HAIVISION

Makito X Encoder 2.3

User's Guide

HVS-ID-UG-MAKX-23, Issue 01

Edition Notice

© 2015-2023 Haivision. All rights reserved.

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

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

Edition Notice 2
About Haivision 2
Trademarks 2
Disclaimer 2

Contents 3

About This Document 8
Conventions 8
Typographic Conventions and Elements 8
Action Alerts 8
Obtaining Documentation 9
Getting Service Support 9

Introduction 11
New Product Features 12
Product Overview 13
Chassis Styles 16
HEVC Encoding 19
Dual Channel vs. High/Low Encoding 20
Secure Reliable Transport (SRT) 21
IPv6 Support 22
Storage and Recording 23
Applications 23
Physical Description 24
System Interfaces 24
Storage Options 25
Audio/Video Interfaces 27
LED Status Indicators 30
Audio Talkback 35
Hardening 37

Installing the Encoder 38
Setting Up the Encoder 39
Safety First 39
Safety Guidelines 39
Waste Electrical and Electronic Equipment (WEEE) Disposal 42
Connecting the Encoder to the Network and a Computer 43
Serial Interface Setup (Makito X SDI) 45
COM1 Serial Port RJ45 Pinout (Makito X SDI) 46
Serial Management Adapter DB9 Pinout (Makito X SDI) 47
Connecting the Encoder to A/V Sources 48
Connecting the BNC/S-Video Interface (Makito X SDI) 48
Connecting the DVI-I Interface (Makito X-DVI) 50
Audio Connector Pinout 51
Unbalanced Audio Connections 52
Balanced Audio Connections 55
Audio Breakout Cables 56
Powering Up the Unit 57
Resetting the Encoder 60
Default Network Settings 60
Hardware Maintenance 62
Cleaning the Ventilation Intake-Outtake 62

Monitoring the Fan Operation 62
Replacing the RTC Battery 62

Getting Started with the Web Interface 65

Accessing the Web Interface 66
Security Steps 66
Default Encoder IP Address 66
Role-based Authorization 67
Signing In to the Web Interface 69
Exploring the Web Interface 71
Selecting Items from Lists 72
User Preferences 74
Changing Your Password 75
Password Requirements 76
Signing Out 77

Managing the Encoder 78

Configuring Video Encoders 79
Video Encoders List View 79
Configuring Video Encoder Settings 80
Configuring HEVC Video Encoding 83
Video Encoder Settings 84
Video Encoder Statistics 93
Makito Decoder Interoperability 95
Configuring Audio Encoders 96
Audio Encoders List View 96
Configuring Audio Encoder Settings 98
Audio Encoder Settings 99
Audio Encoder Statistics 100
Configuring Metadata Capture 102
Metadata List View 102
Configuring Serial Metadata Sources 104
Configuring HD-SDI Metadata Sources 105
Configuring Network Metadata Sources 108
CoT/UDP with SPI Message Filtering Based on UID 110
Configuring CoT Retransmission 110
Configuring KLV Metadata Insertion 112
Filtering UAS KLV Metadata Tags 114
Metadata Settings 116
Metadata Statistics 124
Configuring Streaming Outputs 125
Outputs List View 125
Setting Up Streaming 127
Configuring Secure Reliable Transport (SRT) 133
CDN Interoperability (RTMP) 135
Publishing an RTMP Stream to YouTube 137
Streaming Output Settings 138
Streaming Output Statistics 148
Configuring Recording Outputs 152
Setting Up Recording 152
Recording Settings 155
Roll-Over and Uploading to HVC or Haivision Media Platform 157
Managing Recordings 158
Viewing Options 160
Playing Back .MP4 Recordings 162
Managing Recorded Content 164
Viewing Recordings from a Removable Drive on a Computer 166
Configuring Logo Overlays 167
Logo Settings 169
Capturing Image Snapshots 170
Configuring Still Image Streaming 173
Managing External Storage 175

System Administration and Storage 177

Viewing System Status Information ... 178
Status Settings ... 179
Rebooting the Encoder ... 181
Taking a System Snapshot ... 181
Saving and Loading Presets ... 184
Installing Firmware Upgrades ... 187
Configuring Network Settings ... 190
Network Settings ... 193
Configuring Date and Time ... 198
Date and Time Settings ... 199
NTP Statistics ... 200
Enabling and Disabling Network Services ... 201
Service Settings ... 202
Managing Licenses ... 205
License File Errors ... 207
Managing the COM Port ... 208
COM Port Settings ... 210
Managing Storage Drives ... 211
Managing Network Storage ... 212
Network Storage Settings ... 212
Configuring Export Destinations ... 213
Export Destination Settings ... 215
Managing Snapshot Storage Locations ... 216
Snapshots Location Settings ... 217
Managing File Transfer History ... 218

Managing Users and Security 219

Managing User Accounts ... 220
Account Management ... 222
Account Settings ... 223
Managing Public Key Authentication ... 225
Managing Messages ... 226
Managing Banners ... 227
Synopsis ... 227
Actions ... 227
Parameters ... 227
Examples ... 228
Managing Security Policies ... 230
Policy Settings ... 232
Managing Certificates ... 234
Viewing Certificate Details ... 237
Certificate Settings ... 238
Managing Audits ... 241
Audit Settings ... 242

Configuring A/V Services Using SNMP 244

SNMP Overview ... 245
Supported MIBs ... 245
SNMP Agent Components ... 248
snmpd ... 248
snmpd.conf ... 248
snmpd.local.conf ... 248
nmcfg ... 249
SNMPv3 ... 250
SNMP Utilities ... 252
SNMP Syntax for Setting Up Streams ... 253

CLI Command Reference 256

Accessing the CLI ... 256
Syntax Conventions ... 256
Command Summary and Access Control ... 257
Operation Commands ... 263
audenc ... 263
leds ... 267

logo ... 268
metadata ... 271
mklogo ... 284
mkstill ... 285
passthrough ... 287
record ... 291
roi ... 294
session ... 296
snapshot ... 298
still ... 301
stream ... 302
talkback ... 312
temperature ... 315
videnc ... 316
vidin ... 323
Administration Commands ... 325
account ... 325
audit ... 328
banner ... 330
bist ... 332
certificate ... 333
config ... 336
date ... 338
dest ... 339
dtconfig ... 342
edid ... 343
ethercfg ... 345
haiversion ... 347
hdcp ... 348
ipconfig ... 349
ipv6config ... 353
license ... 356
messages ... 358
nas ... 360
nmcfg ... 362
package ... 365
passwd ... 367
personality ... 368
policy ... 369
pubkey ... 372
reboot ... 373
service ... 374
storage ... 375
system_snapshot.sh ... 377
transfer ... 378
tzconfig ... 380

Technical Specifications **381**

Audio/Video Interface Specifications ... 382
Video Encoding ... 383
Supported H.264 Video Encoding Input and Downscale Resolutions ... 385
Supported H.264 Graphic Encoding Input and Downscale Resolutions ... 387
Audio Encoding ... 389
Advanced Features ... 390
Metadata (Optional) ... 391
KLV Data Specifications ... 392
Asynchronous KLV Metadata Support ... 393
Network and Management Interfaces ... 394
Chassis Options ... 395
Single-Height Appliance ... 395
Dual-Height Appliance (Storage Mezzanine) ... 395
Dual-Height Appliance (HEVC Mezzanine) ... 396
MB6X – 6 Blade Chassis ... 396
MB21B (#F-MB21B-R) ... 397
MB21X (#F-MB21X-R) ... 397

Makito XR (Military Spec) Appliance 398
Makito X Harsh Environment Chassis 398
Supported Storage Devices 399
Regulatory/Compliance 401
Closed Captioning 402

Open Source Software Credits 404

References 404
Open Source Software Credits List 405
Third Party License Information 409
UDT4, 4.11, UDP-based Data Transfer, Permissive free software license. 409
expat Custom License 409
libuuid Modified Licensed (Modified BSD) 410

Warranties 411

1-Year Limited Hardware Warranty 411
EXCLUSIONS AND LIMITATIONS 411
OBTAINING WARRANTY SERVICE 412
APPLICABLE LAW 412
EULA - End User License Agreement 413
READ BEFORE USING 413
SLA - Service Level Agreement 413
1. Introduction 413
2. Definitions 413
3. Service Levels for the Video Content Management System 413
4. Exceptions to Availability for the VCMS 414
5. Credits for Downtime for the VCMS 415
6. Support Services for the VCMS 415
7. Service Levels for Haivision Streaming Media Service 416
8. Credits for Outages of Haivision Streaming Media Service 416
9. No Secondary End User Support 416

Getting Help 417

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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

Tip

Indicates highlights, suggestions, or helpful hints.

Note

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

Important

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

Caution

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

Warning

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

Obtaining Documentation

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

Getting Service Support

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

This user's guide explains how to install, configure, and manage the Makito X encoder to stream audio, video, and metadata to a compatible decoding device, using either the Web interface, the Command Line Interface (CLI), or an SNMP server.

Introduction

Note

References to the "Makito X" can be taken to include the following interfaces unless specifically stated otherwise:

- Makito X DVI (#S/B-292E-DVI)
- Makito X SDI: Dual-Channel (#S/B-292E-HDSDI2) or Single-Channel (#S/B-292E-HDSDI1)
- Makito X HEVC: Dual-Channel (#S/B-292E-SDI2-HEVC) or Single-Channel (#S/B-292E-SDI1-HEVC)
- Makito X (DVI or SDI) with Storage: Removable SSD (SKUs ending -RS) or Fixed SSD (SKUs ending -FS)
- Makito X Harsh Environment SDI: Dual-Channel (#S-292E-X2H) or Single-Channel (#S-292E-X1H)
- Makito XR (Ruggedized) SDI: with Dual Input (#S-292E-X2R) or Quad Input (#S-292E-X4R)
- Makito XCR (Compact Ruggedized) SDI: with Dual or Quad Input (#S-292E-XCR)
- Makito X HEVC Rugged: with Dual Input (#S-292E-HEVC-R)

Unless otherwise specified, references to the "Makito X SDI" include 3G/HD/SD-SDI.

Topics in This Chapter

- New Product Features
- Product Overview
- Physical Description
- Audio Talkback
- Hardening

New Product Features

Makito X Version 2.3 introduced the following new features and enhancements to existing capabilities:

IPv6 Support

The Makito X now supports deployment on IPv6 or mixed IPv6/IPv4 networks in addition to the existing IPv4 network support. This includes IPv6 network and device administration and streaming support.

SRT Streaming Stats in SNMP

SRT streams can be monitored in real-time using an SNMP network management system (NMS). The SNMP MIB now includes SRT statistics which are useful for monitoring the health of an SRT link.

Device Discovery Aids

Enhancements have been added to allow easier determination of the IP address or location of a Makito X device. These include the display of the device IP address on the serial port login prompt (SDI encoder blades/appliances only), as well as enhancements to encourage the use of mDNS for easier device discovery on a network.

Device Location (Blinking LEDs)

The Makito X face-plate LEDs can be optionally set to blink which allows easy location of the device in large server room deployments. For example, the blinking LEDs can be used to help identify a specific blade in a rack.

Security Enhancements

The operator and user accounts are now locked at factory to minimize the chances of unauthorized access.

Streaming to NGINX servers

The Makito X Encoder now supports RTMP streams to NGINX servers.

Ubuntu NFS Server

NFS shared drives from Ubuntu servers can now be mounted on Makito X Encoders with Storage.

Related Topics

- IPv6 Support
- Viewing System Status Information
- Managing User Accounts

Product Overview

The Makito X Encoder Family delivers up to 12 HD channels of High Profile 1080p60 video with extremely low encoding latency, all within a single rack unit. The Makito X is available as an ultra compact SDI or DVI H.264 encoding appliance with optional HEVC encoding support, internal or removable storage, or within a high density 1RU (6 blades) or 4RU (21 blades) chassis.

The Makito X DVI supports HD up to 1080p60 (Component Analog or Digital) or computer resolutions up to 1920x1200 at 60 Hz (RGB or DVI-D) input via its DVI-I connector. The Makito X SDI Single- or Dual-Channel supports SDI, HD-SDI, 3G-SDI and Composite on its BNC interfaces.

Supporting AES stream encryption and forward error correction (FEC), the Makito X is ideal for headend applications within enterprise, education, broadcast monitoring, medical, and military applications. Combined with Haivision's Furnace IP video system, the Makito X offers administrators fine-grained control over video stream access and distribu tion. The Makito X may be paired with the Makito decoder to achieve low end-to-end latency, as well as combined with Haivision's InStream multi-view performance player technology.

With four internal H.264 encoding engines, the Makito X can encode video at up to four different bitrates and profiles for Multi-bitrate (MBR) streaming to optimize video distribution. In addition, each engine can be then directed at multiple network destinations (unicast, multicast, TS and RTMP) concurrently, to serve desktops, laptops, mobile devices, set-top boxes, signage players, recorders, and streaming servers. The Makito X HEVC provides two HEVC Single- or Dual-Channel encoding engines.

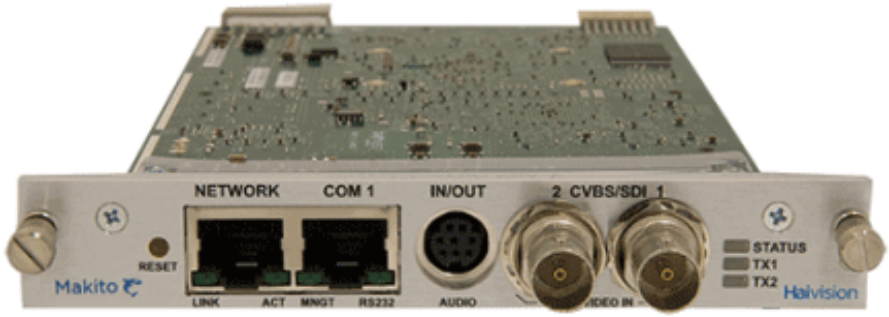
The Makito X with Storage dual-height model allows the compressed content to be recorded and stored locally on either a removable SSD (solid-state drive, SKUs ending -RS) or an internally installed fixed SSD (SKUs ending -FS). Recorded sessions may be exported to an FTP/SFTP server for use within Haivision media systems including Haivision Media Platform and the Haivision Video Cloud (HVC), or stored locally on an SD card or USB storage device, or transferred to a network attached storage configuration drive (if installed).

Makito X Encoder (Front View, Single Height Chassis)

Makito X HEVC Encoder (Front View, Dual Height Chassis)

Sample Rear View (DVI Blade #B-292E-DVI)

Sample Rear View (Dual SDI Blade #B-292E-HDSDI2)



Topics Discussed

- Chassis Styles
- HEVC Encoding
- Dual Channel vs. High/Low Encoding
- Secure Reliable Transport (SRT)
- IPv6 Support
- Storage and Recording
- Applications

Chassis Styles

The Makito X is available in the following chassis styles:

- as an ultra-compact appliance (single-height or dual-height) for single or dual channel encoding.
- as a blade within a 1RU chassis (MB6X) that can contain up to six single-height or three dual-height Makito X or other Haivision encoder/decoder blades.
- as a blade within a 4RU chassis (MB21) that can contain up to 21 single-height or ten dual-height Makito X or other Haivision encoder/decoder blades.

In addition, the following harsh or ruggedized appliances are available:

- Makito X Harsh semi-ruggedized, industrial single or dual SDI encoder appliance.
- Makito XR ("Ruggedized") platform supporting two or four video input variants in a MIL-STD rugged appliance. Note that support for analog and embedded audio capture or encoding is not currently provided for the Makito XR.
- Makito XCR ("Compact Ruggedized") SDI platform supporting two or four video input variants in a compact and ruggedized military-grade appliance.
- Makito X HEVC Rugged platform supporting HEVC encoding in a ruggedized military-grade appliance.

The Makito X single-height and dual-height chassis appliances and single blades are shown in the **Product Overview**. The Makito X with HEVC, MB21 and MB6X chassis, Makito X Harsh, and Makito XCR are shown in the following figures.

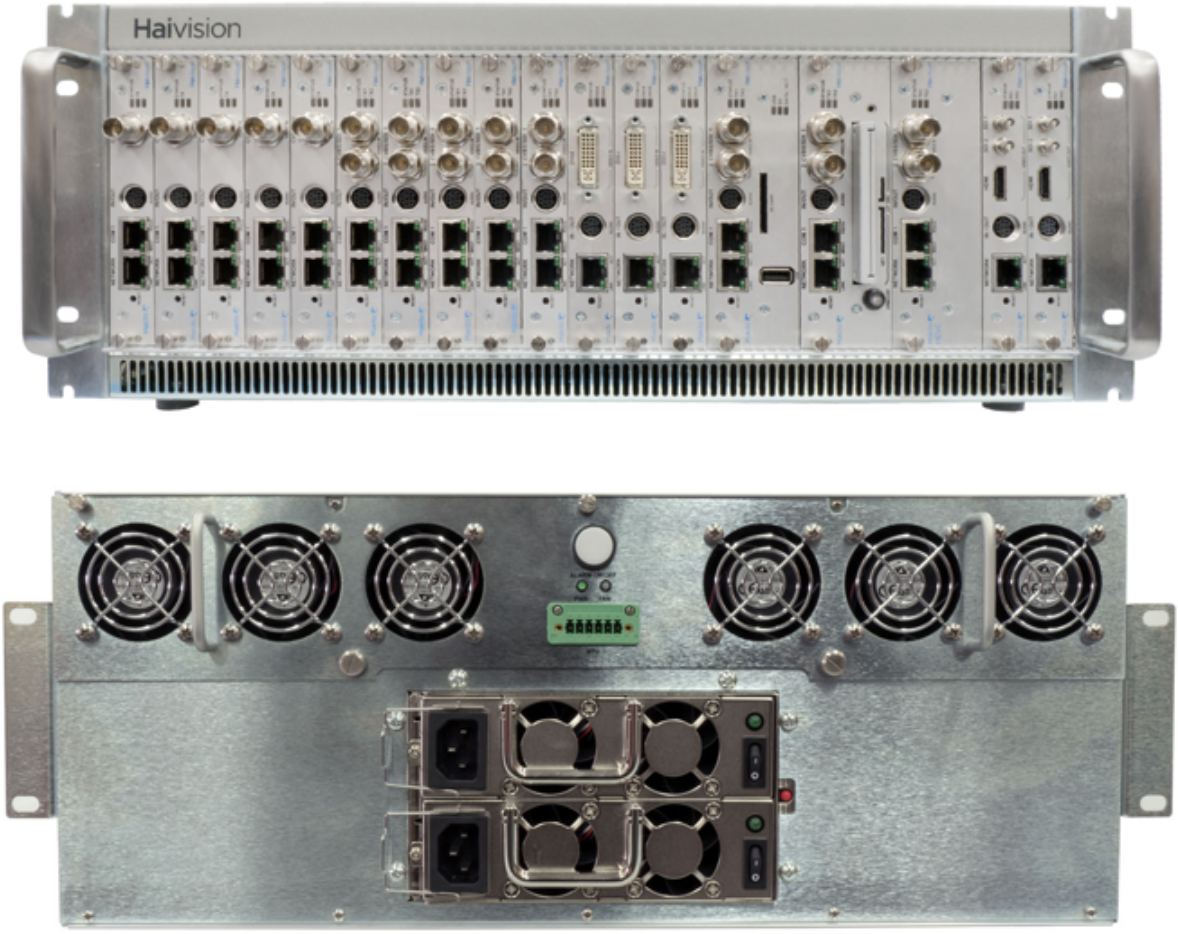
Makito X HEVC Encoder, Rear View (#S-292E-SDI2-HEVC)

MB6X Multichannel Chassis (Front and Rear Views, #MB6X-RAC)

Note

The MB6X is available with a single AC, DC, or medical grade AC power supply. For details, please refer to the *MB6 Chassis Installation Guide*.

MB21 Multichannel Chassis (Front and Rear Views, #F-MB21X-R)



Makito X Harsh (Dual SDI Encoder Appliance)

*Makito XCR (**compact and** ruggedized Makito military-grade appliance)*

Note

For details on the Makito X harsh or ruggedized encoders, please refer to the following documents (available on the Haivision InfoCenter):

- *Makito XCR Encoder Installation Guide*
- *Makito X HEVC Rugged Encoder Installation Guide*
- *Makito X Harsh Installation Guide*
- *Makito XR (Ruggedized) Installation Guide*

HEVC Encoding

The Makito X HEVC encoder is designed to support extreme low-latency broadcast and intelligence surveillance reconnaissance (ISR) applications. Features include:

- **Live Video Backhaul** - From anywhere, transport the highest quality, lowest latency, live video over any network with the Makito X HEVC encoder.
- **More Content - Less Operational Cost** With HEVC and Haivision's SRT (Secure Reliable Transport) support, the Makito X HEVC encoder makes low-cost, readily available public Internet connections secure and reliable for high quality live video transport, while saving bandwidth yet maintaining H.264 picture quality.
- **Performance Encoding with Metadata** In ISR applications, many full motion video (FMV) systems bundle additional information with video streams in the form of metadata. The Makito X HEVC optimizes the task of disseminating information in formats required by downstream networks, exploitation systems, and viewers, with the lowest possible delay, while preserving and enhancing metadata with frame accurate synchronization.

Dual Channel vs. High/Low Encoding

In addition to encoding single input sources, the Makito X supports dual channel and High/Low encoding. Dual channel encoding features two input sources as two independent encoders. With High/Low encoding, the Makito X encodes a single input source and emits both high and low bandwidth streams simultaneously. Following are some differences between the two in H.264 vs. HEVC encoding:

H.264 Encoding | HEVC Encoding

H.264 Encoding

Dual Channel	Both inputs can be up to 1080p60, with no limitations on the coded picture resolution or frame-rate.
High/Low	There are no limitations on the two resolutions/frame-rates that a single input video source can encode.

H.264 Encoding | HEVC Encoding

HEVC Encoding

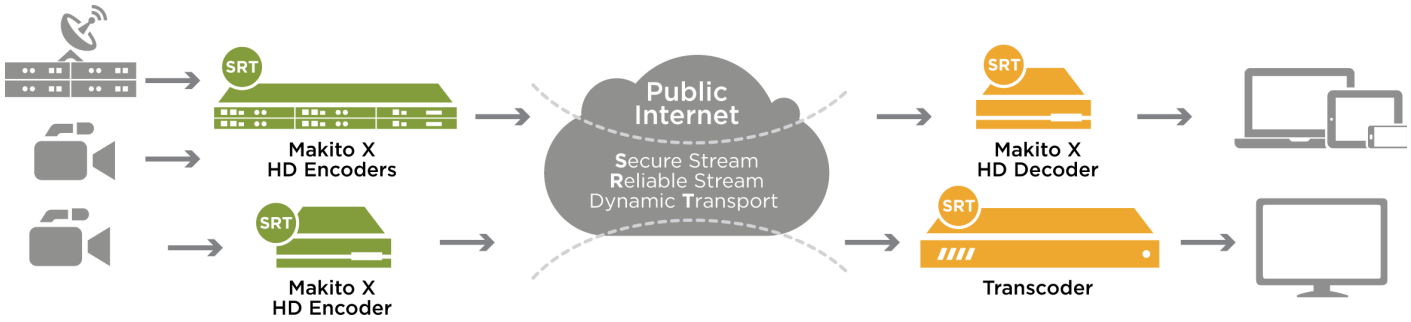
Dual Channel	Each input (BNC1 and BNC2) supports up to a 720p60/1080i30/1080p30 HD-SDI signal.
High/Low	A single input can be up to 1080p60, but both HEVC encoders must select lower coded picture resolutions/frame-rates. For example, Input is 1080p60 video, HEVC Video Encoder 4 is set to 1080p30, and HEVC Video Encoder 5 is set to 720p60.

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 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 realtime network performance between the encode / decode / transcode endpoints. The endpoints can be dynamically adjusted for optimal stream performance and quality.

Makito X SRT Workflow



For additional information required to set up and tune SRT streams from the encoder to the decoder, please refer to the SRT Deployment Guide.

Related Topics

- Configuring Secure Reliable Transport (SRT)

IPv6 Support

Version 2.3 introduces IPv6 support for Makito X encoders and decoders in addition to the existing IPv4 network support. Makito X devices now support IPv6-only networks as well as dual IPv4 and IPv6 network environments. You can install the Makito X on an IPv6 network or on a network supporting both IPv4 and IPv6. You will be able to access the Web Interface, CLI and SNMP via the IPv4 and/or IPv6 addresses assigned to the device. You will be able to perform normal administrative functions from the IPv4 and/or IPv6 addresses.

Version 2.3 IPv6 capabilities include the following:

1. Static and dynamic assignment of IPv6 addresses via DHCPv6 or Stateless Autoconfiguration (SLAAC) to Makito X products in addition to the existing IPv4 capabilities.
2. Dual-stack IPv4 and IPv6 may be used simultaneously for management and video streaming purposes.
3. All administration functions may be performed from an IPv6 network client, including upgrade/downgrade, preset import/export, license install, system snapshots and specifying audit servers.
4. User functions include creating and starting streams, specifying an NFS server for recording, specifying a Talkback device, capturing image snapshots, and importing logos and still image files from an IPv6 device.

Related Topics

- Configuring Network Settings
- ipv6config (CLI command)

Storage and Recording

The Makito X with Storage dual-height models include 250 GB of either fixed or removable SSD (solid-state drive) storage that enables users to record content directly on the encoder, while simultaneously streaming live video from two sources.

The Makito X with Storage provides the following benefits:

- Streaming Content Storage. Encoded stream content may be stored for later retrieval, allowing continuous local recording of compressed content in real-time.
- Snapshot Content Storage. The storage module increases the amount of space that can be used to store image snapshots. Furthermore, if the storage media is removable (such as an SSD or USB thumb drive), the content can be moved without the need to download the content via the Ethernet port.
- Record streams in TS or MP4 file formats and automatically segment the recorded streams based on time and size.
- Browse recorded assets and play back MP4 recorded files directly within the Makito X user interface.
- Record high quality video (i.e., 20 Mbps) while streaming low to save on bandwidth.
- Automatically segment recordings to files (i.e., for long duration or continuous recording).
- Automatically export via FTP/SFTP.
- Ingest to Haivision Video Cloud (HVC) through a watch Folder.

For more information, see **Storage Options**.

Applications

Typical examples of Makito X applications include:

- **IPTV Distribution** – delivering video channels to viewers in schools, financial institutions, live event venues, control rooms, and within government organizations.
- **Medical Systems** – driving controlled and secure video throughout healthcare facilities enabling education, consultation, and procedural review.
- **Streaming Services** – connecting facilities, affiliates, and event locations with realtime high definition video, simultaneously addressing streaming and distribution challenges.
- **ISR (Intelligence, Surveillance, Reconnaissance)** – combining the excellent image quality and performance of 1080p60 high definition video with KLV/CoT metadata capabilities.

Physical Description

Note

For details on the Makito X harsh or ruggedized interfaces, please refer to the installation guides. See Chassis Styles for the list of available harsh and ruggedized appliances.

Following is a description of the Makito X interfaces, connectors, and LED status indicators:

System Interfaces

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

Ethernet Connection (Makito X DVI, #S/B-292E-DVI)

On the Makito X with SDI, a computer can be connected to the COM1 RS-232 serial port through its RJ45 connector. A Serial Management adapter is required (see Connecting the Encoder to the Network and a Computer).

