any of the Product, except as explicitly permitted under this Agreement and only in the quantities designated in the Entitlement. However, You have the right to make copies of the Product solely for archival purposes, but only in quantities necessary and typical for your Organization. You shall not modify, adapt, translate, export, prepare derivative works from, decompile, reverse engineer, disassemble or otherwise attempt to derive source code, hardware designs or other proprietary information from the Product or any internal data files generated by the Product, or use the Product embedded in any third party hardware or software. You shall also not use the Product in an attempt to, or in conjunction with, any device, program or service designed to circumvent technological measures employed to control access to, or the rights in other work protected by copyright laws. You shall not remove, modify, replace or obscure Haivision's copyright and patent notices, trademarks or other proprietary rights notices affixed to or contained within any Product. No right is granted hereunder for any third party who obtains access to any Product through You to use the Product to perform services for third parties. Most sublicensing arrangements are prohibited under this Agreement. However, if You are a Reseller, You are permitted to sublicense the Product to single end-users under terms and conditions similar to the provisions of this Agreement; however, You are responsible and liable pursuant to the terms and conditions of this Agreement for Your sublicensees' actions and failures to take required actions with respect to the Product.

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

3. TERM AND TERMINATION

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

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

3.3. Termination for Bankruptcy. Haivision may terminate this Agreement, effective immediately, if You file, or have filed against You, a petition for voluntary or involuntary bankruptcy or pursuant to any other insolvency law, makes or seeks to make a general assignment for the benefit of its creditors or applies for, or consents to, the appointment of a trustee, receiver or custodian for a substantial part of its property.

3.4. Termination; Effect; Survival. Upon the termination of this Agreement for any reason:

(a) All license rights granted hereunder shall terminate;

(b) You shall immediately pay to Haivision all amounts due and outstanding as of the date of such termination or expiration; and

(c) You shall return to Haivision all Product and all Haivision Reference Manuals or certify that all such Product and Reference Manuals have been destroyed. Notwithstanding any termination of this Agreement, the following provisions of this Agreement shall survive for the relevant period of time set forth therein, if any: Sections **2.2**, **4**, **5** and **6**.

4. REPRESENTATIONS, DISCLAIMER AND LIMITATION OF LIABILITY

4.1. Limited Warranty. Haivision warrants that: (i) the Product will operate substantially in accordance with the Reference Manuals provided and (ii) any media on which the Product is provided will be free of material damage and defects in materials and workmanship under normal use for a term of ninety (90) days (the "Warranty Period") after its delivery date. As Your sole and exclusive remedy for any breach of this warranty, Haivision will use its commercially reasonable efforts to correct any failure of the Product to operate substantially in accordance with the Reference Manuals which is not the result of any improper or unauthorized operation of the Product and that is timely reported by You to Haivision in writing within the Warranty Period, provided that in lieu of initiating commercially reasonable efforts to correct any such breach, Haivision may, in its absolute discretion, either: (i) replace the Product with other software or technology which substantially conforms to the Reference Manuals or (ii) refund to You a portion of the fee paid for the relevant Product, whereupon this Agreement shall terminate. This warranty shall immediately terminate if You or any third party makes or attempts to make any modification of any kind whatsoever to the Product, engages in any improper or unauthorized operation of the Product, including uses prohibited by the Entitlement or installs or uses the Product on or in connection with any hardware or software not specified in the Entitlement or product data sheets.

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

4.3. Liability Limitation. IN NO EVENT SHALL HAIVISION OR ITS OFFICERS, EMPLOYEES, AGENTS, REPRESENTATIVES, OR MEMBERS, NOR ANYONE ELSE WHO HAS BEEN

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

5. INDEMNIFICATION

5.1. Indemnification by Haivision.

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

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

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

5.2. Indemnification by You. You shall indemnify and hold Haivision harmless against any and all Claims directly or indirectly arising out of, or in any manner whatsoever associated or connected with Your performance, purported performance or non-performance of your rights and obligations under this

Agreement, and against any and all Claims incurred by or on behalf of any of the foregoing in the investigation or defense of any and all such Claims.

6. OTHER PROVISIONS

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

6.2. Content. Your data and/or your use of the Product may not: (i) interfere in any manner with the functionality or proper working of the Product; (ii) stream any material that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including privacy and publicity rights, unless You are the owner of such rights or have permissions from the rightful owner to post the material; (iii) constitute, promote, facilitate or permit any illegal activities, including without limitation, activities that might be libelous or defamatory, invasive of privacy or publicity rights, abusive or otherwise malicious or harmful to any person or entity; (iv) distribute, share or facilitate unauthorized data, malware, viruses, Trojan horses, spyware, worms or other malicious or harmful distributions; or (v) otherwise violate, misappropriate or infringe the intellectual property, privacy, publicity, contractual or other proprietary rights of any third party.