Serial Connection (Makito X SDI, Dual-Channel #S/B-292E-HDSDI2)

Note

The COM1 port may also be used for KLV and CoT Metadata Capture and stream insertion (the KLV software option must be installed at the factory), as well as for bidirectional serial pass-through for controlling serially attached devices such as cameras.

Related Topics:

- Connecting the Encoder to the Network and a Computer
- Serial Interface Setup (Makito X SDI)

Storage Options

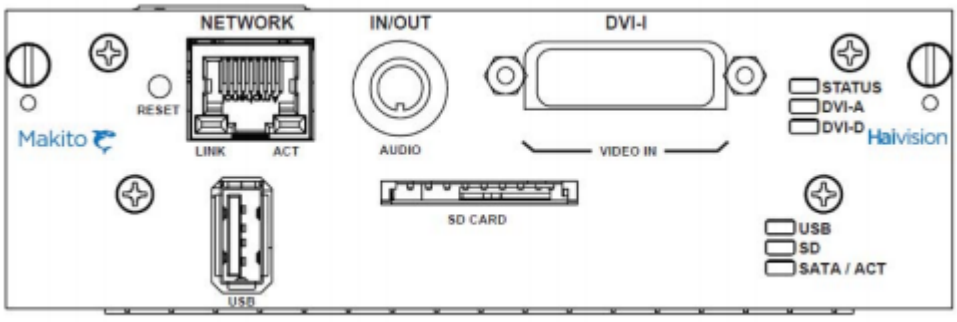
The Makito X provides the following mezzanine storage options for either the SDI or DVI appliances:

- Fixed (i.e., not accessible from the face-plate) mSATA SSD (solid-state drive) with USB 2.0 and SD card interfaces accessible from the face-plate.
- Removable 2.5" SATA SSD (solid-state drive), accessible from the face-plate with an Unmount push button with LED (showing mount status).

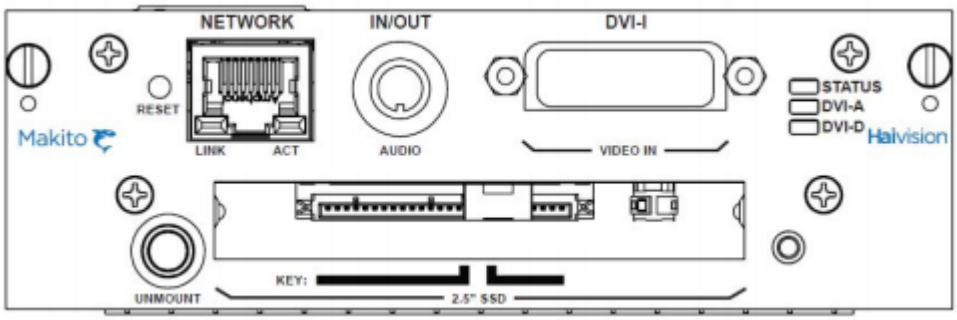
Dual SDI Appliance with Fixed Storage (Internal mSATA SSD) (#S-292E-SDI2-FS)

Dual SDI Appliance with Removable Storage (SATA SSD) (#S-292E-SDI2-RS)

DVI Rear View with Fixed Storage (Internal mSATA SSD) (#S292E-DVI-FS)



DVI Rear View with Removable Storage (SATA SSD) (#S-292EDVI-RS)



Note

The USB port and SD card port are currently limited to a destination for recording asset moves/copy operations or as a location to save image snapshots.

Audio/Video Interfaces

Following is a description of the available Makito X audio/video interfaces:

- SDI Video and Embedded Digital Audio Interface
- DVI Video and Embedded Audio Interface
- Analog Audio Interface

SDI Video and Embedded Digital Audio Interface

The Makito X SDI video interface consists of either one or two 75 BNC connectors.

***Makito X** SDI Dual-Channel Video Interface (#S/B-292E-HDSDI2)*

***Makito X** SDI Single-Channel Video Interface (#S/B-292E-HDSDI1)*

The BNC connector(s) are used for Composite (CVBS), SD-SDI (Serial Digital Interface) and HD-SDI video input signals. It is also a 3G-SDI capable interface supporting 1080p 50/60 fps video @ 3Gbps.

Caution

Be sure to use an HD video-capable RG-6 coaxial cable such as the Belden 1694A up to 300 feet. Otherwise, the video signal may be too attenuated and the encoder will not sync on it.

DVI Video and Embedded Audio Interface

The Makito X DVI video interface consists of a single DVI-I connector.

Makito X DVI-I Video Interface (#S/B-292E-DVI)

The DVI-I connector supports the following inputs:

- Component Analog video (Y,Pb,Pr / RGBHV)
- Component Digital video (Y,Cb,Cr / DVI)
- SD and HD video
- Computer graphics
- Two channels of DVI-I digital audio

Note

The Makito X encoder supports EDID resolution capabilities negotiation.
If the content is HDCP copy-protected, the stream will not be encoded.

Analog Audio Interface

Note

The Analog Audio interface is the same for both the Makito X DVI (#S/B-292E DVI) and the Makito X SDI (#S/B-292E-HDSDI2).

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

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 the pinout, see Audio Connector Pinout.

Related Topics

- Connecting the Encoder to A/V Sources
- Audio Talkback
- Audio Breakout Cables
- Technical Specifications
- Supported H.264 Video Encoding Input and Downscale Resolutions (in Technical Specifications)
- Connecting the BNC/S-Video Interface (Makito X SDI)

LED Status Indicators

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

LED Status Indicators (Rear Panel)

General | Network Port | COM1 Port

General

Function	Description	Indication
STATUS	Off	No power
	Red solid	Error/Fault
	Green blinking	Booting/Initialization
	Green solid	No fault/OK
TX1/TX2 [SDI]	Off	**Note** Each TX LED is associated with the corresponding BNC connector.
	Amber solid	Either of the conditions below is sufficient to turn the LED amber: • Encoder booting • Valid video input not detected (i.e., if you configure an encoder to use a BNC and there is no video input lock).
	Green solid	Valid video input detected (i.e., you have signal lock).

Function	Description	Indication
DVI-A/DVI-D	Off	No valid signal is recognized; both LEDs are off.
	Green solid	For DVI-D, a valid digital signal is plugged in. For DVI-A, a valid analog/component signal is plugged in.

General Network Port COM1 Port

Network Port

Function	Description	Indication
LINK	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
ACT	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)

General Network Port COM1 Port

COM1 Port

Function	Description	Indication
MNGT	Off	Port configured in Metadata Capture Mode
	Green solid	Port configured in Management Mode
RS232	Off	Port configured in RS-422
	Green solid	Port configured in RS-232

Topics Discussed

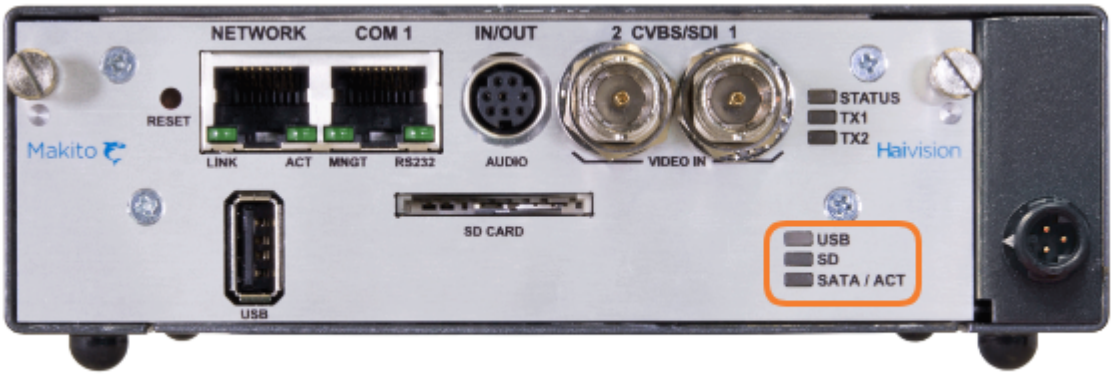
- Storage Mezzanine LED Status Indicators

Storage Mezzanine LED Status Indicators

The Makito X Storage Mezzanine LEDs are shown following.

Fixed mSATA SSD | Removable SATA SSD

Fixed mSATA SSD



Description	Indication
USB	
Off	LED remains off until drive has booted.
Green solid	Indicates drive is ready to use.
SD	
Off	LED remains off until drive has booted.
Green solid	Indicates drive is ready to use.
SATA/ACT	
Off	LED remains off until drive has booted.
Green solid	Indicates drive is ready to use.
Green blinking	SATA LED blinks briefly off when the SATA drive is being accessed.

Fixed mSATA SSD | Removable SATA SSD

Removable SATA SSD

Description	Indication
Mount Status LED/Unmount Button	
Off	SSD not mounted.
Blue solid	SSD mounted and ready to use.
Blue blinking	Blinks briefly off when the SATA drive is being accessed.
Blue blinking two times per second	**Note** To unmount SATA drive, press the Unmount button for three seconds.

Related Topics

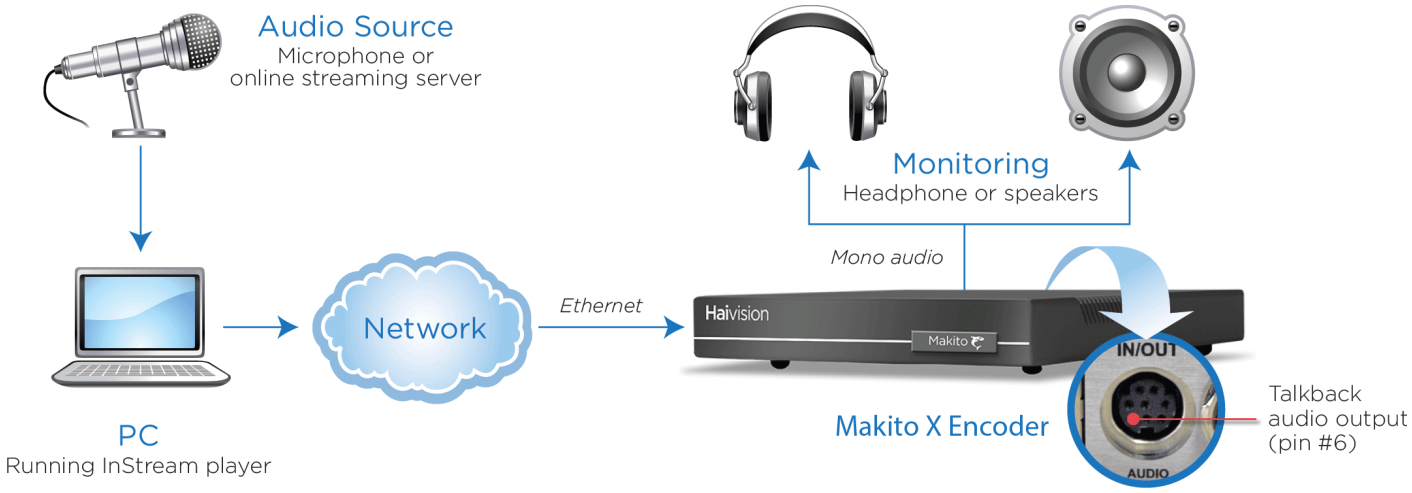
- Powering Up the Unit

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 enables end users monitoring a streaming session to "talk back" to individuals at the video source. For example, talkback enables students at remote classroom locations to ask their teacher questions, or a chief surgeon observing a surgery to collaborate.

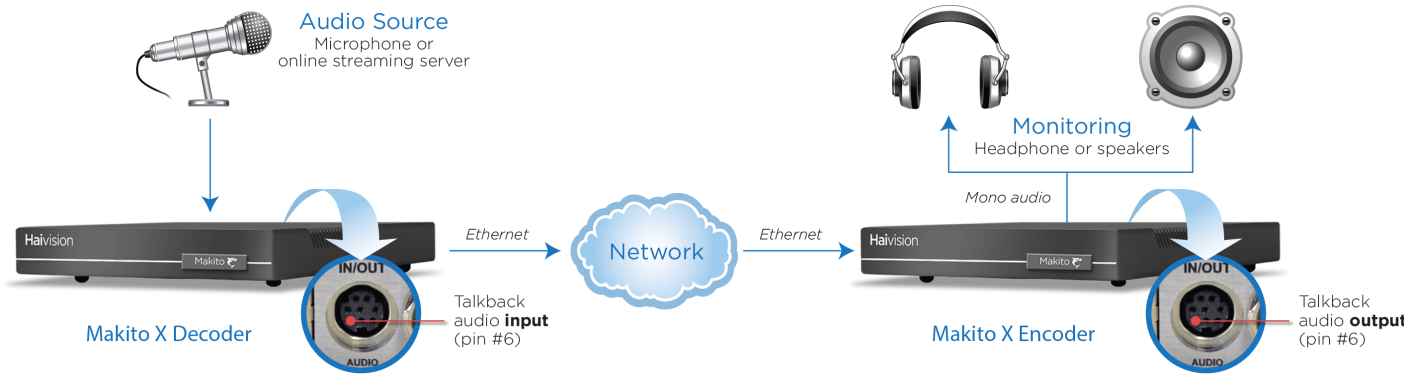
Audio talkback uses the InStream software player application or the Makito X decoder (release 1.2 and later) to send the talkback audio to the Makito X encoder. The talkback audio stream is output via a speaker or headphones connected to the encoder's 8-pin MiniDIN connector (see **Audio/Video Interfaces**). The following figure illustrates a sample talkback signal path from the audio source through the Makito X's audio output when using InStream.

Audio Talkback Signal Path (InStream)



The following figure illustrates a sample talkback signal path when using the Makito X Decoder.

Audio Talkback Signal Path (Makito X Decoder)



There is no audio mixer on the Makito X, so the talkback feature is “First-In/First Served”, meaning that only one user can use the return audio channel at a time. The InStream player application 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. This prevents the user from accidentally locking and not releasing the channel.

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

The Talkback network service may be stopped or started from the Web interface (Services page, see **Enabling and Disabling Network Services**) or using the **service** command.

CLI commands are used to enable and disable reception of talkback audio, set the talkback volume, clear talkback statistics, and display talkback information. For details, see **talkback** (CLI). Talkback audio is not configurable through SNMP in the current release.

> **Note**
>
> Audio talkback is uncompressed audio (using approximately 350 kbps of network bandwidth).

Related Topics

- **Enabling and Disabling Network Services**
- **service**

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 includes features that allow the administrative interface to be secured. These features are described in detail in the *Makito X Hardening Guide* (available from the **Download Center** on the Haivision Support Portal: Resources>Download Center>Support Documentation>Makito X).

The *Makito X Hardening Guide* provides the procedures to install and configure Makito X encoders and decoders 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.

Note

Any Makito X encoder at Version 1.5 or higher can be hardened by following the procedures described in this guide.

Installing the Encoder

Note

For instructions on installing the Makito X ruggedized or harsh encoders, please refer to the following documents (available on the Haivision InfoCenter):

- *Makito XCR Encoder Installation Guide*
- *Makito X HEVC Rugged Encoder Installation Guide*
- *Makito XH Encoder/Decoder Installation Guide*

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

Topics in This Chapter

- Setting Up the Encoder
- Connecting the Encoder to the Network and a Computer
- Serial Interface Setup (Makito X SDI)
- Connecting the Encoder to A/V Sources
- Powering Up the Unit
- Resetting the Encoder
- Hardware Maintenance

Setting Up the Encoder

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

Please choose a suitable location for operating the encoder(s). By doing so you will preserve the operating life span and stability of the unit(s).

Caution

The MB21 chassis must either be installed on a securely fastened rack shelf, or fastened directly to the rack using support brackets. For instructions on how to properly secure or support the MB21, refer to the *MB6 and MB21 Multichannel Chassis Installation Guide*.

Safety First

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

- The Makito X is an indoor appliance and should be kept in a dry, dust free environment.
- The only user-serviceable part is the RTC battery. There are no other 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.
- Refer to Safety Guidelines.

Safety Guidelines

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

When using the AC/DC power adapter, the power cord is the main disconnect device. Ensure that the socket-outlet is located/installed near the equipment and is easily accessible.
ATTENTION Quand on utilise l'adaptateur AC à DC, le cordon d'alimentation est utilisé comme interrupteur général. La prise de courant doit être située ou installée à proximité de l'équipement et être facile d'accès.

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.

Warning

Any power supply shipped with a Haivision Makito X Series encoder or decoder is to be used *only* with that product. Haivision supplied power supplies are *not* for general use.
ATTENTION Tout bloc d'alimentation électrique livré avec un encodeur ou un décodeur de la série Haivision Makito X doit être utilisé uniquement avec ce produit. Les blocs d'alimentation fournis par Haivision ne sont pas destinés à un usage général.

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 floor pads and workbench pads.

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.

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 nonconformité 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.

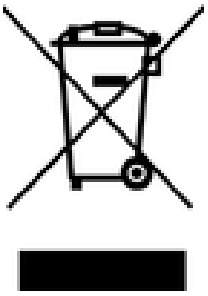
Safety instructions for Class A for CISPR32

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 CISPR32

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.

Waste Electrical and Electronic Equipment (WEEE) Disposal

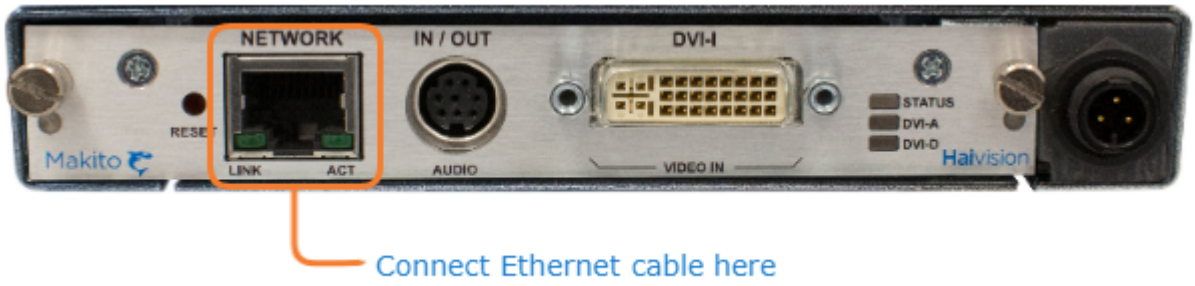
	This symbol on Haivision products or packaging means that the product should not be disposed of with general waste. It is your responsibility to dispose of your waste equipment by handing it over to a designated recycling collection point. The correct disposal of your end-of-life equipment will help 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: https://www.haivision.com/environment.

Connecting the Encoder to the Network and a Computer

To connect the Network Interface:

1. Connect the encoder's Network 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.

Network Connector (#S-292E-DVI)



To connect the Serial Interface (Makito X SDI only):

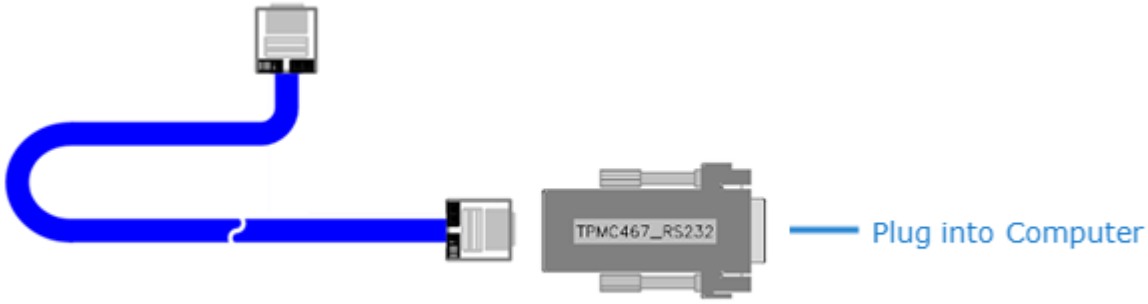
1. (Optional) Connect the encoder's COM1 port to the serial port of a computer. Use the gray RS-232 DB9 to RJ45 Serial Management Adapter (shown following, included in the package for appliances) and a standard straight Ethernet cable.
   This will allow you to communicate directly from your computer to the Makito X using a serial communication application such as HyperTerminal or Minicom. This is only required if you wish to use the Serial Management COM1 port instead of the Web interface. For more information, see Serial Interface Setup (Makito X SDI).

Network and Serial Connectors (#S-292E-HDSDI2)

Caution

Take care not to plug the Ethernet cable from an Ethernet switch (especially a Power over Ethernet (PoE) switch) directly into the COM1 serial port as it may damage the encoder.

Serial Management Adapter



Related Topics:

- For details on the connectors, see **System Interfaces**.
- To set the terminal parameters to interface with the serial COM1 port, see **Serial Interface Setup (Makito X SDI)**.

Serial Interface Setup (Makito X SDI)

The serial interface is available on the following Makito X models:

- Makito X SDI Dual-Channel (# S/B-292E-HDSDI2)
- Makito X SDI Single-Channel (#S/B-292E-HDSDI1)
- Makito X with Storage: Removable SSD (SKUs ending -RS) or Fixed SSD (SKUs ending -FS).

Prior to logging in to the Makito X for the first time, you may wish to change the unit's default network settings to match the network in which it will be used. You can do so by connecting directly to the Makito X's serial COM1 port from your computer using HyperTerminal (or other serial communication application).

Tip

The Makito X also supports bi-directional serial pass-through (RS-232/RS-422) for controlling serially attached devices such as PTZ controlled cameras. Passthrough settings are managed from the CLI. For more information, see passthrough.

Important

IP display is enabled on the serial port login prompt by default and takes precedence over a banner. If both Banner and IP display are enabled, users will see the IP, not the banner on the serial port.
You can disable and re-enable IP display using the CLI commands `disable_ip_display_on_serial_port` and `enable_ip_display_on_serial_port`. If you disable IP display with this CLI command, the banner works.

To get started, you must set the terminal parameters to communicate with the Makito X.

To set up the serial interface:

1. Connect the Makito X's COM1 port to your computer as described in Connecting the Encoder to the Network and a Computer.
2. Power up the computer and start the serial communication application.
3. Set up the terminal parameters as follows:

Parameter	Setting
Baud Rate	115,200 bps
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

4. Power up the Makito X. (See Powering Up the Unit.)
5. From the serial communication application, press **Enter** to get a prompt from the Makito X.

Tip

You can view the COM port settings from the Web interface. For information, see Managing the COM Port.

We recommend that you log out from the Makito X and exit from the serial communication application *before* disconnecting the COM1 port.

COM1 Serial Port RJ45 Pinout (Makito X SDI)

The COM1 serial port uses an RJ45 connector which has the following pinout:

Pin #	Signal RS-232	Signal RS-422
1	Not connected	Not connected
2	Not connected	Received Data -
3	Not connected	Transmitted Data +
4	Signal Ground	Signal Ground
5	Received Data	Received Data +
6	Transmitted Data	Transmitted Data -
7	Not connected	Not connected
8	Not connected	Not connected

Note

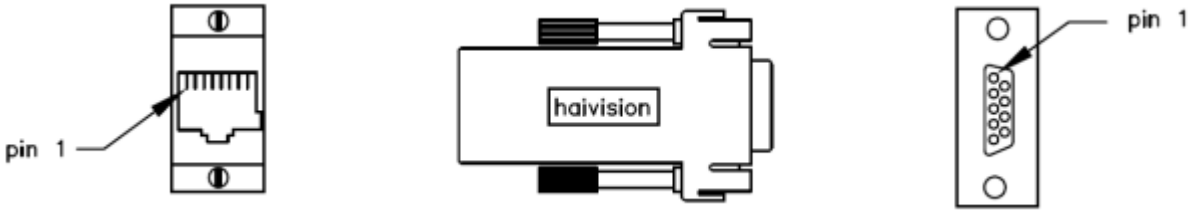
The COM1 Port is DTE (Data Terminal Equipment) which defines the direction of the signals (IN/OUT).

Serial Management Adapter DB9 Pinout (Makito X SDI)

An adapter is required to interface with the serial port. A (gray) DB9 to RJ45 Serial Management adapter (shown in **Connecting the Encoder to the Network and a Computer**) is included in the package.

The Serial Management adapter has the following pinouts:

Management Port (RJ-45 Jack)		**Serial Port (DSub-9 Female Connector)**	
Pin #	**Signal**	**Pin #**	**Signal**
1	RI (Ring Indicator)	9	RI (Ring Indicator) N/C
2	DCD (Data Carrier Detect)	4	DTR (Data Terminal Ready)
3	DTR (Data Terminal Ready)	6	DSR (Data Set Ready)
4	GND (Ground)	5	GND (Ground)
5	RXD (Receive Data)	3	TXD (Transmit Data)
6	TXD (Transmit Data)	2	RXD (Receive Data)
7	CTS (Clear to Send)	7	RTS (Request to Send)
8	RTS (Request to Send)	8	CTS (Clear to Send)
		1	DCD (Data Carrier Detect)



Connecting the Encoder to A/V Sources

This section explains how to connect the Makito X encoder to audio/video sources.

Connecting the BNC/S-Video Interface (Makito X SDI)

> **Note**
>
> The same BNC connector is used for Composite and Serial Digital Interface (SDI) Video Input and Embedded Digital Audio Input.

To connect the Makito X SDI Audio/Video Interface:

1. **Video In:** Connect your Video Source cable(s) to one or both of the encoder's Video Inputs, using the BNC connectors:
   - Composite (CVBS) Video
   - SDI Video/Audio (either SD, HD, or 3G-SDI)
2. **Analog Audio In:** Connect your Audio Source cable to the encoder's 8-pin Mini-DIN connector (shown below).
   - For unbalanced audio, use the 8-pin audio to 3-RCA female cable adapter (included in the package, shown below).
   - A balanced audio cable adapter is available from Haivision upon request. (See **Audio Breakout Cables**.)

SDI-I Input Connections (#S/B-292E-HDSDI2)

Audio to RCA Female Cable Adapter (Unbalanced)

Note

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

Related Topics:

- See **Audio Connector Pinout** for the balanced/unbalanced audio pinout.
- To configure the encoders, see **Video Encoder Settings** (Web interface), or **videnc** (CLI).

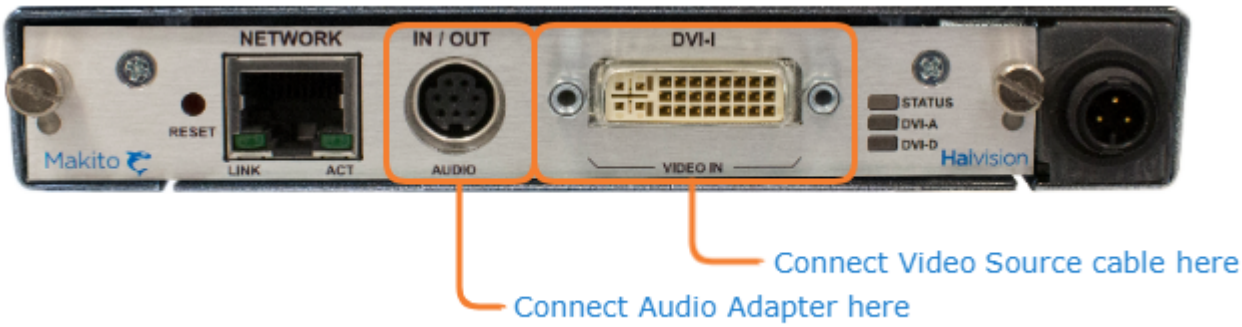
Connecting the DVI-I Interface (Makito X-DVI)

> **Note**
>
> The same DVI connector is used for Analog (Component/RGB) or Digital (HDMI/DVI) input.

To connect the Makito X DVI-I Interface:

1. **Component Analog/Digital Video/Computer Graphics:** Connect your Video Source cable to the encoder's DVI-I Input connector.
2. **Analog Audio In:** Connect your Audio Source cable to the encoder's 8-pin Mini-DIN connector (shown below).
   - For unbalanced audio, use the 8-pin audio to 3-RCA female cable adapter (included in the package, shown below).
   - A balanced audio cable adapter is available from Haivision upon request. (See Audio Breakout Cables.)

DVI-I Input Connections (#S/B-292E-DVI)



Audio to RCA Female Cable Adapter (Unbalanced)

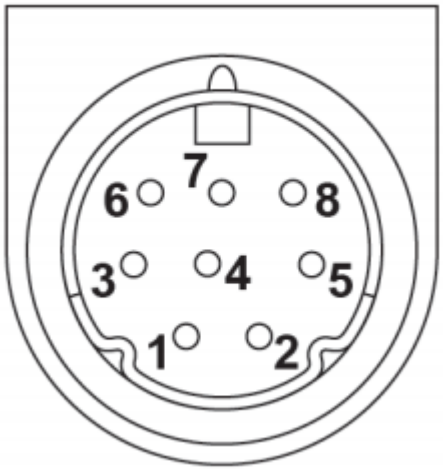
Related Topics:

- See Audio Connector Pinout for the balanced/unbalanced audio pinout.
- To configure the encoders, see Video Encoder Settings (Web interface), or videnc (CLI).

Audio Connector Pinout

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

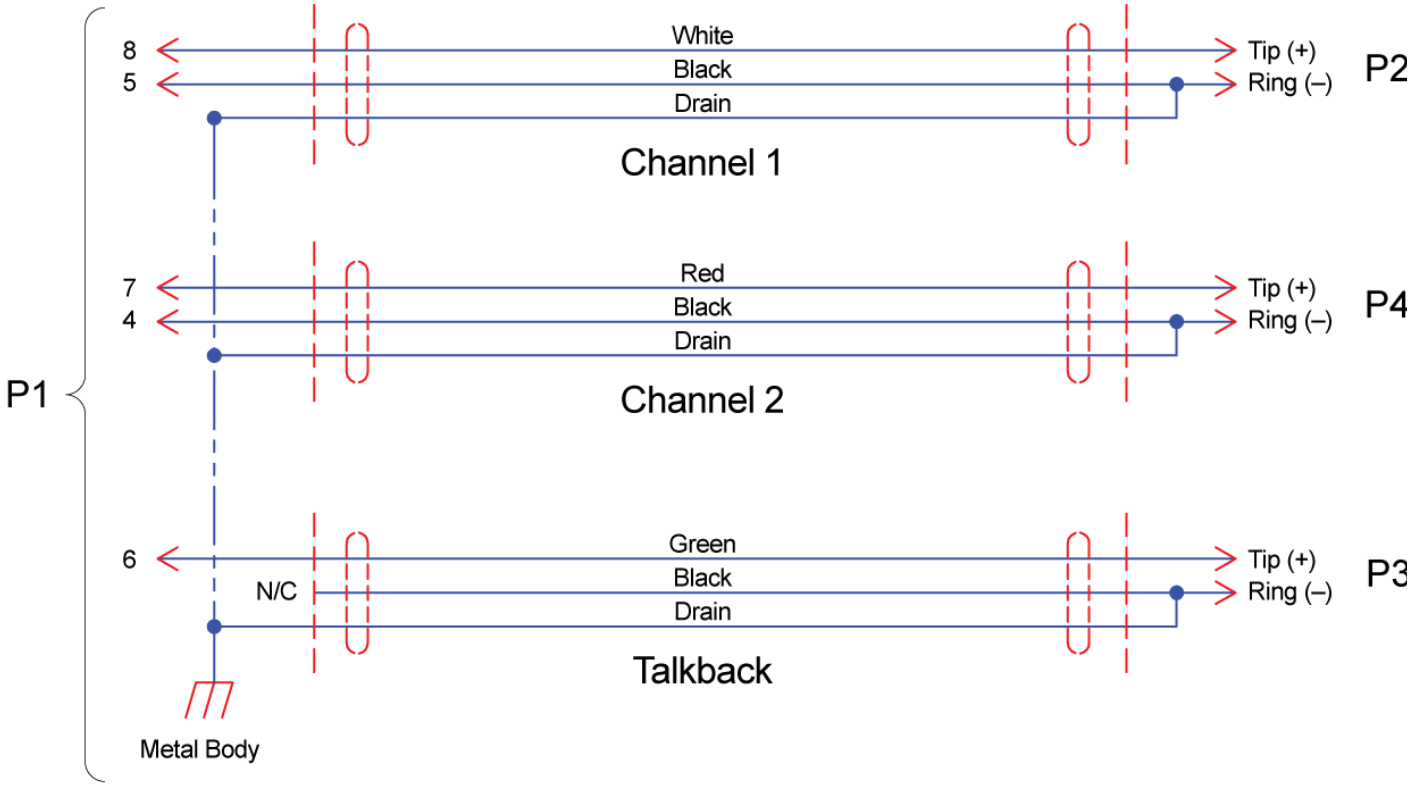
Pin #	Description
1	Reserved / Not Connected
2	Reserved / Not Connected
3	Reserved / Not Connected
4	Channel 2 Negative Signal
5	Channel 1 Negative Signal
6	Talkback Positive Signal
7	Channel 2 Positive Signal
8	Channel 1 Positive Signal

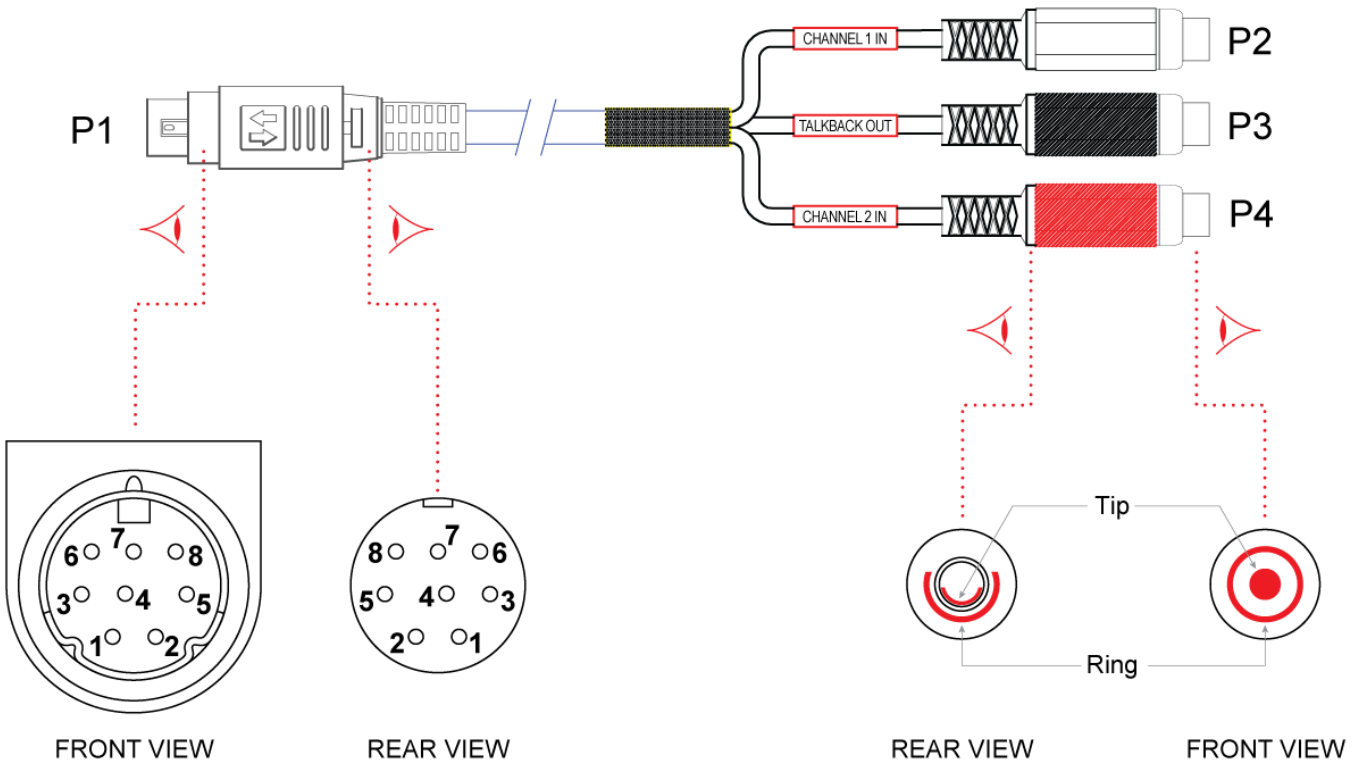


Related Topics

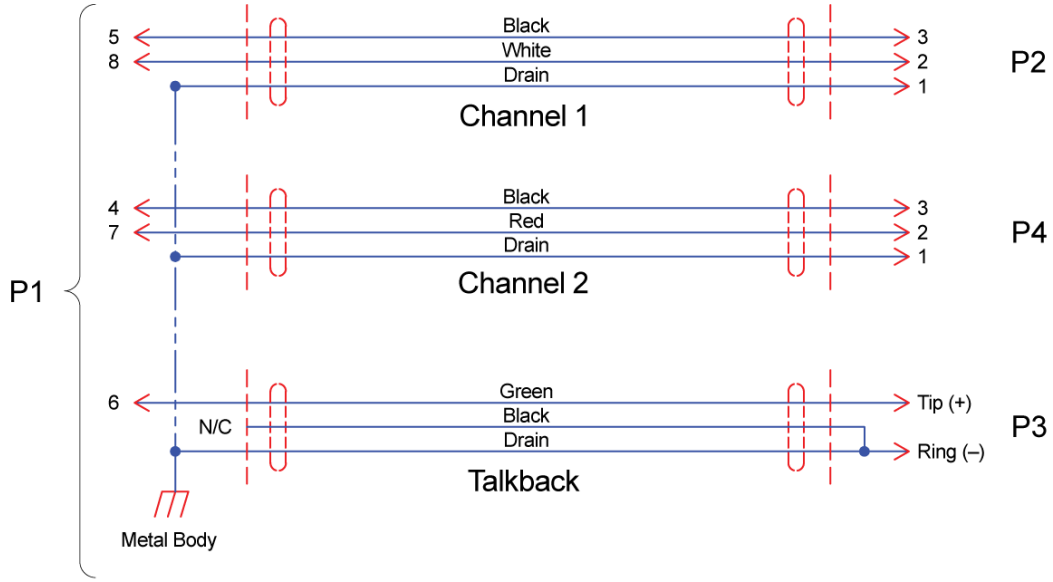
- Audio/Video Interfaces
- Unbalanced Audio Connections
- Balanced Audio Connections

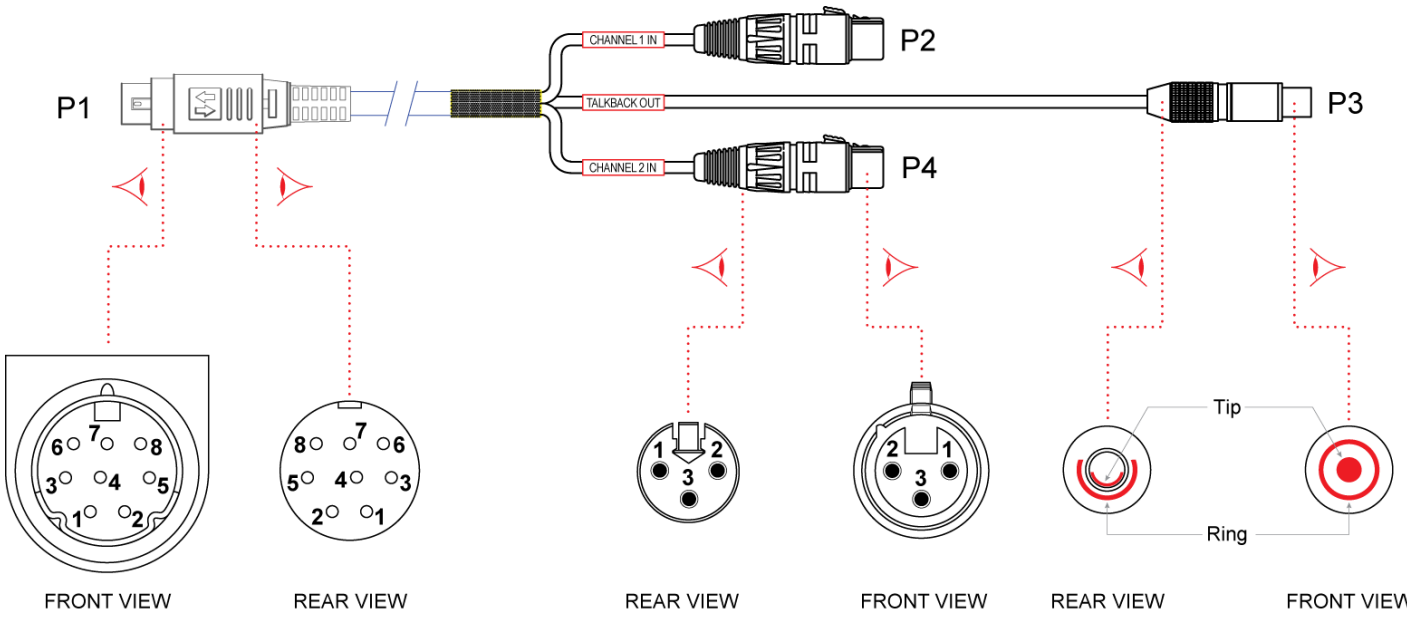
Unbalanced Audio Connections


P1
8
5
White
Black
Drain
Tip (+)
Ring (–)
P2
Channel 1
7
4
Red
Black
Drain
Tip (+)
Ring (–)
P4
Channel 2
6
N/C
Green
Black
Drain
Tip (+)
Ring (–)
P3
Talkback
Metal Body


P1
CHANNEL 1 IN
TALKBACK OUT
CHANNEL 2 IN
P2
P3
P4
Tip
Ring
FRONT VIEW
REAR VIEW
REAR VIEW
FRONT VIEW

Balanced Audio Connections





Audio Breakout Cables

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

Cable	Description	Part Number
Audio Breakout Cable, Unbalanced	Unbalanced mini-DIN 8 to RCA Female • 2 channels input • 1 channel output for talkback support Included in the package (shown in Connecting the DVI-I Interface (Makito X-DVI)).	CA-292-2RTB
Audio Breakout Cable, Balanced	Balanced mini-DIN 8 to XLR Female • 2 channels input • 1 RCA female channel output for talkback support May be ordered from Haivision. Please contact your sales representative or email Haivision at: sales@haivision.com	CA-292-2XFTB

Powering Up the Unit

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

Caution

To prevent damage to the Makito X 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.

Important

There is no power switch on the Makito X appliance. The power is automatically on when the unit is plugged in. When using the AC/DC power adapter, the power supply cord is used as the main disconnect device.
Ensure that the AC socket outlet is located near the equipment and is easily accessible.

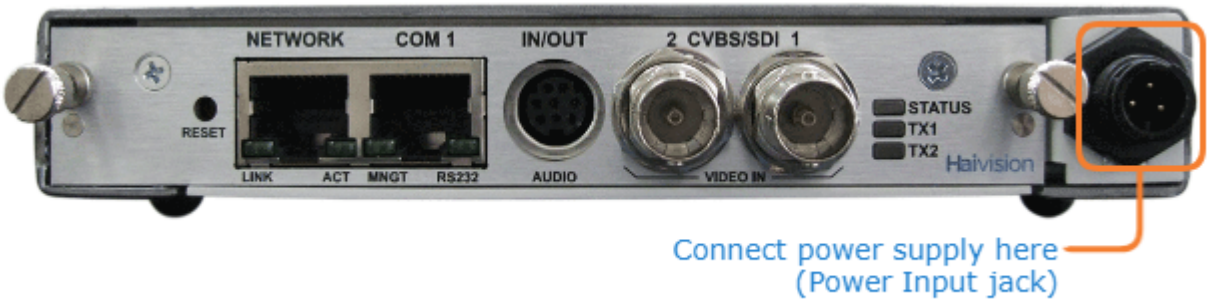
To power up the Single-Height or Double-Height Chassis:

1. Insert the 3-pin connector on the 12V power supply into the Power input jack at the rear of the Makito X.
2. Connect the power cord to the power supply and plug the cord into a grounded AC power source.
3. Wait until the Status LED stays solid green, indicating that the encoder is ready for operation.

Single-Height Chassis | Dual-Height Chassis

Single-Height Chassis

Rear View (Makito X SDI, #S/B-292E-HDSDI2) showing Conxall 3-pin Locking Connector



Conxall 3-pin Connector (Power Adapter 12VDC)

Single-Height Chassis | Dual-Height Chassis

Dual-Height Chassis

Rear View (Makito X HEVC Dual-Channel #S-292E-SDI2-HEVC) ***showing HiRose 3-pin connector***

HiRose 3-pin connector (power supply)

To begin configuring video streams, you can either open the Web interface, or sign in to the CLI.

- To use the Web interface, see **Signing In to the Web Interface**.
- To enter CLI commands, see **CLI Command Reference**.

Resetting the Encoder

- Default Network Settings

This section describes the steps to perform a hardware reset on the Makito X. The Reset button is used either to reset the system or to restore the factory default settings.

- **System Reset:** In some cases, if your encoder is experiencing a problem, resetting the system can return the encoder to normal operation.
- **Factory Reset:** If the problem remains after performing a reset, it may help to restore the encoder to its factory default settings. A factory reset returns the encoder to the same settings it originally had when shipped from Haivision, including the factory default IP address, subnet, and gateway.

Note

After a factory reset, only the firmware revision, serial number, and MAC address are preserved. All other data is deleted (including saved presets, added user accounts, modified passwords, and encoding settings). All settings are returned to their factory preset conditions (including the IP address).

Use one of the following methods to either reset or restore the Makito X settings:

1. With the encoder on, insert a small plastic tool into the small opening labeled **Reset** on the Makito X faceplate.
   Reset micro switch

2. **System Reset:** Press the recessed micro switch (you will feel the button depress) for at least one second and release. Be sure to release the button in less than five (5) seconds.
   -or-
   Factory Reset: Press and hold the recessed micro switch for five (5) seconds.
3. Wait for the encoder to reboot.

   As soon as the lights stop blinking and the Status LED is solid green, the encoder is ready.

Default Network Settings

After a factory reset, the Network settings should be:

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 appliance.

- Cleaning the Ventilation Intake-Outtake
- Monitoring the Fan Operation
- Replacing the RTC Battery

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 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).
- You can check the Web Interface (Status page) or use the CLI (`temperature get` command) to get information from the built-in temperature sensors. If the internal temperature of the unit is rising, that is an indication that the fan may not be operating properly.
- See temperature.

Replacing the RTC Battery

The Makito X 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.

Ruggedized enclosures such as the Makito XR and the Makito XCR do not have a battery.

Tip

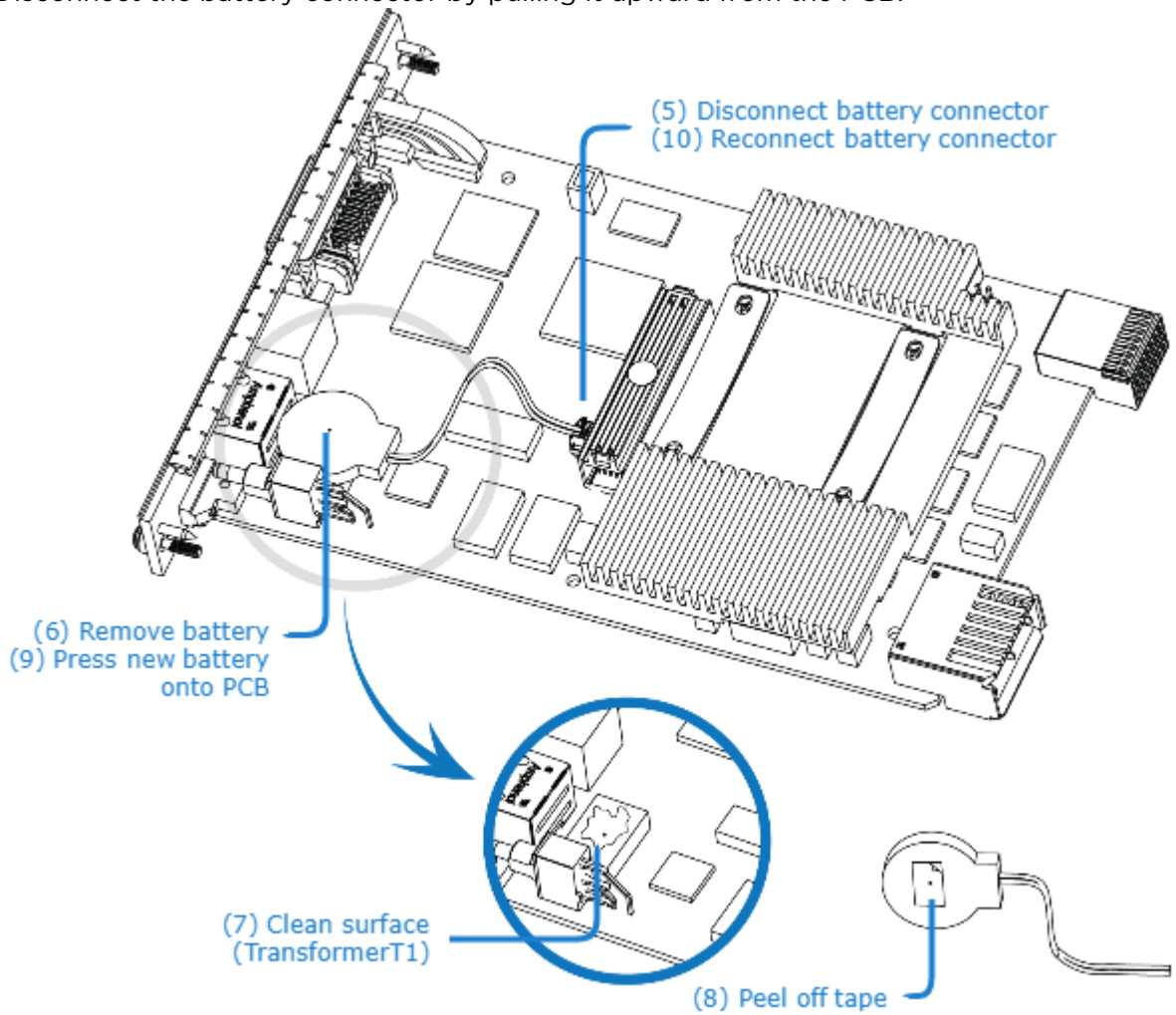
The RTC battery needs to be replaced if at a power-cycle event, the system time and date are reset to within 24 hours, depending on your time zone, of January 1, 1970 (Coordinated Universal Time, UTC).

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.



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.

Getting Started with the Web Interface

Important

Before proceeding, make sure that the encoder is set up correctly and all necessary network and A/V connections are established. See Installing the Encoder.

All Makito X 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 Makito X through its Ethernet LAN port or (if applicable) the Serial Management port.

Topics in This Chapter

- Accessing the Web Interface
- Signing In to the Web Interface
- Exploring the Web Interface
- Changing Your Password
- Signing Out

Accessing the Web Interface

- Security Steps
- Default Encoder IP Address

Managing the Makito X 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.

To access the encoder configuration Web page:

1. **Note**

   The Makito X supports the latest production versions (as of this document date) of the Firefox, Internet Explorer, Safari, and Chrome browsers. Please see the Release Notes (available from the Download Center on the Haivision Support Portal) for any limitations for specific versions of these browsers.

2. Type the encoder's IP Address in the browser's address bar and press Enter.
3. Sign in. (See Signing In to the Web Interface.)

- For a list and description of the CLI commands to configure and manage the Makito X, see CLI Command Reference.
- For information on SNMP management of the Makito X, see Configuring A/V Services Using SNMP.

Security Steps

Only secured HTTP (HTTPS) is supported for the Web interface; therefore, a server certificate is required. The encoder 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 encoder, 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).

Note

The Makito X identity certificate and trusted root certificates are managed using the CLI `certificate` command or Web interface Certificates page. For details, see certificate (CLI) or Managing Certificates (Web interface).

Default Encoder IP Address

Note

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

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

> **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 Encoder.

Role-based Authorization

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

The Makito X 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.

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* (postcard included in the box or available from the Download Center on the Haivision Support Portal) for the default sign-in credentials.

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

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

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

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

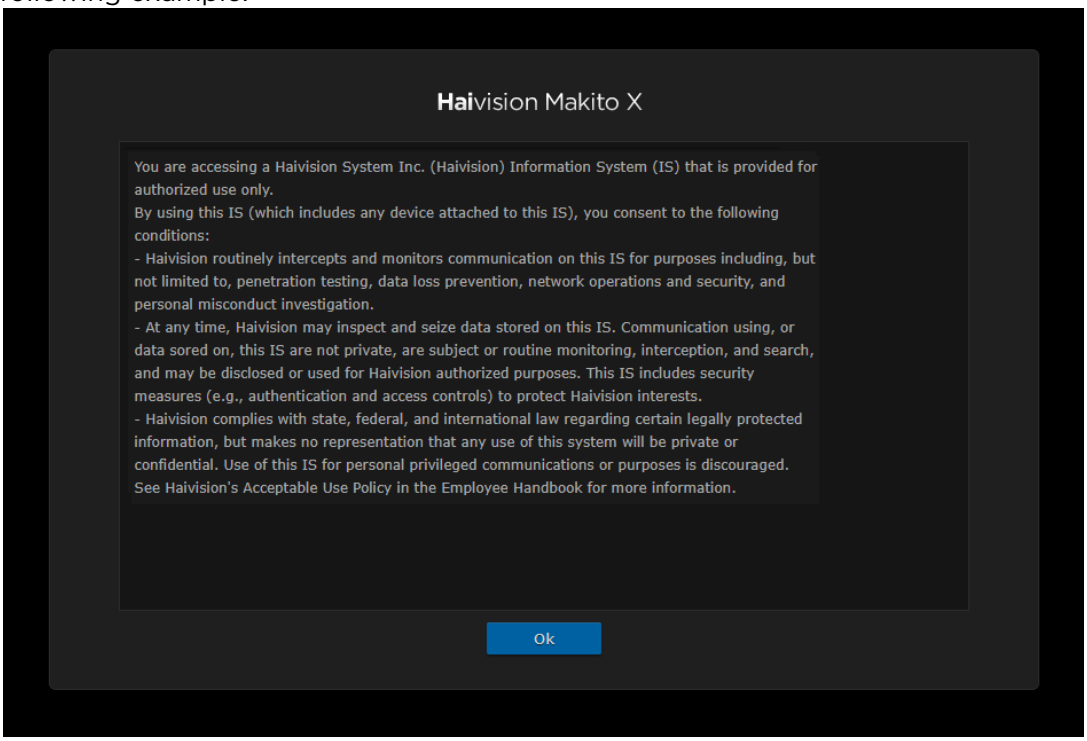
Related Topics

- Command Summary and Access Control

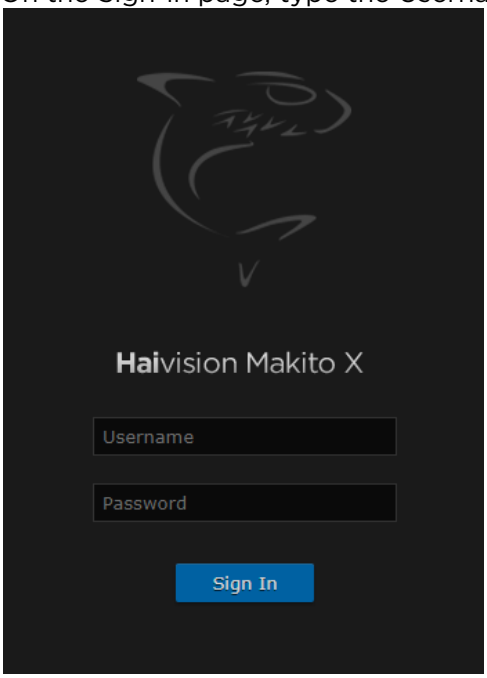
Signing In to the Web Interface

To sign in to the Makito X configuration Web page:

1. From your Web browser, type the Makito X'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**.
3. On the Sign-in page, type the Username and Password and click **Sign In** (or press Enter).