6.3. Consent to Use Data. You agree that Haivision may collect and use technical data and related information, including but not limited to technical information about Your device, system and application software and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to You (if any) related to the Product. Haivision may use this information, as long as it is in a form that does not personally identify You, to improve its products or to provide services or technologies to You.

6.4. Transfer and Assignment. Haivision may assign, sublicense, or transfer this Agreement and/or any or all of its rights or obligations hereunder. You may not assign, transfer or delegate any of its rights or obligations hereunder (whether by operation of law or otherwise) without the prior written consent of Haivision. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation or reorganization involving You (regardless of whether You are a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations or performance under this Agreement for which Haivision's prior written consent is not required. Any unauthorized assignment, transfer or delegation by You shall be null and void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

6.5. Waiver and Amendment. No modification, amendment or waiver of any provision of this Agreement shall be effective, unless in writing signed by both parties. No failure or delay by either party in exercising any right, power or remedy under this Agreement, except as specifically provided herein, shall operate as a waiver of any such right, power or remedy. Without limiting the foregoing, any additional legal terms and conditions submitted by You in any other documents, including but not limited to the Entitlement, shall be of no legal force or effect.

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

6.7. Third Party Content. Haivision is not responsible for examining or evaluating the data, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of any Third Party Content. Haivision does not warrant or endorse and does not assume and will not have any liability or responsibility to You or any other person for any Third Party content. You agree that any Third Party Content may contain proprietary information and material that is protected by applicable intellectual property and other laws, including but not limited to copyright, and that you will not use such proprietary content, information or materials in any way whatsoever except for permitted uses of the Third Party Content.

6.8. Third Party Royalties. Your further reuse, retransmission, rebroadcast, display or other distribution of your Third Party Content using the Product may require that you obtain a license from and / or pay royalties to the owners of certain third party audio and video formats. You are solely responsible for obtaining such licenses and paying such royalties.

6.9. Governing Law/Submission to Jurisdiction. This Agreement shall be governed by and construed in accordance with the laws of the Province of Québec, Canada and the Laws of Canada applicable therein (excluding any conflict of laws rule or principle, foreign or domestic), exclusive of the U.N. Convention on the International Sale of Goods. You hereby consent to the jurisdiction of any provincial or federal court located within the Province of Quebec and waive any objection which You may have based on improper venue or forum non conveniens to the conduct of any proceeding in any such court.

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

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

6.12. Entire Agreement. This Agreement, together with the Entitlement and all other documents that are incorporated by reference herein, constitutes the sole and entire agreement between Haivision and You with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to such subject matter.

6.13. Language. The parties confirm that it is their wish that this Agreement, together with the Entitlement and any other documents relating hereto, have been and shall be drawn up in the English language only. Les parties conferment que c'est leur volonte expresse que ce contrat et tous documents y etant relative, y compris les bons de commande, le avis, le anneses, les autorisations, les pieces jointes et les amendments solent rediges en langue anglais seulement.

6.14. Headings Not Controlling. The headings used in this Agreement are for reference purposes only and shall not be deemed a part of this Agreement.

6.15. US Government Rights. Some Products are commercial computer software, as such, term is defined in 48 C.F.R. §2.101. Accordingly, if You, as the Licensee, is the US Government or any contractor therefor, You shall receive only those rights with respect to the Product and Reference Materials as are granted to all other end users under license, in accordance with:

(a) 48 C.F.R. §227.7201 through 48 C.F.R. §227.7204, with respect to the Department of Defense and their contractors; or

(b) 48 C.F.R. §12.212, with respect to all other US Government licensees and their contractors.

6.16. Notices. All notices, requests, consents, claims, demands, waivers and other communications hereunder shall be in writing and shall be deemed to have been given:

(a) When delivered by hand (with written confirmation of receipt);

(b) When received by the addressee if sent by a nationally recognized overnight courier (receipt requested);

(c) On the date sent by facsimile (with confirmation of transmission) if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient; or

(d) On the third day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid. Such communications must be sent to the respective parties at the addresses set forth on the Entitlement (or to such other address as may be designated by a party from time to time in accordance with this Section **6.16**.

If you have questions, please contact Haivision Systems Inc., at 4445 Garand, Montréal, Québec, H4R 2H9 Canada or legal@haivision.com.