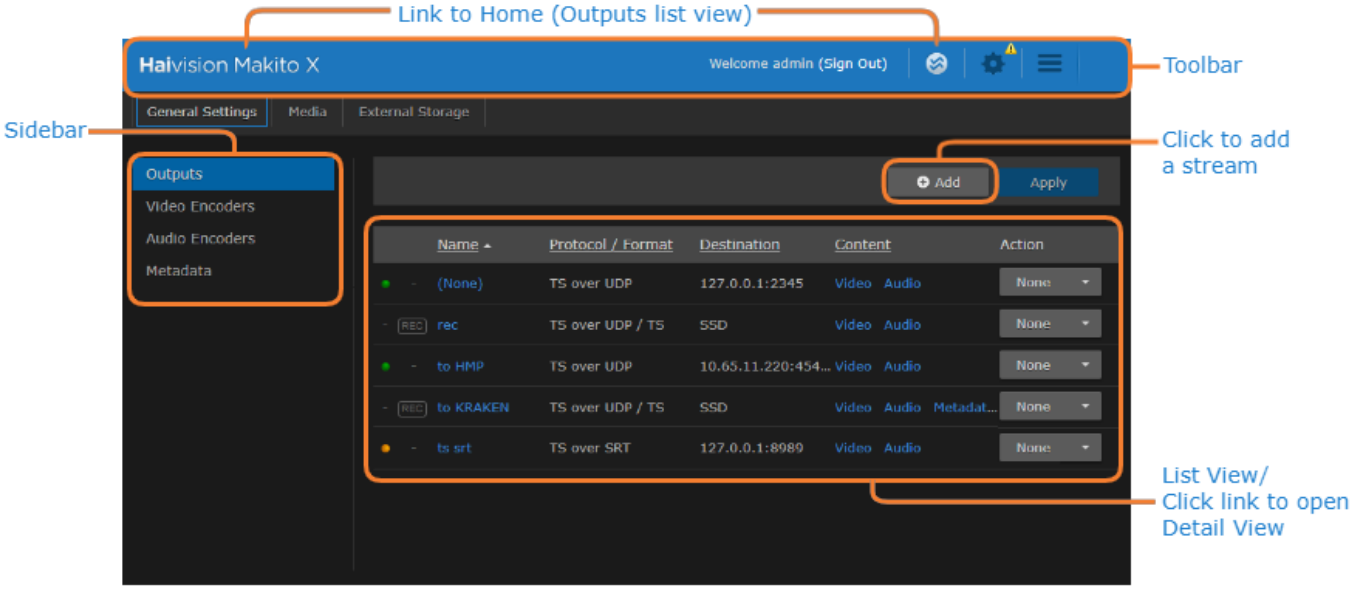
Please refer to the *Important Notice* (postcard shipped with the appliance or available from the **Download Center** on the Haivision Support Portal) for the default sign-in credentials.

Makito X provides three pre-defined user accounts. For information, see **Role-based Authorization**.

Exploring the Web Interface

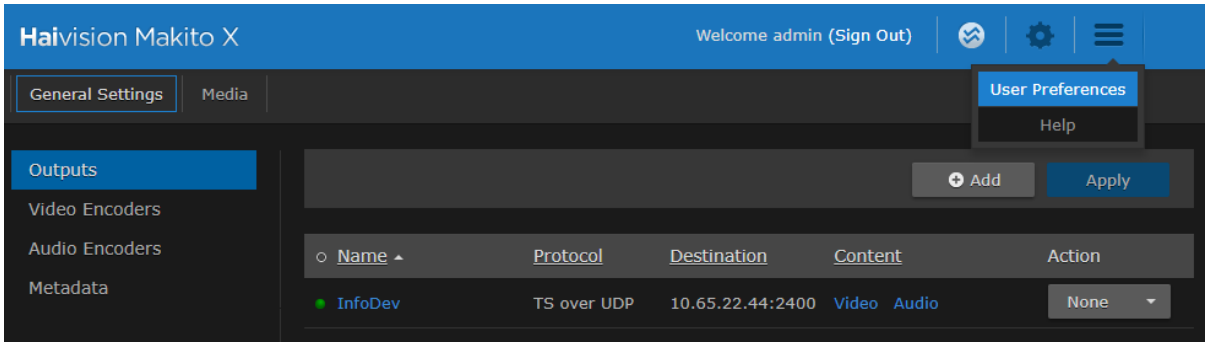
After logging in to the Web interface, you will have access to the encoder configuration settings. All of the settings can be adjusted via the Web browser.

The Web interface opens to the Streaming page (General Settings> Outputs List View, as shown in the following example). Your account information is displayed on the toolbar (along the top).



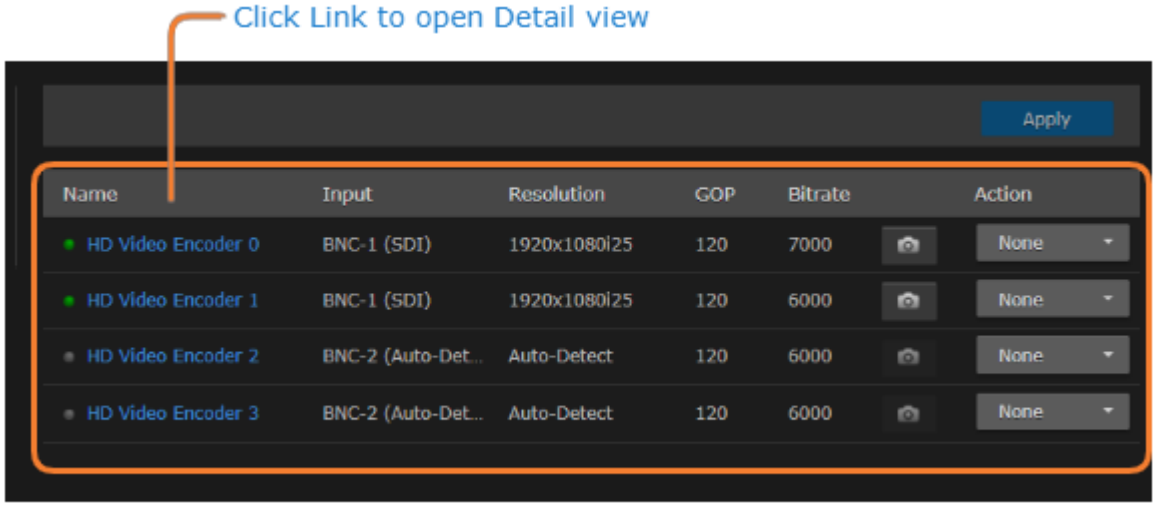
- To set up encoding, select the configuration option from the sidebar, for example, **Video Encoders** or **Audio Encoders** (under **General Settings**).
- To set up streaming or recording, select **Outputs** from the sidebar.
- To manage media, select **Media** on the navigation bar and then the option from the sidebar, for example, **Recordings** or **Snapshots**.
- To access the encoder administration settings, click the **Administration** icon on the toolbar, and then select the option, for example **Network** (under **Settings**) or **Accounts** (under **Security**).
- To access the **User Preferences** or online **Help**, click the icon on the toolbar, and then select either:
  - User Preferences — Opens a dialog to configure preferences such as user interface brightness and contrast control and browser cache reset.

- Help button — Opens the Haivision InfoCenter website that contains the Makito X Encoder documentation.



> **Note**
>
> If no external internet connection is available, a local Makito X Encoder online Help is opened in your web browser

- (Where applicable) On the List View, click a link in the table to open the Detail View. For example, on the Video Encoders List View (shown below), click a link to open the Video Encoder Detail View.

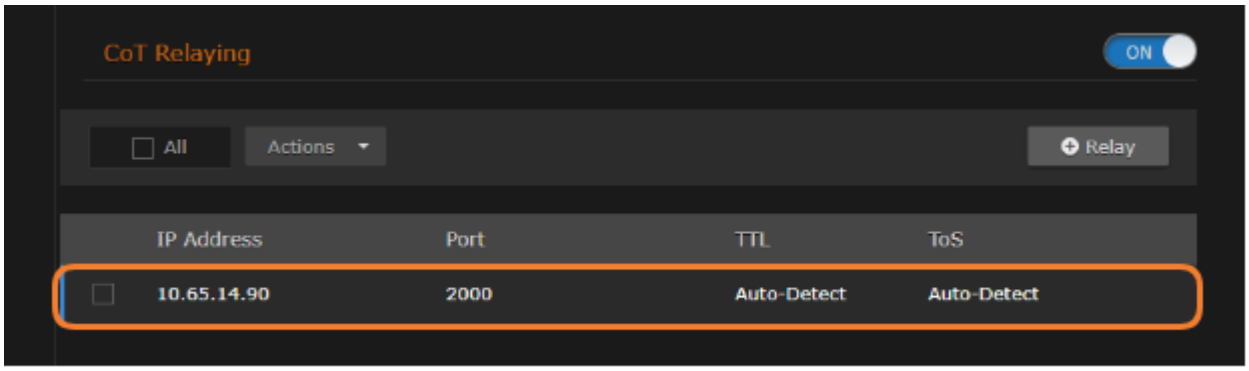


Selecting Items from Lists

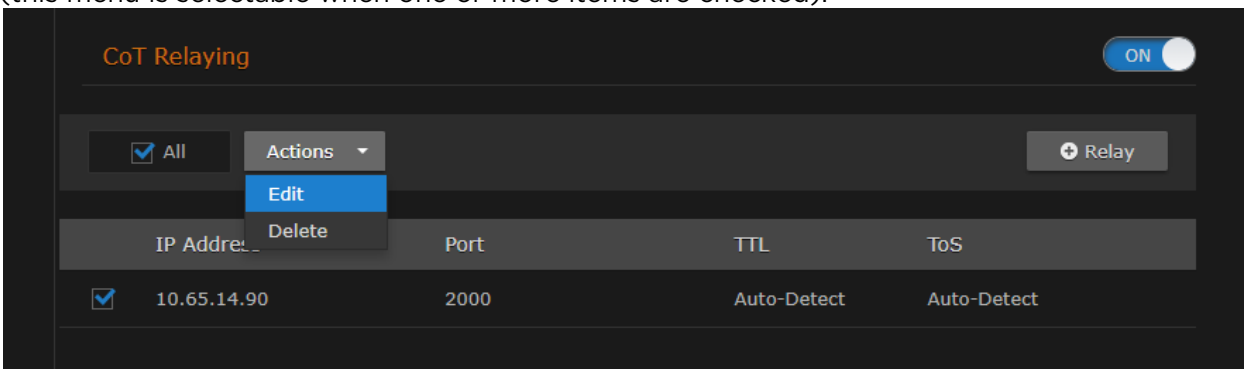
On some Web interface pages, configuration items are presented in lists. Examples include recordings on the Recordings page and CoT Relaying destinations on the Metadata Detail View. This section summarizes the different ways to select list items to perform actions such as editing, deleting, copying, moving, downloading, or exporting.

To select items from a list:

1. Locate the item in the list and click anywhere in the row.



Or check the checkbox next to the item and select the action from the Actions drop-down menu (this menu is selectable when one or more items are checked).



2. To perform actions (such as copy, move, delete or export) on multiple items, you can check multiple items in the list or check **All**.

> **Tip**
>
> You can also shift-click (i.e., click multiple items while holding the Shift key down) to select a range of items (checkboxes).

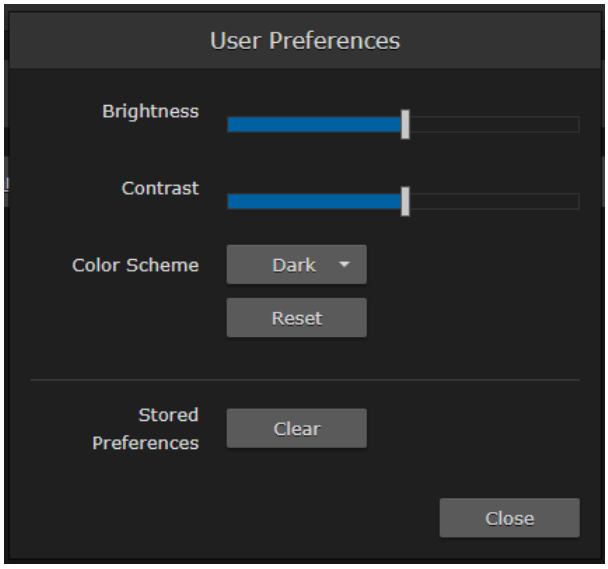
Related Topics

- User Preferences

User Preferences

From the User Preferences dialog, you can customize the following user interface (local browser) options:

- Adjust display settings such as Brightness and Contrast.
- Color Scheme: Switch the color scheme between dark (default) or light.
- Reset Brightness, Contrast and Color Scheme to defaults.
- Local Storage: Clear browser local storage (i.e., User Preference settings that are saved by the browser on the local client PC, such as sort order, list vs. thumbnail view and color scheme).



Related Topics

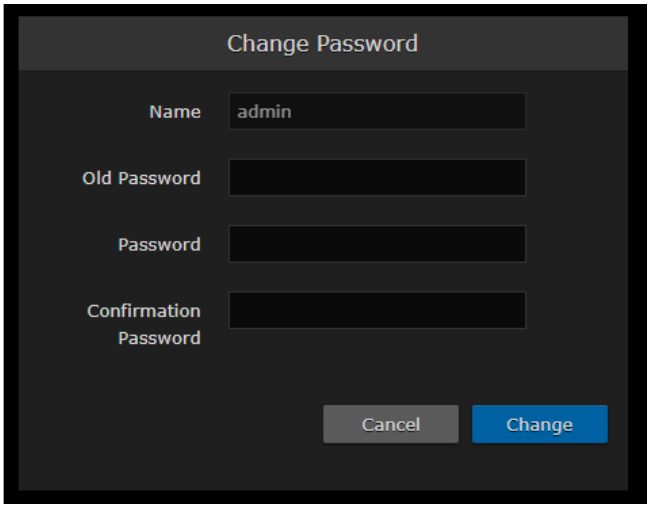
- Changing Your Password

Changing Your Password

- Password Requirements

Important

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



Users assigned either **Operator** or **Guest** roles can change their passwords from the My Account page, as described in this section. This is useful when logging into a Makito X on which the factory defaults have not been changed.

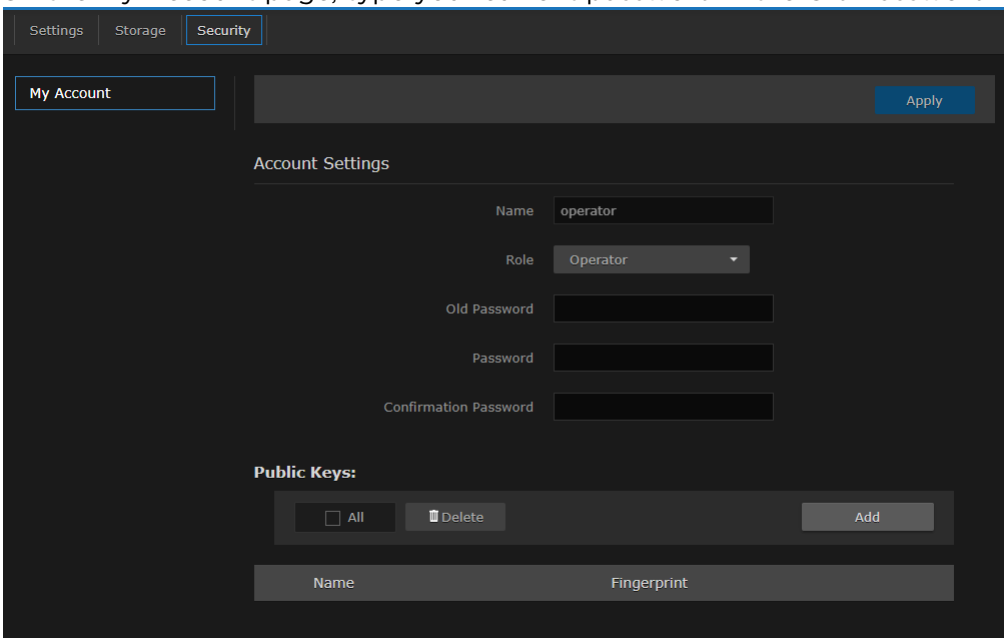
Note

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. Then click **Security** on the navigation bar and **My Account** on the sidebar.

2. On the My Account page, type your current password in the Old Password field.



3. Type the new password in the Password field and again in the Confirm New Password field.
4. Click **Apply**. The new password will take effect immediately.

> **Tip**
>
> Be sure to write down the new password.

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 encoder. For more information, see Managing Public Key Authentication.

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.

Signing Out

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

Signing out prevents misuse and unauthorized access to the encoder.

Managing the Encoder

Note

For a management overview of the Makito X as well as an overview of the Web interface, see Getting Started with the Web Interface.

Topics in This Chapter

- Configuring Video Encoders
- Configuring Audio Encoders
- Configuring Metadata Capture
- Configuring Streaming Outputs
- Configuring Recording Outputs
- Managing Recordings
- Configuring Logo Overlays
- Capturing Image Snapshots
- Configuring Still Image Streaming
- Managing External Storage

Configuring Video Encoders

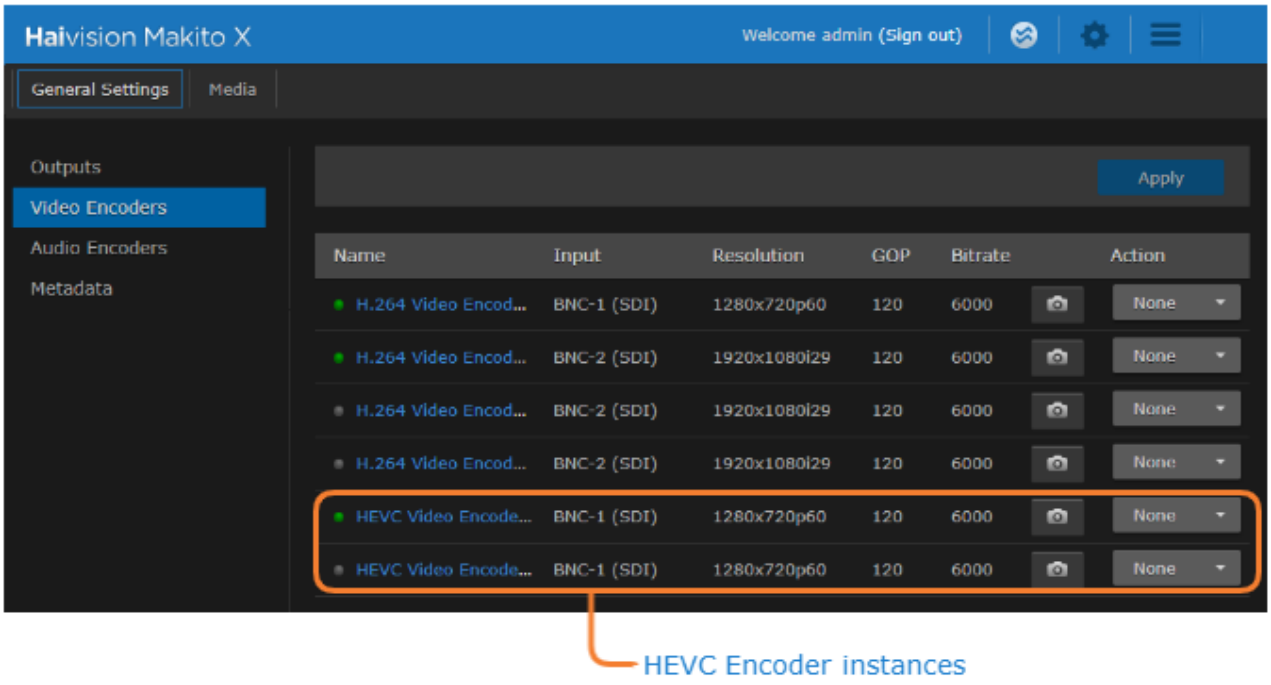
From the Video Encoders pages, you can configure four or eight (Makito X4R only) independent H.264 video encoders to apply to streams. You can start and stop each video encoder, as well as display statistics for the encoder.

With the Makito X HEVC, you can also configure two (additional) HEVC encoders. The Makito X HEVC supports concurrent AVC/H.264 and HEVC/H.265 video encoding.

Video Encoders List View

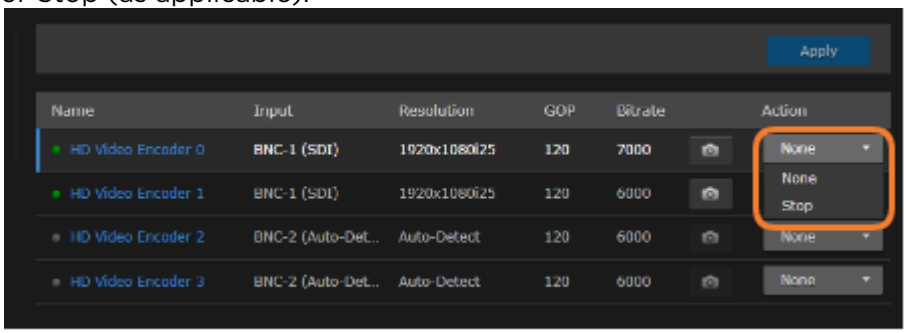
To open the Video Encoders List View:

1. Click the **Streaming** icon on the toolbar. On the Streaming page, click **General Settings** on the navigation bar and **Video Encoders** on the sidebar.
   The Video Encoders List View opens. On the Makito X HEVC, the List View includes two HEVC encoder instances, as shown in the following example:



   The Video Encoders List View displays the status LED, Name, Input format, Resolution, GOP Size, and Bitrate for each video encoder. It also provides an option for you to take a snapshot of an input and either start or stop the encoder.
   - To view details or modify the video settings for an encoder, click a link in the table to open the Video Encoder Detail View.
   - To take a snapshot of an encoder's input, click the Camera icon

- To change the status for an encoder, click the drop-down list under **Action** and select either Start or Stop (as applicable).



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

Configuring Video Encoder Settings

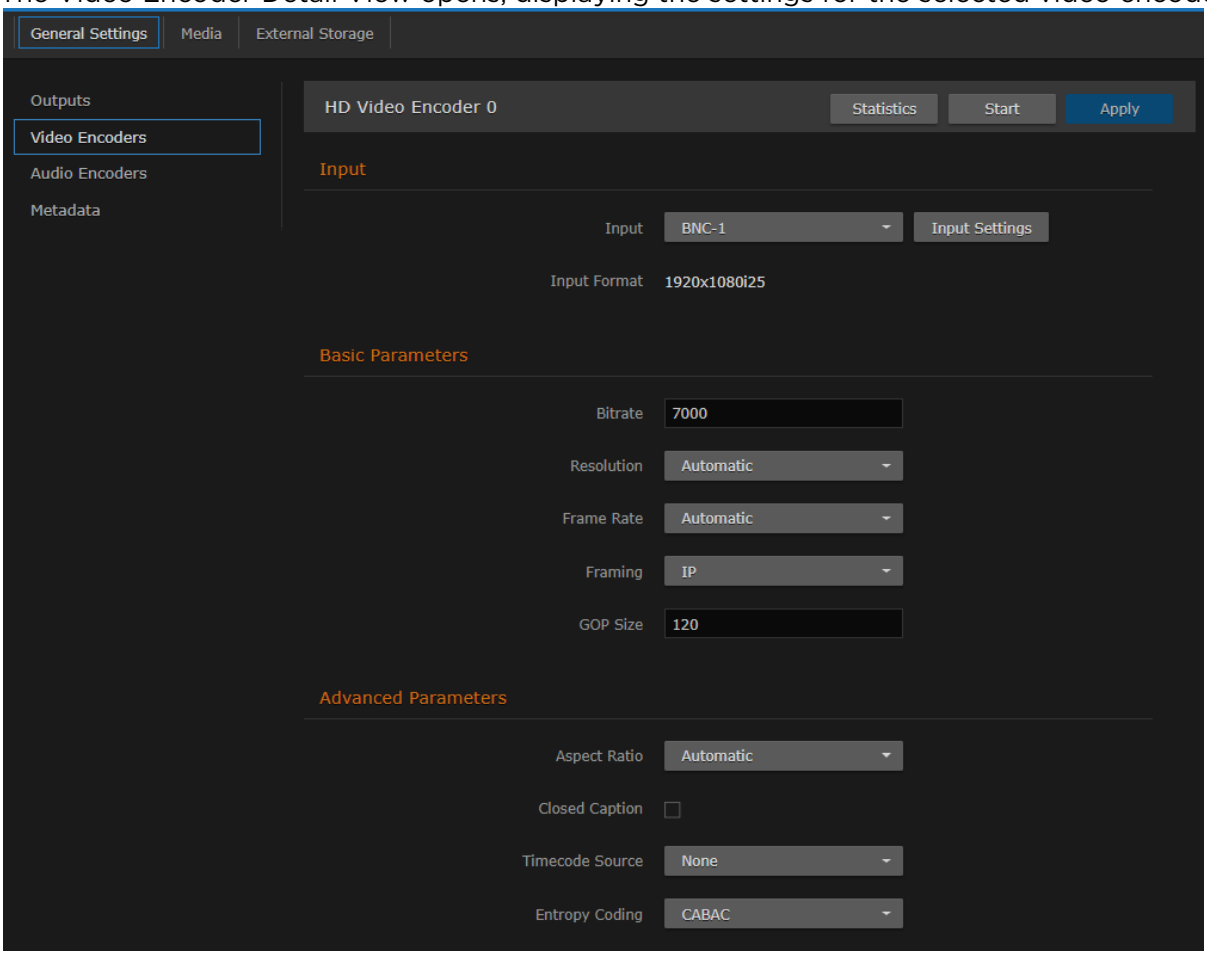
From the Video Encoder Detail View, you can define video encoding parameters for the encoder, such as the Input interface (SDI-only), Bitrate, output Resolution, Frame Rate, and GOP Size.

With H.264 encoding, you can also select a Region of Interest (ROI) to maximize the quality of video within selective portions of the video frame. Or you can enable cropping (within the input image) to enhance the view.

For supported video encoding resolutions, see **Video Encoding** (in **Technical Specifications**).

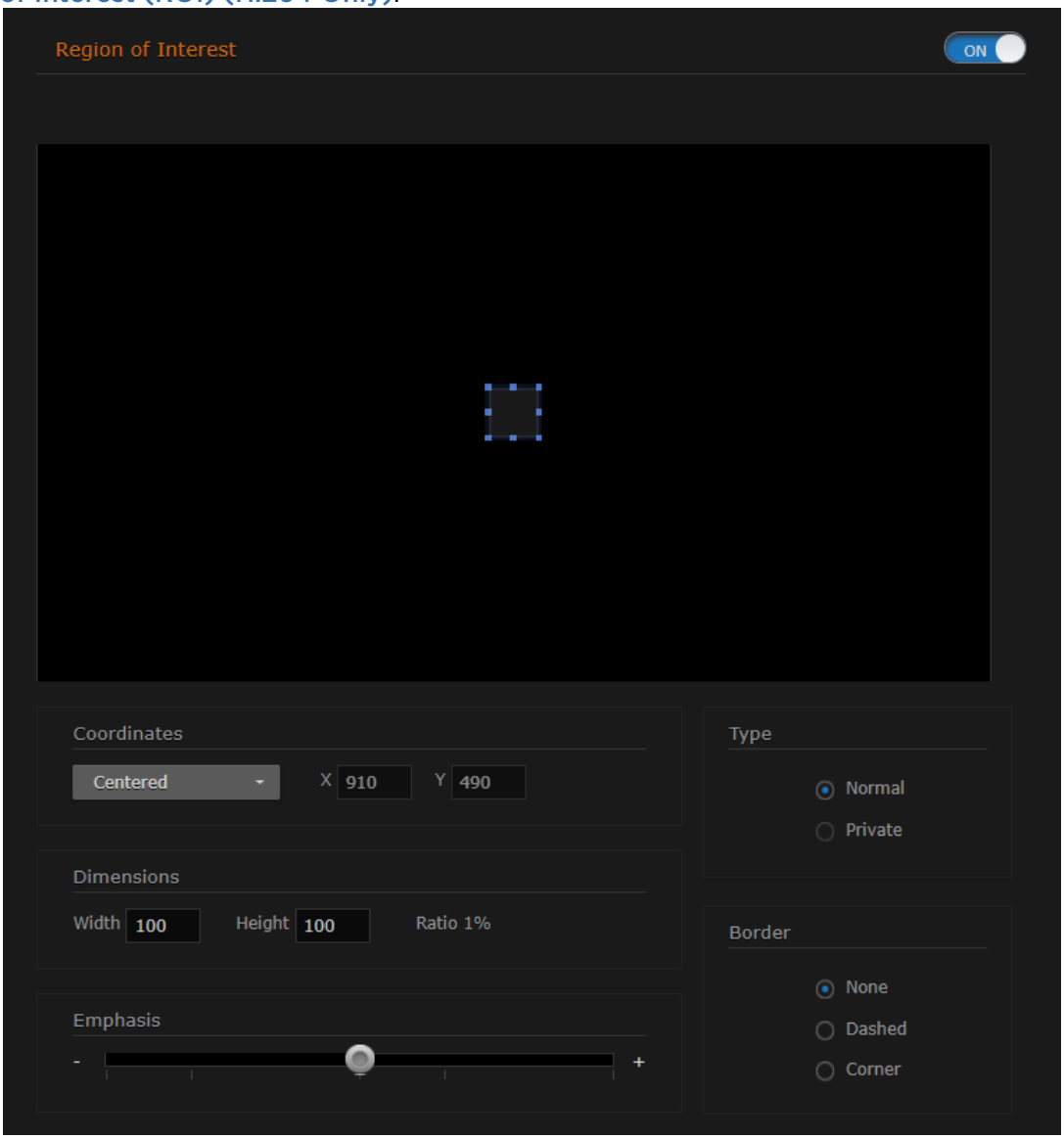
To configure the Video Encoding Settings:

1. From the Video Encoders List View, click a link in the table to select the encoder.
   The Video Encoder Detail View opens, displaying the settings for the selected video encoder.



2. Select or enter the new value(s) in the appropriate field(s). See Video Encoder Settings.

3. (H.264 only) To set up a Region of Interest, toggle the Region of Interest button to **On**. See Region of Interest (ROI) (H.264 Only).



4. To start or stop the encoder, click **Start** or **Stop** (as applicable).
5. To view statistics for the encoder, click **Statistics**. For details, see Video Encoder Statistics.
6. To apply your changes, click **Apply**.
7. To return to List View, scroll up and click **Video Encoders** on the sidebar.

Related Topics

- Video Encoder Settings
- videnc (CLI Command)

Configuring HEVC Video Encoding

From the Video Encoders List View, you can select the HEVC encoding instance and then define the encoding parameters for the HEVC encoder. The Makito X HEVC platform supports three HEVC modes of operation:

- **Single HEVC Encoding** – Up to 1080p60 from an input with frame decimation / downscale support.
- **High/Low HEVC Encoding from the Same Input Source** – A single input signal can be up to 1080p60, but each encoding core can be set up to 1080i30/1080p30/720p60 with frame decimation / downscale support.
- **Dual HEVC Encoding from Different Inputs** – Each input signal can be up to 1080i30/1080p30/720p60 with frame decimation / downscale support.

The total aggregate HEVC encoding capability for all active HEVC video encoders is equivalent to one (1) 1920x1080p60 video signal.

You may select either SD/HD/3G-SDI video input as the video source for each HEVC encoding instance.

Tip

The first HEVC encoder (#4) is the primary encoder and gets preferential treatment when the configuration exceeds the available resources (at least as far as HEVC encoding resources are concerned).
For example, if video encoder #4 is using all HEVC encoding resources (i.e., encoding 1080p60), video encoder #5 is blocked from taking resources from #4, so it cannot be started. But if you reverse the scenario, and video encoder #5 is using all HEVC encoding resources, video encoder #4 is able to start and take all HEVC encoding resources away from #5, and #5 fails/stops.

Related Topics

- Video Encoder Settings
- Dual Channel vs. High/Low Encoding

Video Encoder Settings

The following table lists the Video Encoder controls and settings:

Input | Basic Parameters | Advanced Parameters

Input

Video Encoder Setting	Default	Description/Values
Input		Select the Video Input port for the encoder:
• SDI	BNC-1	• BNC-1 • BNC-2 • BNC-3 (only available on Makito XR) • BNC-4 (only available on Makito XR)
• DVI	DVI	• DVI (read-only)
Input Format	n/a	**Note** If the signal cannot be detected (or is outside the supported range), the Input Format will be Unknown.
Copy Protected Content DVI only	n/a	(Read-only) Indicates whether or not the video source connected to the Makito X DVI is protecting/encrypting its output. If Yes, the stream will not be encoded.
Input Settings		
Type	Automatic	**Note** Automatic mode will cause increased delay during an input switch event. To reduce the re-lock delay, set the Input Type to SDI or Composite as appropriate. BNC: • Automatic • SDI • Composite DVI: • Automatic • Digital (HDMI/DVI) • Analog (Component/RGB)
FIR Filter	Disabled	Check this checkbox to enable Input Image Filtering for the input interface. This parameter filters the video input and removes noise in order to optimize the compression of the image and to enhance the overall quality of the coded video stream.

Colorspace Control (DVI only)	Automatic	(Optional) Select the color space to use while capturing the content. Matching the encoder input color space to the source enhances and optimizes color reproduction. This is useful with source formats such as graphics cards outputting HDTV resolutions. Select either: • Automatic: The encoder determines the appropriate color space to use. • YCbCr: Forces the encoder to use Y,Cb,Cr • RGB (Full Range): Forces the encoder to use RGB Full Range [0..255] • RGB (Limited Range): Forces the encoder to use RGB Limited Range [16..235]
Preferred Resolution (DVI only)	1920x1200p60	Sets the DVI-D preferred input resolution so that connected devices do not scale their output resolutions to undesired resolutions. For more information, see edid.
HDCP (DVI only)	Enabled	Check this checkbox to enable HDCP (High-bandwidth Digital Content Protection) for the DVI interface. • When enabled, HDCP sources will detect the Makito X as a HDCP sink. The source will decide whether or not the content it sends to the Makito X needs to be protected/encrypted. The Makito X will not encode encrypted/protected content. • When disabled, the authentication phase where keys are exchanged will fail and the content source will detect the Makito X as a device that does not support HDCP. At this point, the source will not send any protected content to the Makito X but can still send unprotected content. **Note** Disabling HDCP will allow the Makito X to inter-work with Apple products such as the MacBook and iPad.

Input | Basic Parameters | Advanced Parameters

Basic Parameters

Video Encoder Setting	Default	Description/Values
Bitrate	6000 kbps	Enter the video bitrate for the encoder: 32 to 25,000 kbps

Video Encoder Setting	Default	Description/Values
Resolution	Automatic	Select the stream output resolution (i.e., the number of lines per frame and pixels per line to be encoded): • Automatic: Encodes at the same resolution as the incoming video. • Manually select the coded picture resolution from the list of available options (includes down-scaled resolutions). The options depend on the Input Format detected. **Note** For supported video encoding resolutions, see Video Encoding.
Cropping	Disabled	This parameter crops the input and encodes to a rectangle within the input image while discarding the rest of the input image. **Note** Cropping is disabled if Resolution is Automatic, 960, or 1440, or if Resolution (i.e., output resolution) is set to equal or larger than the input resolution.
Frame Rate	Automatic	Select the coded picture frame rate per second: • Automatic: Encodes at the same frame rate as the input • 60..1 **Note** The frame rate cannot exceed the input frame rate.
Framing	IP	Select the video compression mode for the encoded video: • I: I frames only (lowest delay; lowest quality) • IP: I and P frames only • IBP: I, B and P frames (H.264 only) • IBBP: I, BB (two B frames in sequence) and P frames (highest delay; highest quality) (H.264 only) **Note** B frames require a Main Profile decoder. B frames provide more quality as the encoding is more efficient; thus more details can be rendered in the same bandwidth/bitrate. **Tip** When B frames are used, the GOP may be rounded up to make the sequence end with a P frame.
GOP Size	120	Enter the Group of Pictures size for the encoded video.1..1000

Advanced Parameters

Video Encoder Setting	Default	Description/Values
Aspect Ratio	Automatic	Specifies the aspect ratio of the video source and signals it into the MPEG stream: • Automatic: Aspect ratio is derived from the incoming video source resolution. • Manually force aspect ratio to either: 3:2, 4:3, 5:3, 5:4, 16:9, 16:10, or 17:9. • WSS/AFD: Aspect ratio is extracted from the incoming video source based on WSS (Wide Screen Signaling) or AFD (Active Format Description) if detected. **Note** WSS is only supported with analog PAL video; AFD is only supported with SDSDI video.
Closed Caption	Enabled	**Note** For more information, see Closed Captioning.
TimeCode Source	None	Timecodes are used to mark video frames, mainly for editing purposes. This field either disables timecoding, or selects the source to “timecode” the encoded video frame. The following selections are available: • None: No time code will be inserted in the video stream (saves bandwidth if not required). • Video (SDI only): The timecode will be extracted from the incoming video signal. • System: If no timecode is included in the video feed, the encoded timecode is based on the encoder’s system clock. In this case, it is a good idea to enable NTP (see Configuring Network Settings). **Note** See TimeCode Source for additional information.

Video Encoder Setting	Default	Description/Values
Entropy Coding	CAVLC	(H.264 only) Select the compression scheme: • CAVLC: Context-adaptive Variable-length Coding is a lower-complexity alternative to CABAC. CAVLC produces lower quality, but is easier to decode. • CABAC: Context-adaptive Binary Arithmetic Coding is an algorithm to losslessly compress syntax elements in the video stream. CABAC compresses data more efficiently than CAVLC and should produce better quality, but requires considerably more processing to decode. **Note** The H.264 decoder must be Main Profile compliant or higher to decode a CABAC video stream. **Tip** CABAC provides better visual quality because it is more efficient.
Partitioning	Disabled	(H.264 only) Check this checkbox to enable Intra-Picture Sub-Partitioning. **Note** Intra-Partitioning requires that the H.264 decoder be High Profile compliant. Intra-Partitioning provides better visual quality because it gives the video encoder better coding tools. **Tip** Noisy Matrix completion is enabled automatically when Partitioning is enabled and video bitrate is under 800 Kbps. Noisy Matrix completion enhances video image “noise” reduction to improve video quality at lower bitrates and make blocky artifacts less visible.
Intra Refresh	Disabled	(H.264 only) Check this checkbox to enable Intra-refresh video encoding support. **Tip** Intra-refresh requires that the decoder and streams be started first.
Intra Refresh Rate	60	**Note** If the refresh rate is set too low, a leftto-right wave-like artifact may result.
Partial Image Skip	Disabled	Allows the encoder to skip part of the image in order to respect the bitrate limit.

Related Topics

- Region of Interest (ROI) (H.264 Only)
- TimeCode Source

Region of Interest (ROI) (H.264 Only)

The following table lists the Video Encoder Region of Interest controls and settings:

Video Encoder Setting	Default	Description/Values
Region of Interest	Off	Use to create a static region of interest (one per video encoder) to enhance the quality of the encoded video within the region. This allows you to choose what portion of the image is important to have maximum quality. **Tip** To get started, position the region in the center and then adjust the size.
Coordinates	Centered	Select the position for the region: • Centered • Top Left • Top Right • Bottom Left • Bottom Right • **Note** In Absolute mode, the region is positioned at the exact X and Y coordinates specified. You can type in a value or use the Up and Down arrows on your keyboard to change the value: • Up/Down Arrow: Increase/Decrease value by 1 unit • Shift-Up/Down Arrow: Increase/Decrease value by 10 units If you select any other option than Absolute, the X and Y input boxes are disabled. If you drag the ROI, the Coordinates drop-down automatically switches to Absolute and the X and Y input boxes are enabled.
X, Y	Default varies with input resolution	**Note** Only takes effect if Coordinates is set to Absolute.
Type	Normal	Specifies the effect of the region: • Normal: ROI is translucent, therefore enhances the video in the region. • Private: ROI is opaque to block out the ROI video. Also Emphasis is grayed out (since no longer applicable)
Dimensions	100, 100	Specifies the width and height of the region. You can type in a value or use the Up and Down arrows on your keyboard to change the value. See Coordinates above.

Video Encoder Setting	Default	Description/Values
Ratio	1%	**Note** The ratio must not exceed 30% in order to see the quality difference between the background and the ROI.
Border	None	(Optional) Applies a border to the region: • None: No border around the ROI • Dashed: Thin dashed border around the ROI • Corner: Borders on each corner of the ROI. **Note** Once a region of interest with borders is enabled on a video encoder, all the video encoders using the same video input will show that border in their encoded output regardless of whether or not ROI is enabled on them.

Video Encoder Setting	Default	Description/Values
Emphasis	4	Sets the difference in quality between the ROI and the rest of the input image. **Tip** You can either move the slider to the desired value, click along the slider frame, or click the "-" or "+" to change the slider position.
Stop **Start**	n/a	Click Stop to stop an active encoder. Click Start to start or restart a stopped encoder.
Statistics	n/a	Click Statistics to view statistics for the encoder. See Video Encoder Statistics.

TimeCode Source

The following table lists the possible TimeCode sources when "Video" is selected:

Input Type	Possible TimeCode Source(s)
CVBS Input signal	1) VITC (The timecode is extracted from the Vertical Interval TimeCode of the incoming video signal).
SD/HD/3G-SDI	1. MISB 0605 KLV micro-second timestamp (if KLV is enabled) 2. ATC_VITC 3. MISB 0601 KLV micro-second timestamp (if KLV is enabled) 4. System Time clock **Note** The one to be carried is chosen based on the time difference between the timecode STC (System Time Clock) and the coded picture.

Note

The digitized version of VITC (referred to as D-VITC) is not supported. Only ATC_VITC (Ancillary Timecode) is supported.
Although LTC (Linear Timecode) and VITC timecodes may be present at the same time, the current release only supports VITC. LTC ancillary packets will be ignored.

Video Encoder Statistics

The following table lists the Video Encoder statistics:

Video Encoder Statistic	Description/Values
State	The current operating status of the encoder, either: • WORKING • STOPPED
Up Time	(only available when State is WORKING) The length of time the encoder is actively encoding (e.g., 1d22h5m41s).
Input Present	Indicates whether an input signal has been detected from the video source: Yes / No
Input Type	The video input for the encoder: For example, SDI, Composite, or DVI.
Input Format	The input signal detected from the video source.
Protected Content	(DVI only) Indicates whether or not the video source is protecting/ encrypting its output. Yes / No
Output Resolution	The stream output resolution.
Aspect Ratio	The aspect ratio of the video source.
Encoded Frames	Number of encoded frames.
Encoded Bytes	Number of encoded bytes.
Encoded Frame Rate	The video frame rate per second.
Dropped Frames	Number of dropped frames.
Encoder Resets	Number of encoder resets.
Encoded Bitrate	The video bitrate used for the encoder (in kbps).
Encoder PTS	The current encoder Presentation Time Stamp (PTS) based on a 90 kHz clock: e.g., 0x138a56483
Encoder Load	The video encoding processor usage of the stream instance in percentage (%).
Closed Captioning	Indicates whether Closed Captioning (CC) is Enabled or Disabled on the output Stream.
Extracted CC Bytes	(CC must be enabled) Number of extracted Closed Captioning Bytes.
CC Errors	(CC must be enabled) Number of Closed Captioning errors.
Extracted CSD Bytes	**Tip** CSDs define signaling and announcement of caption services.
Timecode Source	(Timecoding must be enabled) The selected timecode source. See TimeCode Source.

Video Encoder Statistic	Description/Values
Timecode	The timecode for the encoded video frame. Or the system time if user has chosen “system” for the TimeCode Source displayed as (HH:MM:SS:FF) Hours, Minutes, Seconds and Frames.
H.264 Profile	The application profile class for the encoder: e.g., Main, High, or Baseline.
H.264 Level	The required level of decoder performance to be able to process the video incoming stream: e.g., 3, 3.2, 4, or 4.2
Reset	Click to reset the Video Encoder statistics.

Makito Decoder Interoperability

The following table lists recommended settings to optimize the Makito X encoder configuration to stream to the Makito X decoder:

Video Encoder Parameters	**Recommended Settings**
Entropy Coding	CAVLC or CABAC
Partitioning	On or Off
GOP Structure	I/IP/IBP/IBBP
Bitrate	32..25000

The following table lists *required* Video Encoder settings when configuring the Makito X encoder to interoperate with the Makito Classic (*previous generation*) decoder:

Video Encoder Parameters	**Required Settings**
Entropy Coding	CAVLC only
Partitioning	Off only
GOP Structure	I and IP only
Bitrate	150..15000

Configuring Audio Encoders

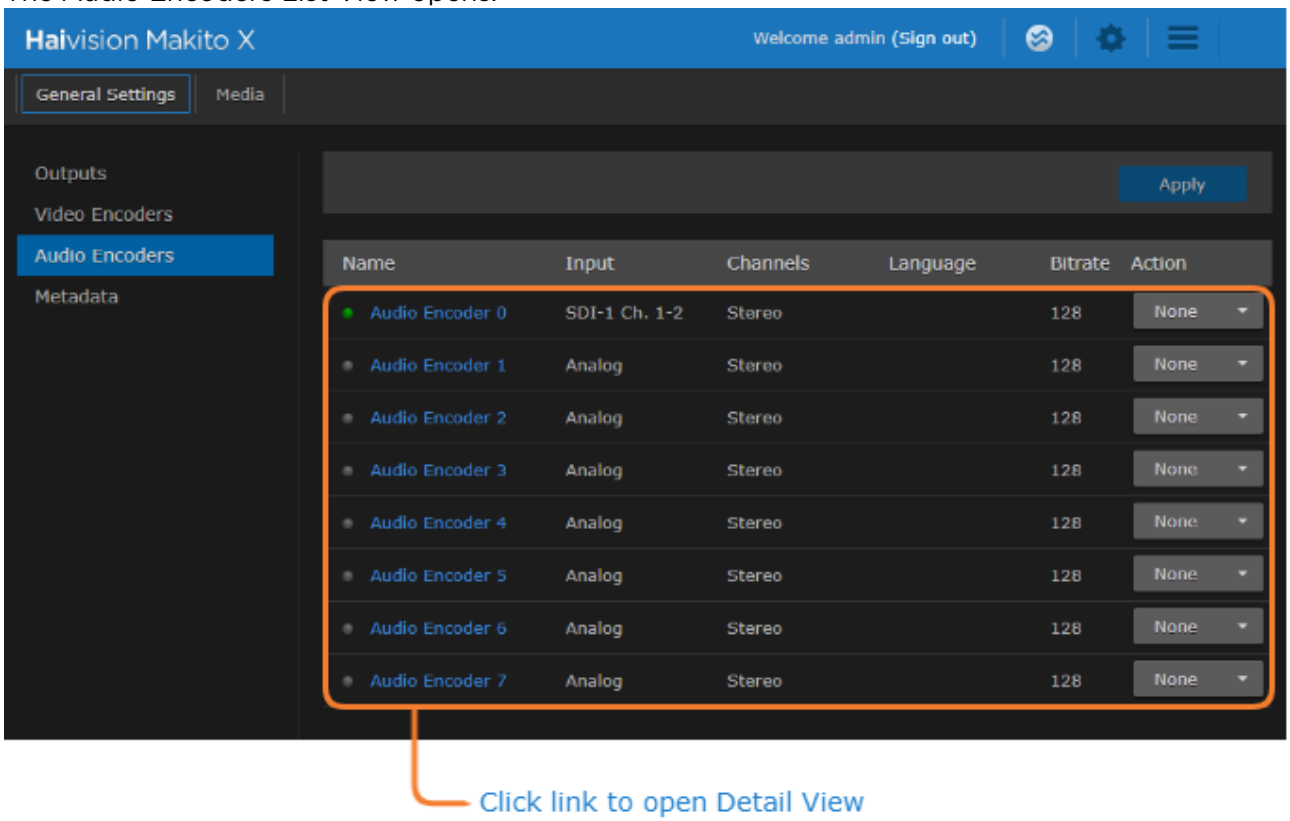
Note

The Makito X SDI and Makito X DVI blades are capable of encoding up to 16 channels of audio in channel pair groups: 16 for dual-channel SDI, 8 for single-channel SDI, 2 for DVI-D, and 2 for Analog audio in any combination.

Audio Encoders List View

To open the Audio Encoders List View:

1. On the Streaming page, click **General Settings** on the navigation bar and **Audio Encoders** on the sidebar.
   The Audio Encoders List View opens.



The Audio Encoders List View displays the status LED, Name, Input, Channel Mode, Language, and Bitrate for each audio encoder. It also provides an option for you to either start, stop, or mute each input.

- To view details or modify the audio settings for an encoder, click a link in the table to open the Audio Encoder Detail View.

- To change the status for an encoder, click the drop-down list under **Action** and select either Start or Stop (as applicable), or Mute.

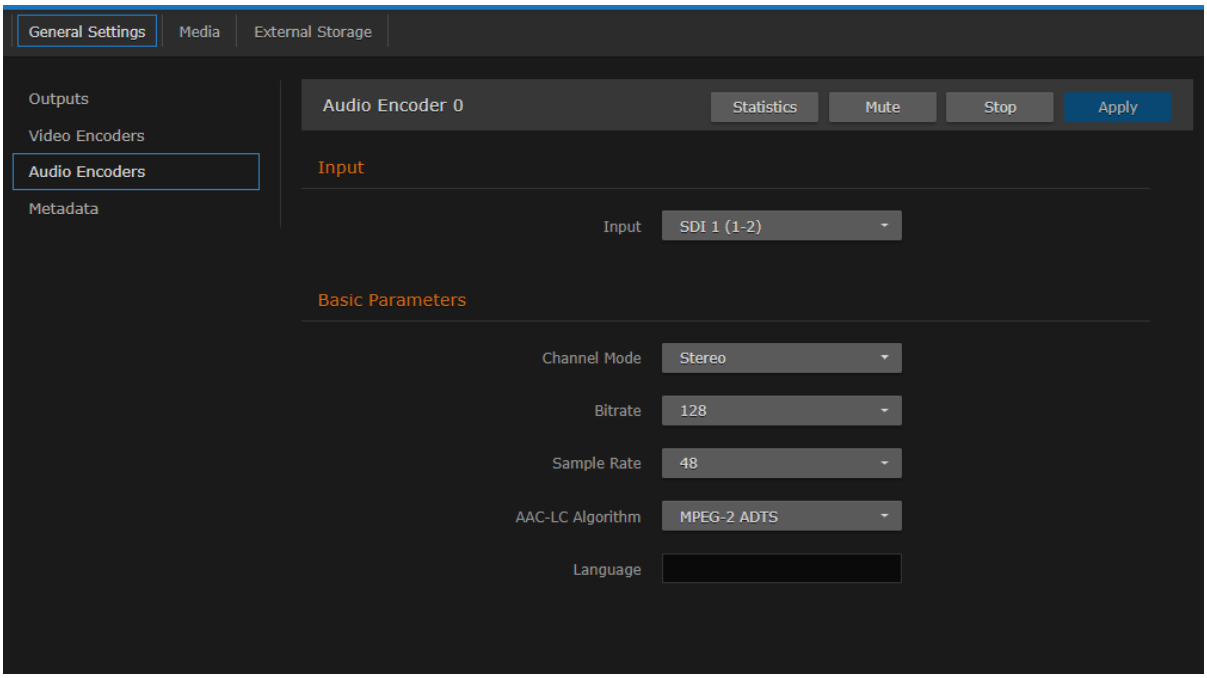
2. To apply your changes, click **Apply**.

Configuring Audio Encoder Settings

> **Note**
>
> Analog audio in cross-clock domain streams (such as audio clocked on one BNC sent with video from another BNC) may have occasional audio artifacts.

To configure the Audio Encoding Settings:

1. From the Audio Encoders List View, click a link in the table to select the encoder.
   The Audio Encoder Detail View opens, displaying the current audio settings for the selected encoder.



2. Select or enter the new value(s) in the appropriate field(s). See Audio Encoder Settings.
3. To start or stop the encoder, click **Start** or **Stop** (as applicable).
4. To mute the audio (when active), click **Mute**.

> **Note**
>
> When an audio encoder is muted, it still generates audio data, but the audio content is silence. For more information, see "Mute" in "Basic Parameters" in Audio Encoder Settings.

5. To view statistics for the encoder, click **Statistics**. For details, see Audio Encoder Statistics.
6. To apply your changes, click **Apply**.
7. To return to List View, click **Audio Encoders** on the sidebar.

Related Topics

- Audio Encoder Settings
- audenc (CLI Command)

Audio Encoder Settings

The following table lists the Audio Encoder controls and settings:

Input Basic Parameters

Input Parameters

Audio Setting	Default	Description/Values
Input		Select the Audio Input for the encoder.
SDI	Analog	• Analog • SDI1 (1-2). . (15-16) • SDI2 (1-2). . (15-16) **Note** The SDI2 audio inputs are only available on dual-channel systems. **Tip** For Analog audio, on dual input SDI encoders, you may need to specify the video input from which to derive the audio encoder's STC source (either Auto, BNC1, or BNC2). This is done using the CLI. For details, see “stcif” in audenc.
DVI	Analog	• Analog • DVI (1-2)

Input Basic Parameters

Basic Parameters

Audio Setting	Default	Description/Values
Channel Mode	Stereo	Select the number and type of audio channels to encode: • Stereo • Mono-Left • Mono-Right
Bitrate	128 kbps	Select the Audio Bitrate for the encoder: • Mono: 56 to 160 kbps • Stereo: 80 to 320 kbps
Sample Rate (kHz)	48 kHz	The number of audio samples per second taken from the incoming signal. 48 kHz only.

Audio Setting	Default	Description/Values
AAC-LC Algorithm	MPEG-2 ADTS	The audio compression algorithm: • MPEG-2 ADTS - Encodes audio using the ISO/IEC 13818-7 MPEG-2 AAC-LC algorithm with an ADTS header. (Default) • MPEG-4 LOAS/LATM - Encodes audio using the ISO/IEC 14496-3 MPEG-4 AACLC algorithm with a LOAS/LATM header.
0 dBFS Audio Level (dBu)	+6 dBu	**Note** This is useful in applications such as broadcast and streaming to allow higher audio headroom. **Tip** This parameter specifies the audio level at which full scale is achieved. 5 = Full scale in the coded audio is achieved when a 5 dBu input signal is input at the audio input. 20 = Full scale in the coded audio is achieved when a 20 dBu input signal is input at the audio input. This means that if the same audio input signal is sent to a Makito, it will sound louder at the decoder when the input signal level is set to 5 than if the level is set to 20.
Language	n/a	To specify the language of the input, start typing letters and select the language from the list.
Mute	n/a	Click Mute to encode silence instead of the selected audio input. For example, this may be used when you do not wish to encode the audio but the decoder being used does not support decoding of video only streams.
Stop **Start**	n/a	Click **Stop** to stop an active encoder. Click **Start** to start or restart a stopped encoder.
Statistics	n/a	Click Statistics to view statistics for the encoder. See Audio Encoder Statistics.

Audio Encoder Statistics

The following table lists the Audio Encoder statistics:

Audio Encoder Statistic	Description/Values
State	The current operating status of the encoder, either: • WORKING • STOPPED
Encoded Frames	Number of encoded frames.
Encoded Bytes	Number of encoded bytes.
Encoded Bitrate	The audio bitrate used for the encoder (in kbps).

Audio Encoder Statistic	Description/Values
Encoder Errors	Number of audio encoding errors.
Encoder PTS	The current encoder Presentation Time Stamp (PTS) based on a 90 kHz clock: e.g., 0x138a56483
STC Source Interface	(only available when State is WORKING) The audio input from which the audio STC (System Time Clock) is derived: either BNC-1 or BNC-2, or DVI-D.
Maximum Sample Value	The largest sample in the last audio frame (total of 1024 samples per frame). (Duration: 21 ms)
Reset	Click to reset the Audio Encoder statistics.

Configuring Metadata Capture

Important

Metadata processing is a licensed feature which may be installed at the factory or via a field upgrade by installing a license file.

From the Metadata pages, you can configure the Makito X to capture either KLV (Key Length Value) or CoT (Cursor on Target) metadata and then incorporate data information within the metadata elementary stream of the standard MPEG Transport Stream.

You can set up multiple metadata inputs to include in Transport Streams. The Makito X supports up to three metadata input types:

- **Serial port (Makito X SDI only):** The Makito X SDI extracts either KLV or CoT metadata packets from the COM1 serial port. See Configuring Serial Metadata Sources.
- **SDI (Makito X SDI only):** The Makito X SDI extracts KLV metadata packets from the HD-SDI interface as per MISB RP 0605.2. See Configuring HD-SDI Metadata Sources.
- **Network:** The Makito X captures metadata from a user definable network port (up to eight UDP inputs). The encoder can receive either (a) KLV payload encapsulated in UDP or (b) CoT inside UDP that is converted to KLV and then streamed. See Configuring Network Metadata Sources.

The Makito X auto-detects the hardware setup of the encoder. If the serial port or SDI video is connected, the serial or SDI metadata source is created automatically at startup by the system. For Serial input, the COM Port Mode must also be set to Metadata (see "Mode" in COM Port Settings). UDP sources must be manually created by the user. The Makito X supports insertion of multiple metadata sources into the same KLV Elementary Stream.

The Makito X supports both synchronous and asynchronous KLV metadata stream signaling and AU (Access Unit) transport support. When configuring a stream, you can select the encapsulation type to use for the associated KLV metadata source. For technical specifications, see Asynchronous KLV Metadata Support.

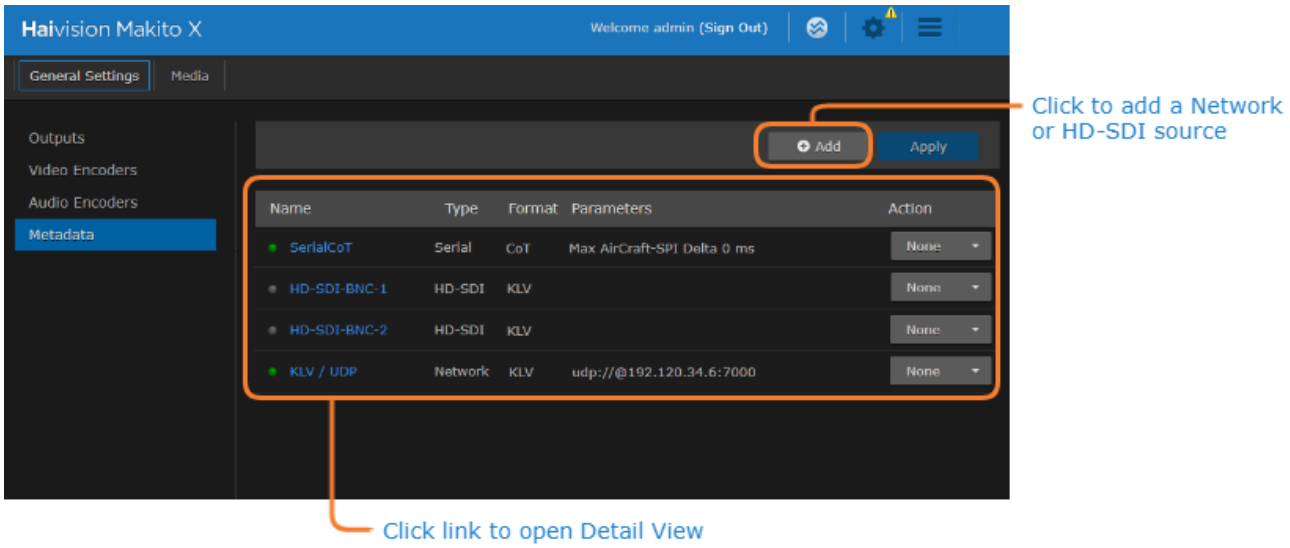
CoT/UDP and CoT/Serial metadata sources can also be retransmitted to other IP destinations for follow-up analysis by third party systems. For more information, see Configuring CoT Retransmission.

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

Metadata List View

To open the Metadata List View:

1. On the Streaming page, click **General Settings** on the navigation bar and **Metadata** on the sidebar. The Metadata List View opens, displaying the list of defined Metadata sources for the encoder. The following example shows Serial, SDI and Network metadata sources.



The Metadata List View displays the Status LED, source Name, Type, Format, and Parameters for each source. It also provides an option for you to either start or stop each source.

- To view or modify source details, click a link in the table to open the Metadata Detail View.
- To add a Network or HD-SDI source, click **Add**.
- To change the status for a source, click the drop-down list under **Action** and select either Start or Stop (as applicable). You can also delete a Network source.

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

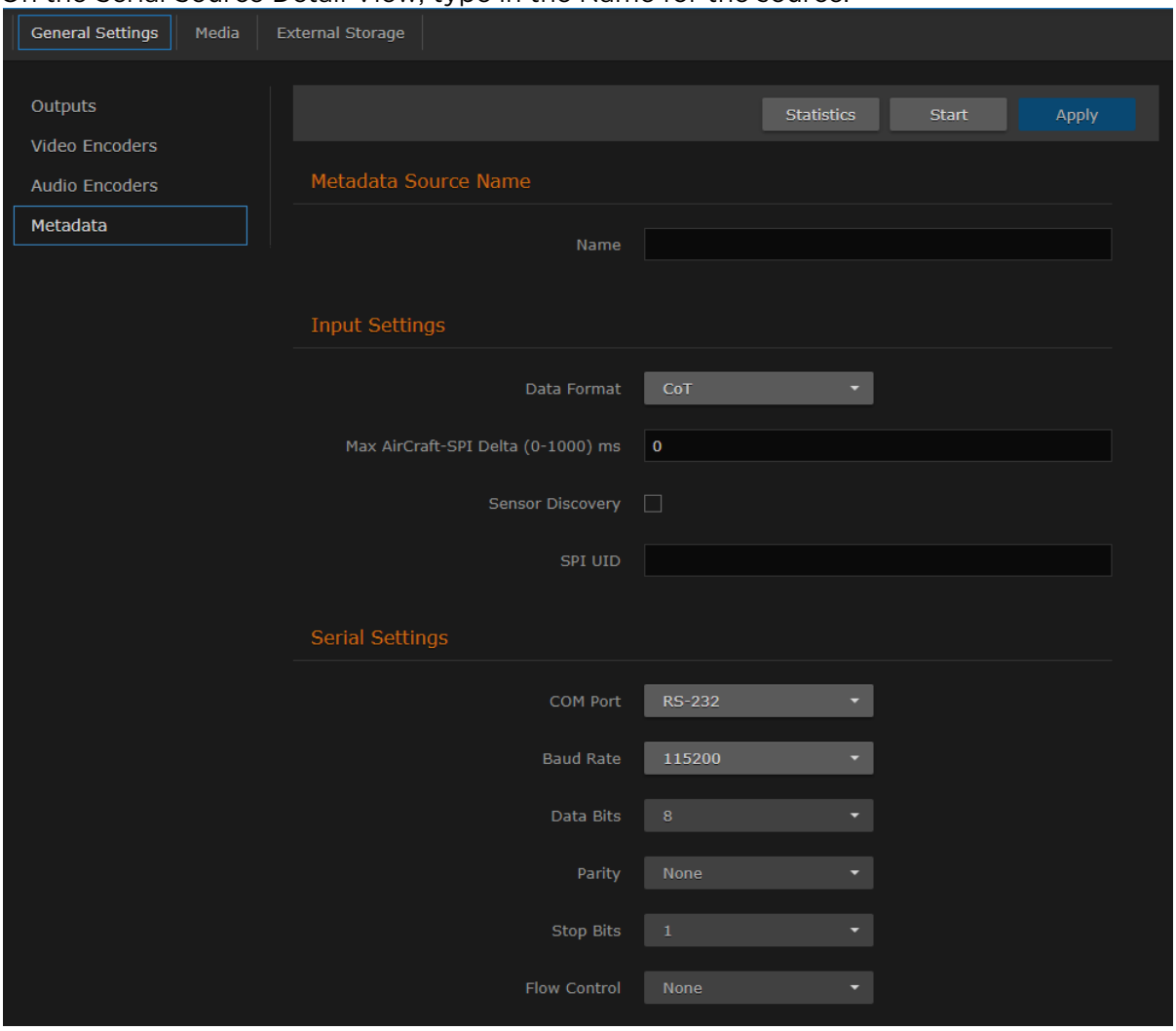
Configuring Serial Metadata Sources

> **Note**
>
> The Makito X auto-detects the hardware setup of the encoder and automatically creates the source if the serial port is connected.

You can configure the Makito X SDI to extract either KLV or CoT metadata packets from the serial port. You must specify the Data Format, and for CoT metadata, the Max AirCraftSPI Delta.

To configure the Serial metadata source:

1. From the Metadata List View, click the link for the Serial metadata source (i.e., the first line in the table).
2. On the Serial Source Detail View, type in the Name for the source.



3. If CoT has been installed, select CoT for the Data Format (under Input Settings).
4. Select or enter the remaining value(s). For details on the Metadata fields, see Metadata Settings.
5. (Optional) To set up CoT retransmission, see Configuring CoT Retransmission.

6. (Optional) To configure a mission ID or security data to replace or insert, see Configuring KLV Metadata Insertion.
7. To apply your changes and start the Metadata stream, click **Apply**.
8. To start or stop the stream, click **Start** or **Stop** (as applicable)
9. To view Metadata statistics, click **Statistics**. For details, see Metadata Statistics.
10. To return to the List View, click **Metadata** on the sidebar.

Related Topics

- Metadata Settings
- metadata (CLI Command)

Configuring HD-SDI Metadata Sources

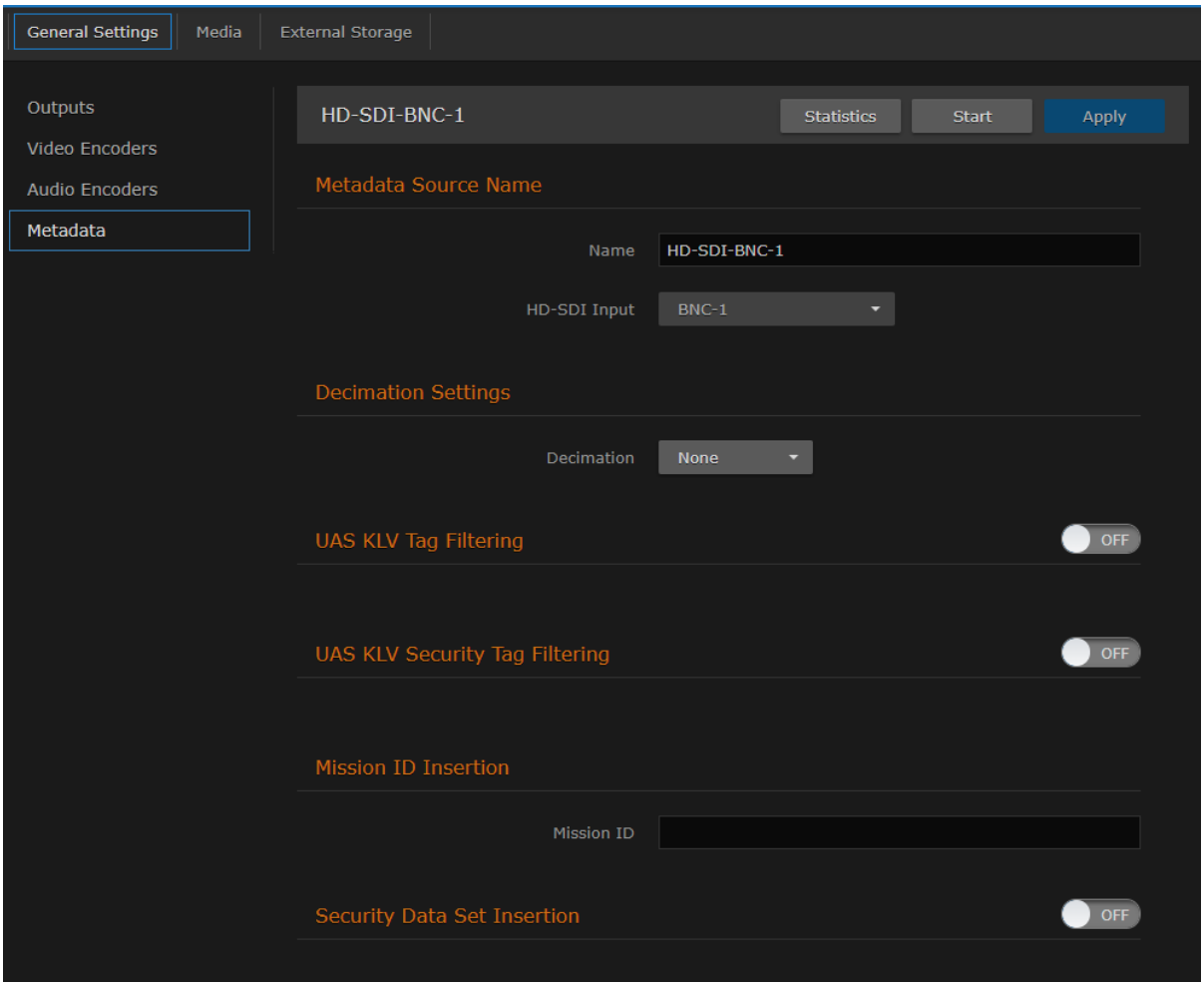
The Makito X auto-detects the hardware setup of the encoder and automatically creates the source(s) if SDI video is connected.

You can also create additional HD-SDI sources linked to the same video input which can be configured to different decimation settings (as well as security reclassification and mission ID override). For example, you can have one high bitrate stream sending out all the KLV as well as a lower bitrate stream that uses KLV decimation.

> **Note**
>
> Only progressive scan formats are supported (i.e., 1280x720p and 1920x1080p). The Makito X can capture only 1024 bytes of KLV metadata per video frame.

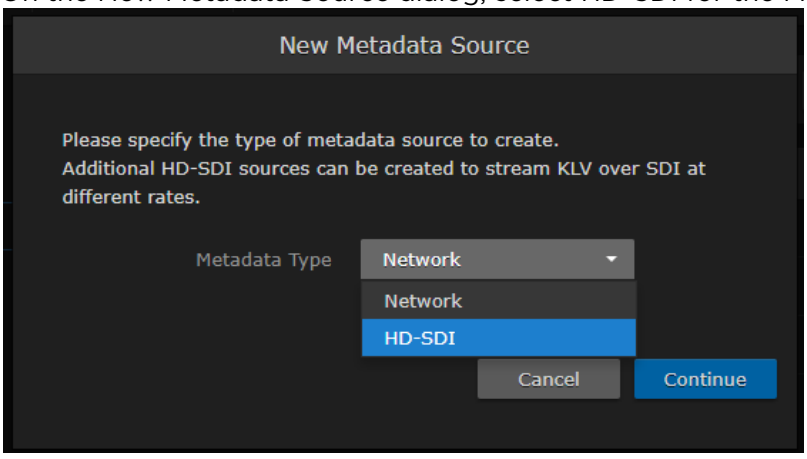
To configure HD-SDI metadata sources:

1. From the Metadata List View, click the link for the HD-SDI metadata source.
   The HD-SDI Source Detail View opens.



or

2. To create an additional HD-SDI source, from the Metadata List View, click **Add**.
3. On the New Metadata Source dialog, select HD-SDI for the Metadata Type and click **Continue**.



The Create New Metadata Source page opens.

4. Type in the Name for the source.

Decimation Settings:

5. To configure frame-decimation to reduce the bandwidth used by the metadata service, select either a decimation factor or reference encoder from the Decimation drop-down list. See “Decimation” (under "HD-SDI Sources") in Metadata Settings.
6. Select or enter the remaining value(s). For details on the Metadata fields, see Metadata Settings.

UAS KLV Tag Filtering:

7. To filter MISB 0601 metadata tags to eliminate unwanted KLV information, see Filtering UAS KLV Metadata Tags.

Mission ID/Security Data Set Insertion:

8. To configure a mission ID or security data to replace or insert, see Configuring KLV Metadata Insertion.
9. To apply your changes and start the Metadata stream, click **Apply**.
10. To start or stop the stream, click **Start** or **Stop** (as applicable).
11. To view Metadata statistics, click **Statistics**. For details, see Metadata Statistics.
12. To return to the List View, click **Metadata** on the sidebar.

Related Topics

- Metadata Settings
- metadata (CLI Command)

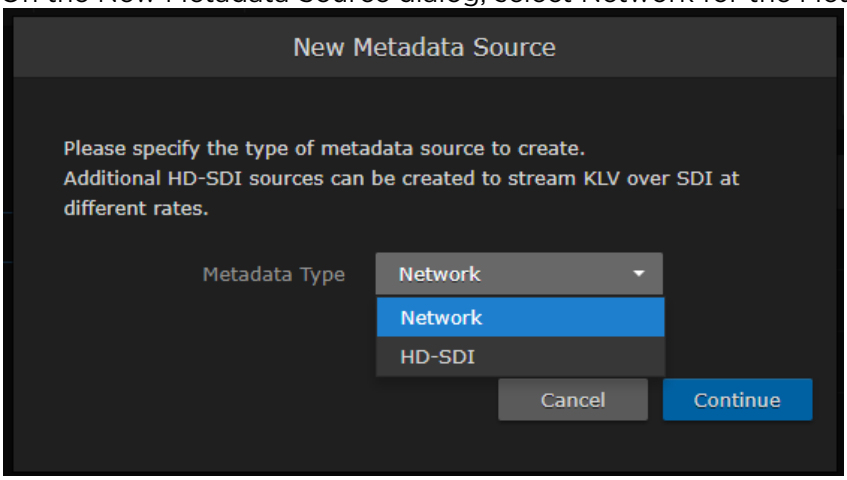
Configuring Network Metadata Sources

You can configure the Makito X to capture metadata from a user definable network port (up to eight UDP inputs). The encoder can receive either (a) KLV payload encapsulated in UDP or (b) CoT inside UDP that is converted to KLV and then streamed (see **CoT/UDP with SPI Message Filtering Based on UID**).

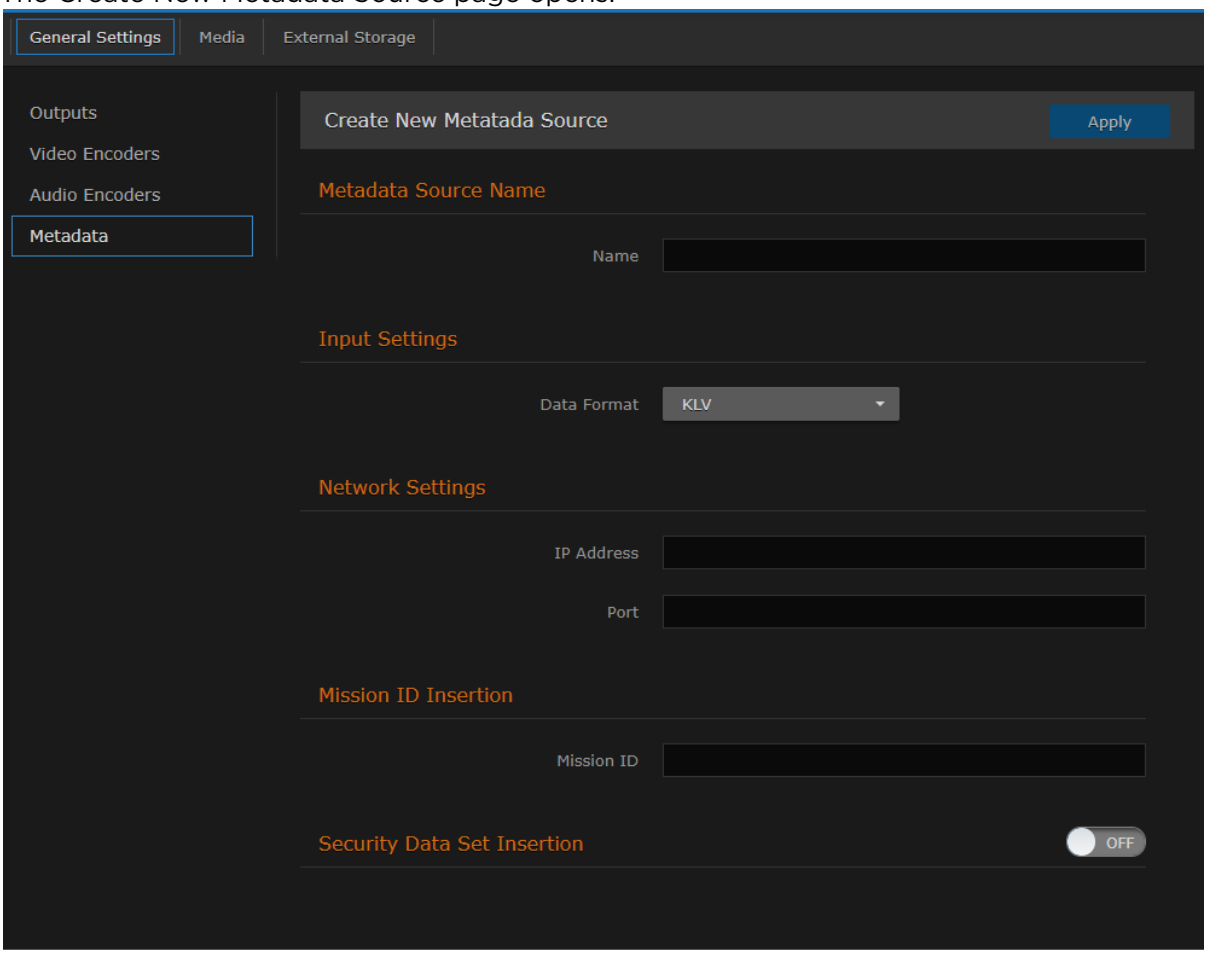
You must specify the UDP port on which the Makito X will listen for incoming metadata. However, the IP Address is only required for reception of multicast metadata, or if you only want to accept messages coming from a specific sender.

To add a network metadata source:

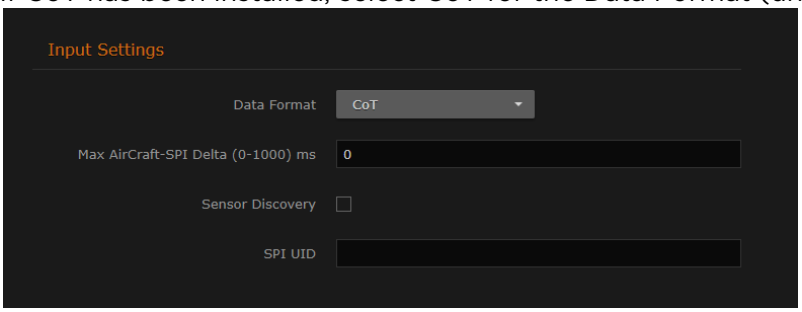
1. From the Metadata List View, click **Add**.
2. On the New Metadata Source dialog, select Network for the Metadata Type and click **Continue**.



The Create New Metadata Source page opens.



3. Type in the Name for the source.
4. If CoT has been installed, select CoT for the Data Format (under Input Settings).



5. Select or enter the remaining value(s). For details on the Metadata fields, see Metadata Settings.
6. (Optional) To set up CoT retransmission, see Configuring CoT Retransmission.
7. (Optional) To configure a mission ID or security data to replace or insert, see Configuring KLV Metadata Insertion.
8. To apply your changes and start the Metadata stream, click **Apply**.
9. To start or stop the stream, click **Start** or **Stop** (as applicable).
10. To view Metadata statistics, click **Statistics**. For details, see Metadata Statistics.
11. To return to the List View, click **Metadata** on the sidebar.

Related Topics

- Metadata Settings
- metadata (CLI Command)

CoT/UDP with SPI Message Filtering Based on UID

> **Note**
>
> CoT SPI filtering applies to CoT/UDP and CoT/Serial services.

The Makito X accepts raw CoT metadata over UDP (no SerialID wrapper) and filters the SPI (Sensor Point of Interest) messages based on a user-supplied string. If the string appears in the SPI message, then it is passed through and combined with the platform message before conversion to KLV. This allows platforms that generate multiple SPI messages to filter out unwanted incoming messages.

If the UDP port is receiving CoT, you may specify a UID filter string. If the string is present in a SPI message UID field, then the message is passed. Otherwise the message is discarded. (The format of the SPI UID filter string is a text string containing alphanumeric characters.)

In order to avoid input errors for the SPI filter string, the Makito X collects a list of the received SPI messages. You can then select a string from this list for the UID filter string.

Platform and filtered SPI messages will be converted to KLV. Only a single SPI message is supported. The KLV (converted from CoT/UDP) is multiplexed into the MPEG-2 TS stream.

The Makito X supports multiplexing of metadata sources.

Related Topics

- Metadata Settings
- metadata (CLI Command)

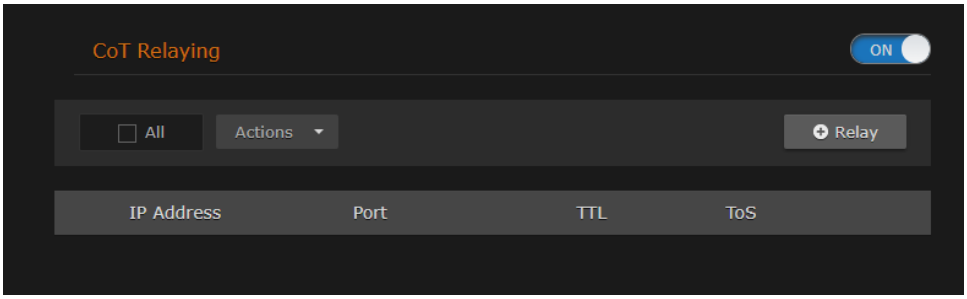
Configuring CoT Retransmission

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

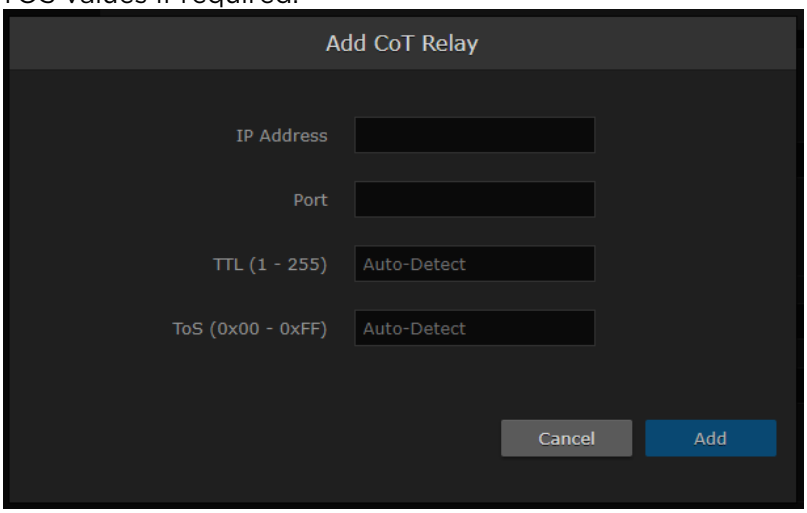
To configure CoT Retransmission:

1. From the Metadata List View, click the link for the CoT metadata source to retransmit. For details on setting up the metadata source, see Setting Up Streaming).

2. On the Metadata Detail View, if necessary, scroll down the page and toggle the CoT Relaying button to **On**.



3. To add a CoT retransmission destination, click **+Relay**.
4. On the Add CoT Relay dialog, enter the IP Address and Port for the destination. Adjust the TTL and TOS values if required.



5. Click **Add**.
   The stream is added to the list:
6. To edit or delete a CoT relay destination, select the relay from the list and select **Edit** or **Delete** from the Actions drop-down menu.

Related Topics

- Metadata Settings
- metadata (CLI Command)

Configuring KLV Metadata Insertion

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

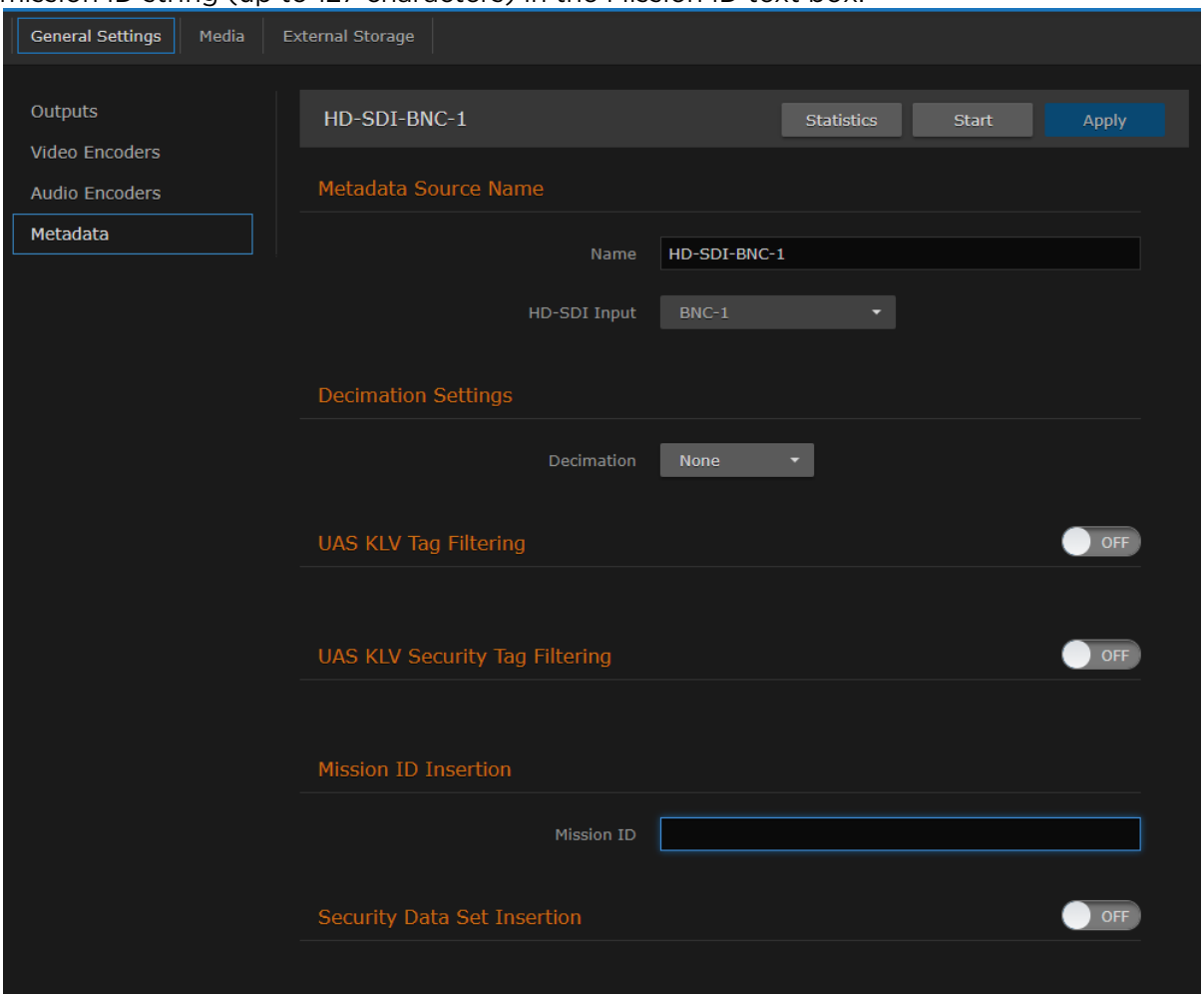
- Configure a mission ID string of up to 127 characters: When the mission ID is configured, any received UAS KLV dataset will be processed in order to modify the existing mission ID or add a mission ID element if not there with the configured value.
- Enable or disable the update/generation of the security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

In both cases, the mission ID or security data will get replaced or inserted with the ones created by the Makito X based on the configuration.

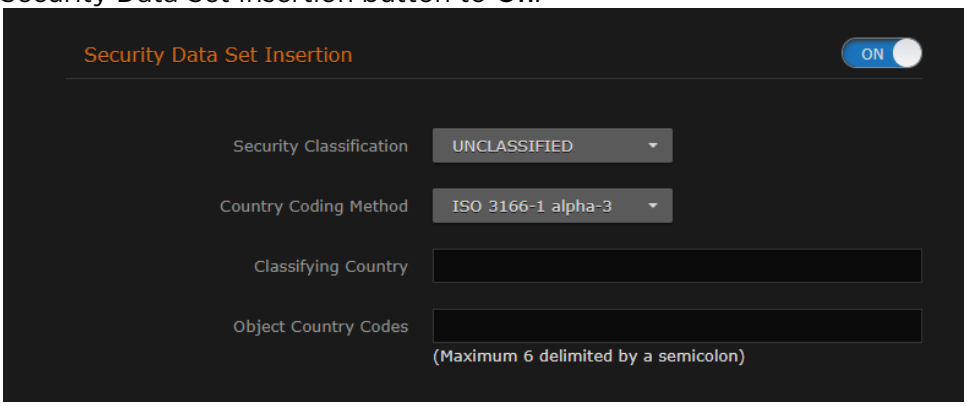
To configure static KLV objects:

1. From the Metadata List View, click the link for the metadata source to define static KLV objects. For details on setting up the metadata source, see **Setting Up Streaming**.

2. On the Metadata Detail View, if necessary, scroll down the page and (optional) type or copy in a mission ID string (up to 127 characters) in the Mission ID text box.



3. (Optional) To enable the update/generation of the security data set in UAS messages, toggle the Security Data Set Insertion button to **On**.



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

Related Topics

- Metadata Settings
- metadata (CLI Command)

Filtering UAS KLV Metadata Tags

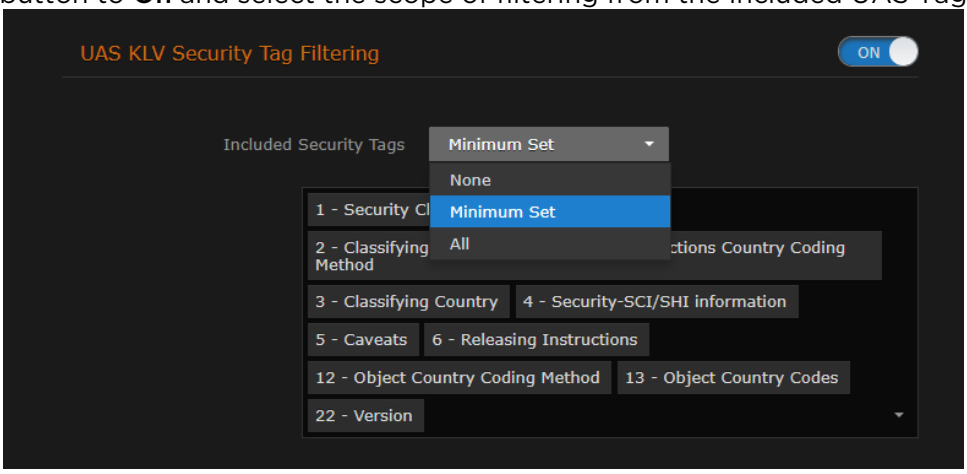
You can filter MISB 0601 metadata tags on a per tag basis, by specifying all or any subset of the MISB 0601 tags. If a tag is included, it is allowed to proceed to the metadata elementary stream (ES). Tags that are not included are filtered out of the metadata AU and not transmitted in the metadata ES.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

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

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

To filter UAS KLV metadata tags:

1. From the Metadata List View, click the link for the metadata source to filter.
2. On the Metadata Detail View, to filter MISB 0601 metadata tags, toggle the UAS KLV Tag Filtering button to **On** and select the scope of filtering from the Included UAS Tags drop-down list.



   - To fine-tune the list on a per tag basis, as you browse through the list, click **X** next to a tag number/label to exclude the tag, i.e., filter it out of the metadata. This creates a new option “Custom Set” on the Included UAS Tags drop-down list.
   - To re-include a tag that has been excluded, click the down arrow at the bottom right of the list box and select the tag from the drop-down list of excluded tags.
3. (Optional) To filter the security metadata tags defined in MISB 0102, toggle the UAS KLV Security Tag Filtering button to **On** and select the scope of filtering from the Included Security Tags drop-down list.

   Tip

   Make sure #48 is included under UAS KLV Tag Filtering.
4. Fill in the remaining fields and click **Apply**.

Related Topics

- Metadata Settings
- metadata (CLI Command)

Metadata Settings

Note

The fields depend on the hardware setup of the encoder; i.e., whether the serial port or SDI video is connected. UDP is always available.

Serial Sources | HD-SDI Sources | Network Sources

Serial Sources

Metadata Setting	Default	Description/Values
Metadata Source Name		
Name	n/a	Enter a unique name for the source.
Input Settings		
Data Format	KLV	Select the data format for the metadata: • KLV (Key Length Value) • CoT (Cursor on Target) **Note** To configure Serial input, the COM Port Mode must first be set to Metadata (see "Mode" in COM Port Settings). CoT must be specified upon purchase. For details, refer to *Cursor-on-Target Capture from the Makito X*.
Max AirCraft-SPI Delta	0 ms	(CoT input only) Specifies the maximum delta between SPI and Aircraft message timestamps for them to be considered a valid pair that can be converted to KLV. 0..1000 ms
Sensor Discovery	Disabled	(CoT input only) Check this checkbox to enable discovery of SPI UIDs that will be shown in the SPI UID field below and can then be potentially used as the SPI UID for SPI message filtering.
SPI UID	n/a	(CoT input only) Double-click the text box to display the list of the SPI messages detected by the Makito Xand select a string for the UID filter.
Serial Settings		
COM Port	RS-232	Select the type of Serial interface: • RS-232 • RS-422 (only available if the Metadata Capture option is installed).
Baud Rate	115200	Select the bitrate for the COM Port to match the protocol for connected RS-232/422 equipment. Choose from: `1200, 2400, 4800, 9600, 19200, 38400, 57600` or `115200`.
Data Bits	8	Select the number of data bits for the COM Port.
Parity	None	Select the parity for the COM Port.
Stop Bits	1	Select the number of stop bits for the COM Port.

Flow Control	None	Select the flow control for the COM Port.

CoT Relaying		
CoT Relaying	off	When set to On, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP. See **Configuring CoT Retransmission** for details of adding a relay host.
+Relay	n/a	Use to specify the IP address and UDP port for each relayed packets. You can optionally specify the TTL and ToS.
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `1..255`
ToS	0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = `0..255` (decimal) or `0x00..0xFF` (hex) **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.
KLV Insertion (See Configuring KLV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLV input only) When set to On, enables reclassification of received UAS KLV messages. `on,off`
Security Classification	unclassified	Specifies the classification of the security data set: • `unclassified, restricted, confidential, secret, topsecret`
Country Coding Method		ISO 3166-1 alpha-3
Classifying Country	n/a	The ISO 3166-1 3-letter code for the classifying country.
Object Country Codes	n/a	The ISO 3166-1 3-letter code(s) for up to six object countries separated by semicolons.

Serial Sources | HD-SDI Sources | Network Sources

HD-SDI Sources

Metadata Setting	Default	Description/Values
Metadata Source Name		
Name	n/a	Enter a unique name for the source.
HD-SDI Input	BNC-1	Select the Input port for the metadata source. • BNC-1 • BNC-2

Decimation Settings		
Decimation	None	(Optional) For KLV over SDI metadata input, the ingested KLV messages can be frame-decimated to reduce the bandwidth used by the metadata service. Select either the decimation factor or a reference encoder to match its video frame rate. • None • By Factor: `1/2..1/60` **Note** `1/2` means divide the amount by half, etc. • With Encoder: Select a video encoder from the drop-down list and the metadata AU rate will match the video encoder frame rate.
KLV Tag Filtering (See Filtering UAS KLV Metadata Tags)		
UAS KLV Tag Filtering	off	Specifies a list of tag numbers/labels from the UAS Datalink Local Set that are allowed to be streamed. Tags not included in this list will be discarded. Select either: • None • Minimum Set: the set of metadata objects as define in MISB 0902. • All: the set of metadata objects as define in MISB 0601.
UAS KLV Security Tag Filtering	off	Specifies a list of tag numbers/labels from the Security Local Data set inside the UAS that are allowed to be streamed. Tags not included will be discarded. Select either: • None • Minimum Set: the set of metadata objects as define in MISB 0902. • All: the set of metadata objects as define in MISB 0102. **Tip** #48 must be included under UAS KLV Tag Filtering.
KLV Insertion (See Configuring KLV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLV input only) When set to On, enables reclassification of received UAS KLV messages. `on,off`
Security Classification	unclassified	Specifies the classification of the security data set: • `unclassified, restricted, confidential, secret, topsecret`
Country Coding Method		ISO 3166-1 alpha-3
Classifying Country	n/a	The ISO 3166-1 3-letter code for the classifying country.
Object Country Codes	n/a	The ISO 3166-1 3-letter code(s) for up to six object countries separated by semicolons.

Note

KLV Metadata over SDI is only used with HD-SDI, and no Closed Captioning services are presently available on HD-SDI Makito X.

Serial Sources HD-SDI Sources Network Sources

Network Sources

Metadata Setting	Default	Description/Values
Metadata Source Name		
Name	n/a	Enter a unique name for the source.
Input Settings		
Data Format	KLV	Select the data format for the metadata. • KLV (Key Length Value) • CoT (Cursor on Target) CoT must be specified upon purchase. For details, refer to the MakitoX CoT Addendum.
Max AirCraft-SPI Delta	0 ms	(CoT only) Specifies the maximum delta between SPI and Aircraft message timestamps for them to be considered a valid pair that can be converted to KLV. 0..1000 ms NOTE: Only available if CoT has been installed.
Sensor Discovery	Disabled	(CoT input only) Check this checkbox to enable discovery of SPI UIDs that will be shown in the SPI UID field below and can then be potentially used as the SPI UID for SPI message filtering.
SPI UID	n/a	(CoT input only) Double-click the text box to display the list of the SPI messages detected by the Makito Xand select a string for the UID filter.
Network Settings		
IP Address	n/a	(Optional) The address is only required for reception of multicast metadata. In this case, you need to provide the multicast IP address to which the data is being sent. You can also specify the address if you only want to accept KLV messages coming from a specific sender.
Port	n/a	(Required) Specifies the local UDP port on the Makito X that is receiving the packets.
CoT Relaying (See Configuring CoT Retransmission)		
CoT Relaying	off	When set to On, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP. See Configuring CoT Retransmission for details of adding a relay host.
+Relay	n/a	Use to specify the IP address and UDP port for each relayed packets. You can optionally specify the TTL and ToS.
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `1..255`

ToS	0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = `0..255` (decimal) or `0x00..0xFF` (hex) **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.

KLV Insertion (See Configuring KLV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLV input only) When set to On, enables reclassification of received UAS KLV messages. `on,off`
Security Classification	unclassified	Specifies the classification of the security data set: • `unclassified, restricted, confidential, secret, topsecret`
Country Coding Method		ISO 3166-1 alpha-3
Classifying Country	n/a	The ISO 3166-1 3-letter code for the classifying country.
Object Country Codes	n/a	The ISO 3166-1 3-letter code(s) for up to six object countries separated by semicolons.

Metadata Statistics

The following table lists the Metadata statistics:

Metadata Statistic	Description/Values
State	The current operating status of the stream, either: • WORKING • STOPPED
Rx Bytes	Number of received bytes.
Rx OK Messages	Number of successfully received messages.
Rx Corrupt Messages	Number of corrupt or failed messages.
Source Address	(UDP input only) The IP address of the Network source.
Rx SPI Messages	(**CoT** input only) Number of received SPI (Sensor Point of Interest) messages.
Rx AirCraft Messages	(**CoT** input only) Number of received Aircraft messages.
Generated KLV Messages	(**CoT** input only) Number of generated KLV messages.
Generated KLV Bytes	(**CoT** input only) Number of generated KLV bytes.
RX Filtered SPI Messages	(**CoT** input only) Number of filtered SPI Messages.
Reset	Click to reset the Metadata statistics.

Configuring Streaming Outputs

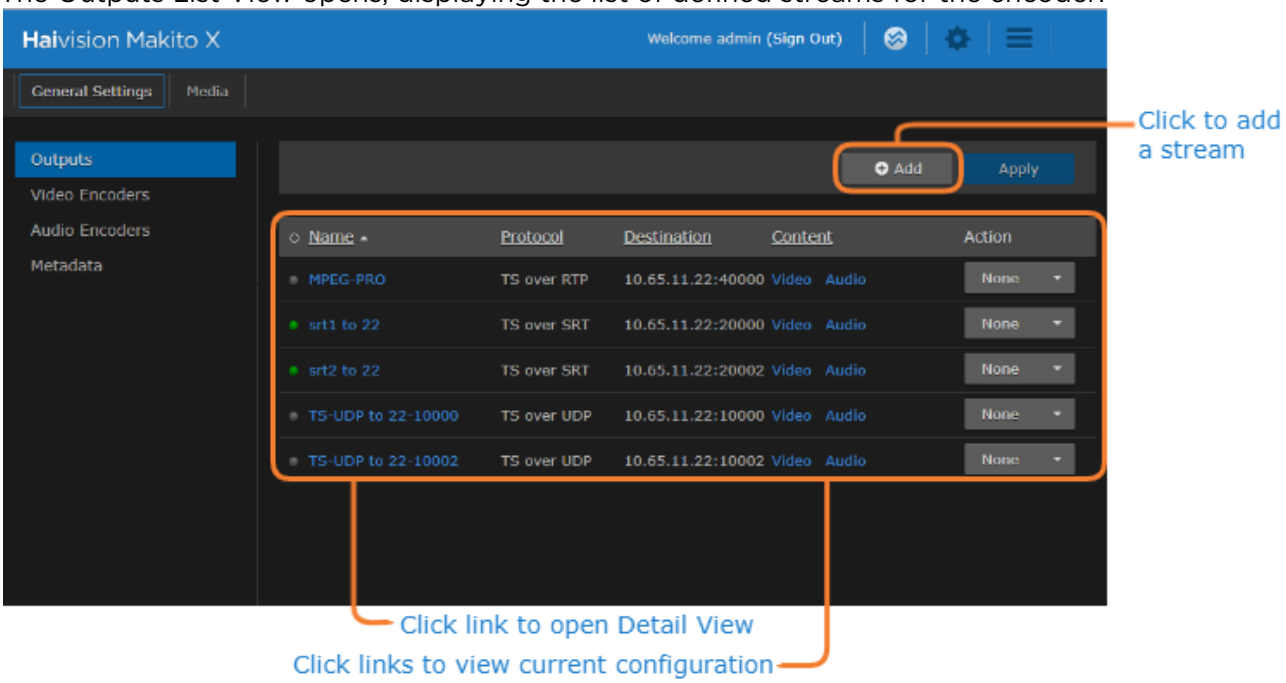
Important

Recording is *only* available on the Makito X with Storage dual-height model (either fixed or removable SSD). For information on recording, see **Configuring Recording Outputs**. Recording is *not* available on HEVC-capable appliances.

Outputs List View

To open the Outputs List View:

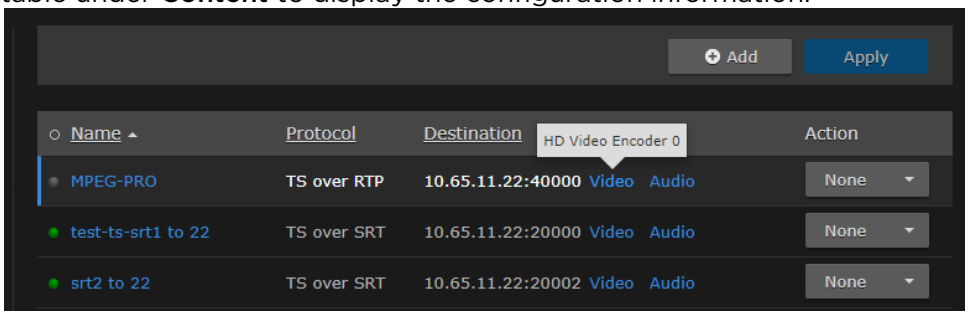
1. On the Streaming page, click **General Settings** on the navigation bar and **Outputs** on the sidebar. The Outputs List View opens, displaying the list of defined streams for the encoder.



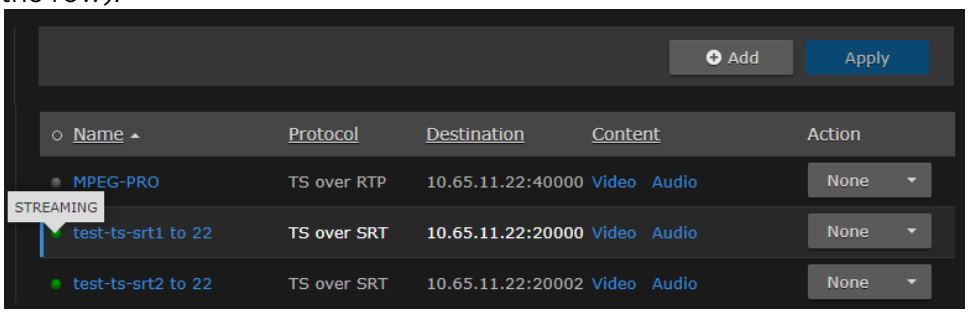
The Outputs List View displays the status LED, Stream Name, Protocol, Destination (IP Address and Port), and selected Content (Video/Audio Encoders and Metadata source) for each stream. It also provides an option for you to either start, stop, pause, or delete the stream.

- To create an output stream or recording session, click **Add**.
- To view details or modify the settings for a stream or recording, click a link in the table under **Name** to open the Outputs Detail View.

- To view the video or audio encoder or metadata source for a stream, hover over a link in the table under **Content** to display the configuration information.



- To view the status of a stream or recording, hover over the status LED or **REC** link (to the left of the row).



- To change the status for an existing stream, click the drop-down list under **Action** and select either Pause, Resume, Start, Stop, or Delete (as applicable).
- To sort the streams by Name, Protocol, Destination IP, or Content, you can click on a column header to sort by that column. The first click sorts by ascending order, indicated by an up arrow next to the column header. Clicking again sorts by descending order, indicated by a down arrow next to the column header.

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

Setting Up Streaming

From the Outputs pages, you can create multiple output streams using the defined video encoders, audio encoders, and metadata (if applicable). Each output stream is configured independently. For details see:

- Configuring Video Encoders
- Configuring Audio Encoders
- Configuring Metadata Capture

Note

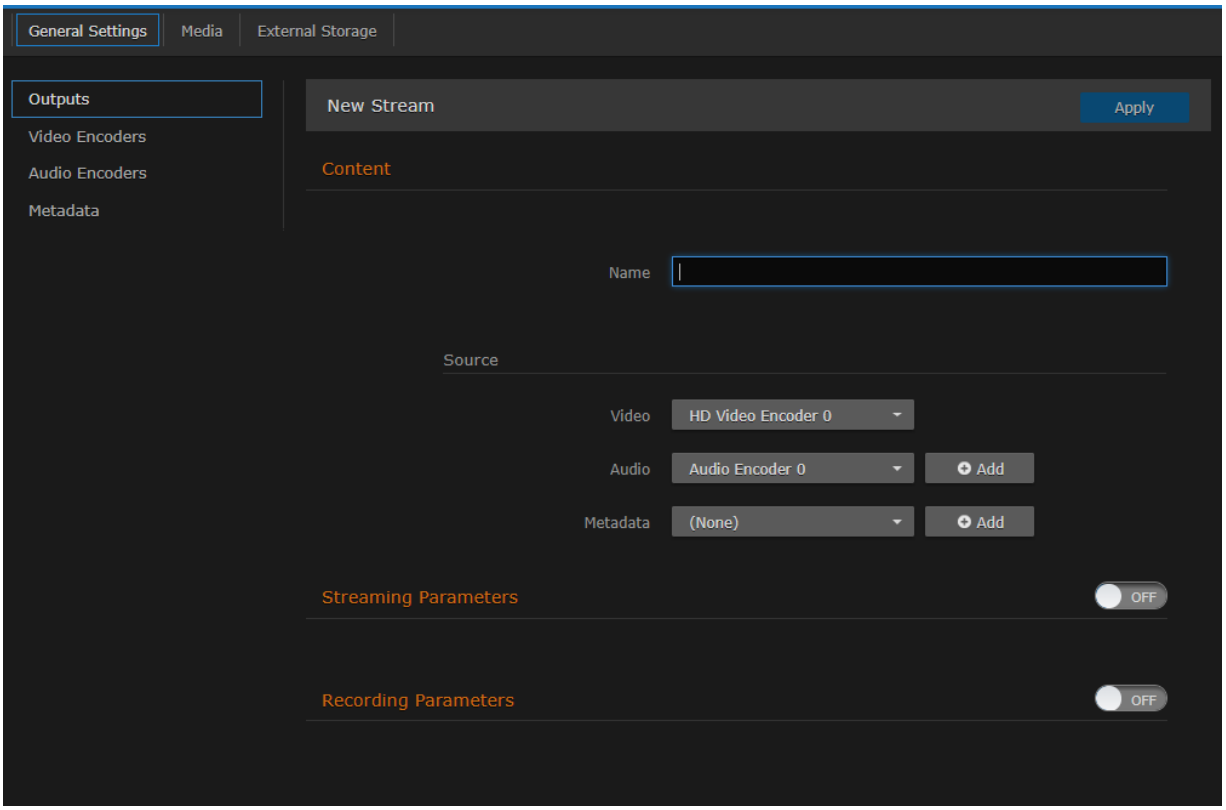
There is a limit of 16 streams that are exact duplicates. This refers to streams that have the exact same content sources (i.e., the same encoders and/or metadata sources).

To configure Output Steaming parameters:

1. From the Outputs List View, click a link in the table for an existing stream, or click **Add** to add a stream.
   The Outputs Detail View opens.

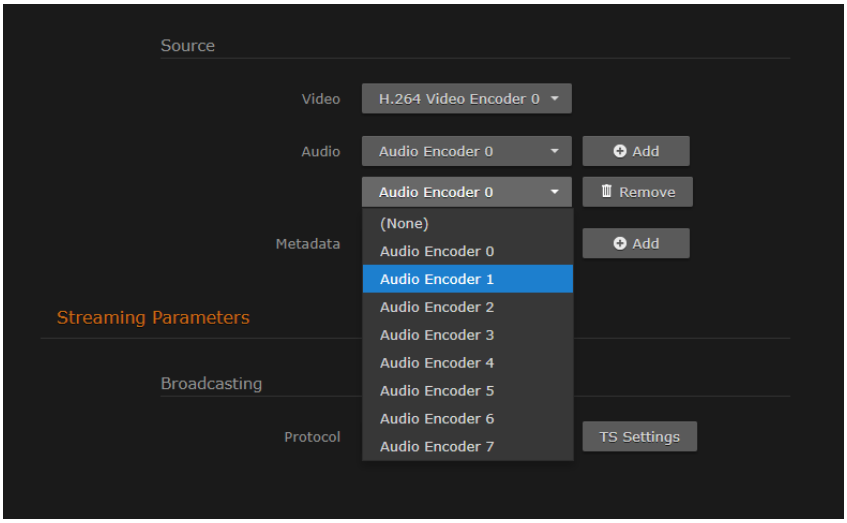
   Tip

   On the Makito X with Storage, you will see the Streaming and Recording Parameters toggle buttons.



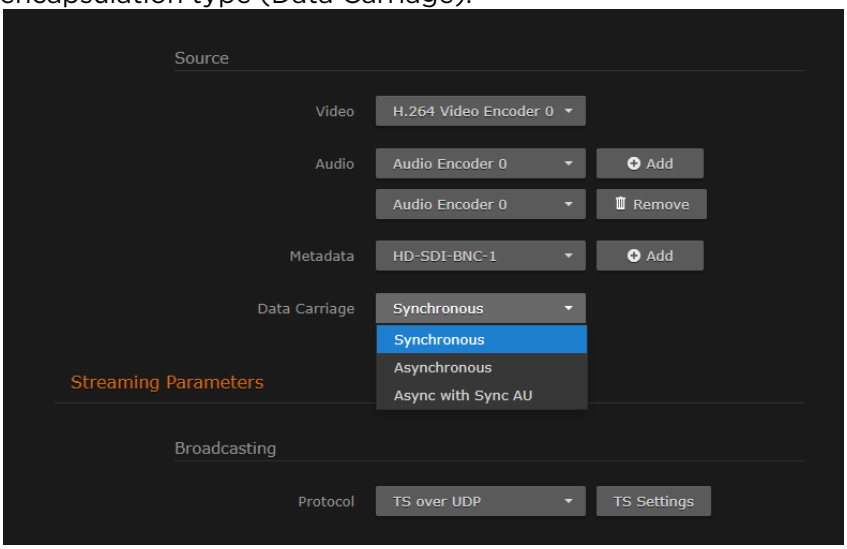
2. Enter the stream name and select the sources (Video, Audio, and Metadata, if applicable). See Streaming Output Settings.

3. To configure multi-track audio, click **Add** next to the Audio field and select the next Audio Encoder to add to the stream.



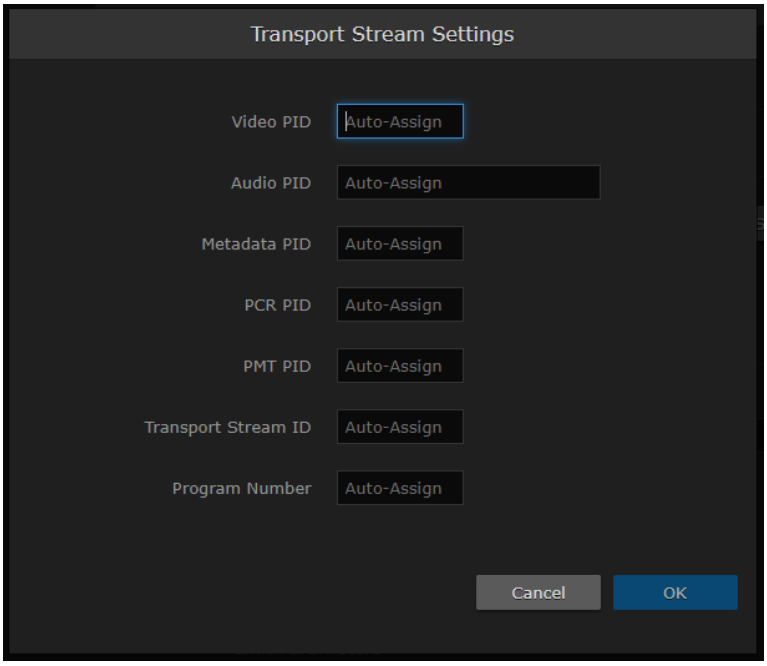
> **Important**
>
> Audio sources should always be associated with the same video interface for the dual channel SDI encoder. Selecting Analog or SDI audio sources that do not originate from the same video source is not recommended as audio artifacts will result at the decoder. For example, selecting video from BNC1 and audio from BNC2 will cause audio artifacts. Analog audio must be associated with a single BNC input.

4. To add metadata to the stream, select the Metadata source, and (optionally) select the encapsulation type (Data Carriage).



5. To stream metadata from multiple sources, click **Add** next to the Metadata field and select the next metadata source to add to the stream.
6. (Makito X with Storage only) To set up streaming, toggle the Streaming Parameters button to **On**. This step is not required if your encoder is not a Storage platform because streaming is already enabled.
7. Under Broadcasting, select the Protocol.

8. To configure the Transport Stream settings (for TS over UDP, RTP, or SRT), click TS Settings and enter the values.

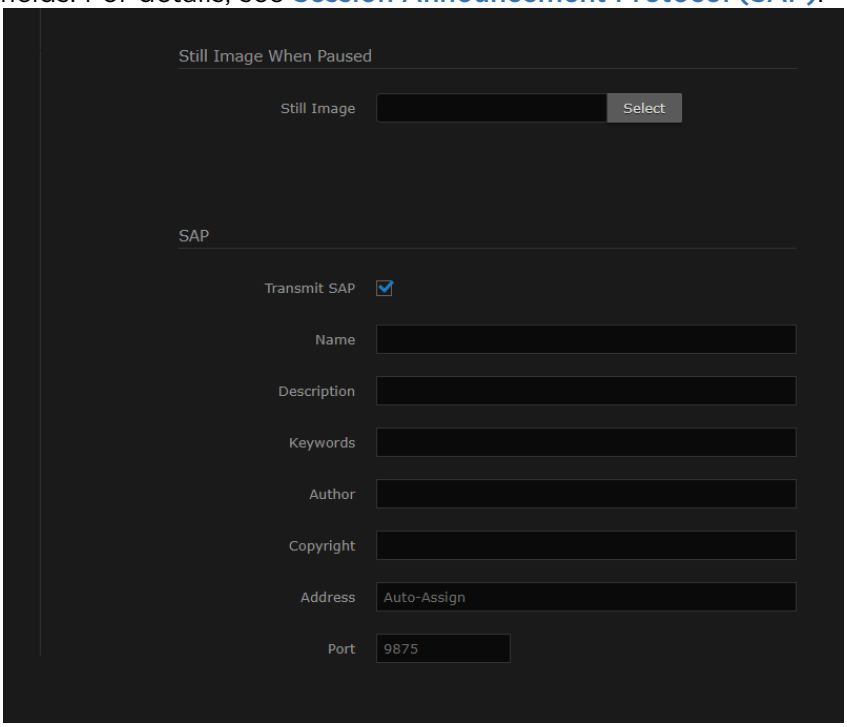


9. **Important**

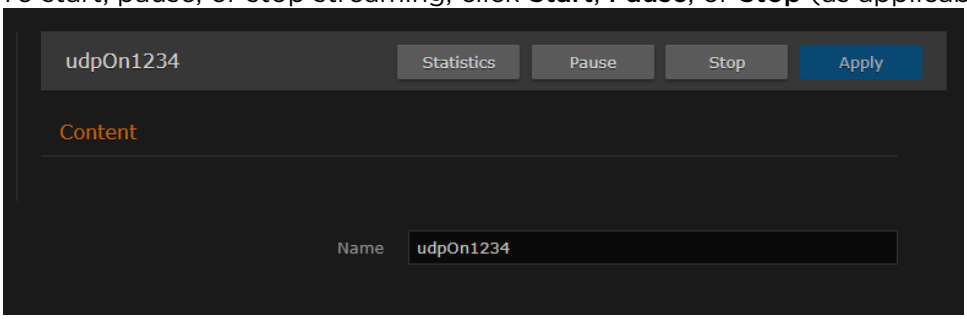
   The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network.

10. To configure a stream using the SRT (Secure Reliable Transport) streaming protocol, select TS over SRT for the Protocol and then complete the additional fields under Connection and SRT Settings. See **Configuring Secure Reliable Transport (SRT)**.
11. To configure a static image to display when the stream is paused, select a Still Image file. (Image files must have been previously uploaded for the encoder. To upload image files, see **Configuring Still Image Streaming**.)

12. To configure SAP network announcements, check the “Transmit SAP” checkbox and fill in the SAP fields. For details, see Session Announcement Protocol (SAP).



13. (Makito X with Storage only) To set up a recording session, toggle the Recording Parameters button to On. See Configuring Recording Outputs.
14. If you only want to create a streaming session, click **Apply** now to apply your changes and start streaming.
15. To start, pause, or stop streaming, click **Start**, **Pause**, or **Stop** (as applicable).



16. To view streaming statistics, click **Statistics**. For details, see Streaming Output Statistics.
17. To return to List View, click **Outputs** on the sidebar.

Related Topics

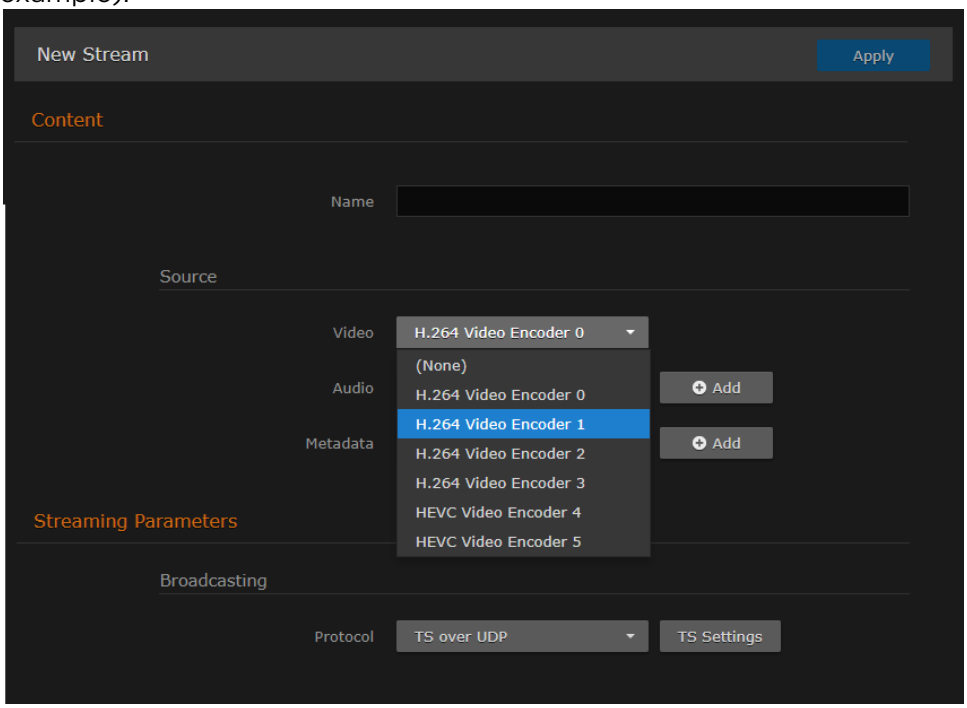
- Streaming Output Settings
- stream (CLI Command)

Setting Up a Second Stream or Recording

To create a second stream (or recording):

1. On the Outputs List View, click **Add** again.

2. Follow the steps in Setting Up Streaming to configure the second session. Except for the Video Source, select a different Video Encoder. For example, if you selected Video Encoder 0 for the first stream, now select Video Encoder 2 (to capture input from SDI Input 2, as shown in the following example).



3. Also, under Streaming Parameters Destination, use a different Port number, for example, `2400`.
4. Follow Steps #1 through #3 from Setting Up Recording to create a recording session with the second session.
5. Click **Apply** to start streaming (as well as recording, if configured).

Session Announcement Protocol (SAP)

You can also enable or disable SAP network announcements. Session Announcement Protocol (SAP) is a protocol for advertising multicast or unicast session information. SAP periodically multicasts session description information on an industry standard multicast address and port. When received by remote participants, these announcements can be used to generate playlists and facilitate the viewing of streams by eliminating the need for user configuration. For example, they may be used to automatically create program listings to allow streams to easily be located, selected and viewed.

You can also specify the address and port to transmit SAP announcements on a stream-by-stream basis. This is useful if you do not want to multicast SAP announcements on the standard IP addresses and ports (as defined in RFC 2974).

Related Topics

- "SAP" under "Streaming Parameters" in Streaming Output Settings
- session (CLI command)

Selective Video Mute

Pausing and then resuming a stream allows you to selectively and temporarily "mute" the video. For example, if you are streaming the same content multiple times to different audiences, you can choose to

mute one or some of the streams (i.e., by pausing them). If a still image has been configured, the encoder will send this image to replace the encoded video stream when the stream is paused. (See **Configuring Still Image Streaming**.)

When the video is "unmuted" (i.e., resumed), the decoder will immediately display the video stream again. In effect, this provides a "privacy mode" and avoids delays that may occur when starting and stopping a stream and waiting for a decoder to start decoding again.

In order to support inter-working with the Furnace, the encoder inserts coded silence when a stream is paused to ensure that (for example, if there is a channel change), the still image will be displayed on Stingray set-top boxes and InStream players. (Note that these players need audio before they play any content.) No user selections are required to enable this feature.

Related Topics

- **Configuring Still Image Streaming**

Bandwidth Overhead for CBR Streams with Metadata

In CBR streams with Traffic Shaping enabled, metadata may cause the stream to exceed the bandwidth overhead (video bitrate + bandwidth overhead percentage). Therefore, when configuring the bandwidth overhead percentage, you need to take into account how much metadata is being generated.

Metadata is not part of the minimum bandwidth calculation used for CBR streams (because it is application dependent). The bandwidth for it is presumed to fit within the bandwidth overhead which is specified at stream creation. However, as the video bitrate drops, the overhead needed to accommodate the worst case bandwidth usage of the metadata must increase.

For example: `bandwidth overhead = ( metadata_bitrate / ( video_bitrate + audio_bitrate ) ) * 100`

Minimum bandwidth overhead should be no less than 5. For example:

```
metadata_bitrate = 500 Kbps, video_bitrate = 1000 Kbps, audio_bitrate = 128 Kbps
```

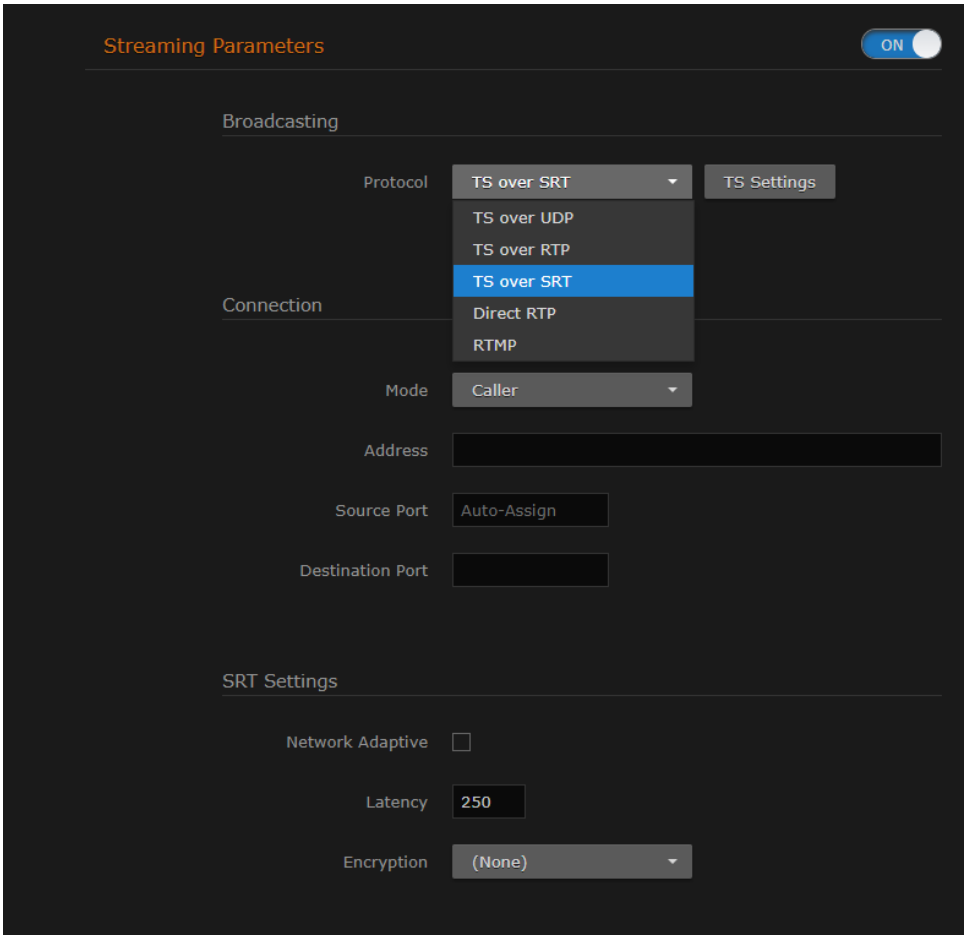
```
bandwidth overhead = ( 500 / ( 1000 + 128 ) ) * 100 = 44
```

Configuring Secure Reliable Transport (SRT)

Haivision's Secure Reliable Transport (SRT) streaming protocol is designed to provide reliable and secure end-to-end transport between two SRT-enabled devices (such as Makito X Series encoders and decoders) over a link which traverses the public Internet. For more information, see **Secure Reliable Transport (SRT)**.

To create an SRT connection:

1. Make sure the encoder and decoder are accessible from the public Internet by appropriate configuration of any firewalls.
2. Follow the steps in **Setting Up Streaming** to set up the SRT stream and start the stream connection.



3. Once you establish the SRT stream, check the statistics and make adjustments to finetune the stream. On the Output Streams page, click the **Statistics** button to see how the SRT stream is performing.
4. Monitor the link statistics to see if the link is over-subscribed (and adjust the video encoder bitrate if it is).
   For example, use the Max Bandwidth and (Buffering) Latency values to set the encoder bitrates appropriately.

Related Topics

- For the SRT-specific parameters, see **SRT Streaming Settings**
- For SRT-specific statistics and graphical display, see **Streaming Output Statistics**

CDN Interoperability (RTMP)

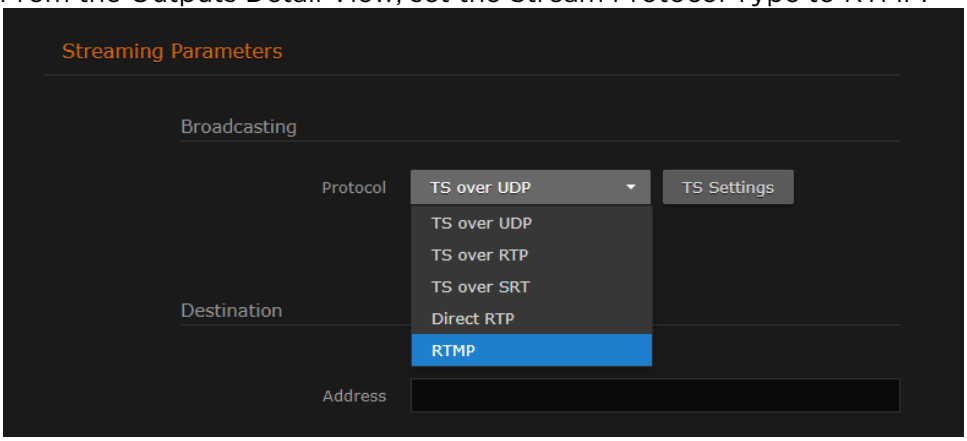
The Makito X can stream directly to an Adobe Media Server (AMS) or Content Delivery Network (CDN) using the Real Time Messaging Protocol (RTMP).

- The supported RTMP servers are AMS and Wowza.
- The supported Transcoders are Wowza and Haivision's KB Transcoder.
- The supported CDNs are Akamai and Limelight.

This section provides the steps to set up an RTMP stream.

To stream to an Adobe Media Server or other CDN:

1. Follow the steps in **Setting Up Streaming** to add a stream and select the sources.
2. From the Outputs Detail View, set the Stream Protocol Type to RTMP.



3. For the Destination Address, type in the URL for the application endpoint of the AMS or CDN server.
4. **Tip**

   By default, RTMP streaming media servers listen for RTMP requests on port 1935, You should only specify the port in the URL for a stream when the media server is not using this default standard port.
5. Type in the username and password for the CDN server. See "Username" and "Password" fields in **Streaming Output Settings**.
6. Click **Apply** to start the stream.
7. To return to List View, click **Outputs** on the sidebar.

Note

You can create and stream multiple RTMP streams with identical server destination and application name URLs in order to stream to both a primary and backup RTMP entry point.

Tip

When creating a stream to an Akamai HD2 CDN, to avoid dropped frames by the HD2 player, make sure that sufficient bandwidth exists between the Makito X and the HD2 node.

Related Topics

- "RTMP" on Streaming Output Settings

Publishing an RTMP Stream to YouTube

Following are the steps to publish an RTMP stream from the Makito X to YouTube:

1. Log in to YouTube, and go to "My Channel" and then to "Video Manager".
2. Select "Live Events" in the navigation pane on the left and click the "New live event" button on the top-right.
3. Enter the event name, start date/time, and set Type to Custom. Click "Create Event".
4. On the "Ingestion Settings / Main Camera" page, choose "Custom ingestion". Create a stream, select "Other encoders" in the encoder list, and note the stream name and the server URL which will appear below.
   - When you click on "Custom ingestion", you must choose the appropriate resolution (e.g., MXE (720p)). If you do not give the resolution you will transmit, YouTube cannot start to display your stream.
   - When you select "Other encoders", YouTube will give you a Stream Name (e.g., makrtmp.ee8a-v8qv-cury-70mg). This name correspond to the Makito X Publish Name field.
5. Start the RTMP stream on the Makito X.
6. On YouTube, go to the "Live Control Room" page, and as soon as YouTube starts to receive your stream (i.e., the stream status appears as GOOD), you can go into preview mode (press the **Preview** button).
7. Shortly before the event start time, you should be able to press "Start Streaming" to actually start your event.

Important

Everything you stream to YouTube becomes public.

Streaming Output Settings

The following table lists the Streaming Output controls and settings:

Content | Streaming Parameters | SAP | RTMP | General

Content

Streaming Setting	Default	Description/Values
Name	n/a	(Optional) Enter a unique name for the stream.
Source		
Video H.264	HD Video Encoder 0	Select the Video Encoder to assign to the stream: • None (no content source selected) • HD Video Encoder 0 • HD Video Encoder 1 • HD Video Encoder 2 • HD Video Encoder 3
HEVC	H.264 Video Encoder 0	Select the Video Encoder to assign to the stream: • None (no content source selected) • H.264 Video Encoder 0 • H.264 Video Encoder 1 • H.264 Video Encoder 2 • H.264 Video Encoder 3 • HEVC Video Encoder 4 • HEVC Video Encoder 5
Audio	Audio Encoder 0	Select the Audio Encoder to assign to the stream. • None (no content source selected) • Audio Encoder 0. . 3 • Audio Encoder 4. . 7 (SDI only) **Note** To configure multi-track audio, click **Add** next to the Audio field and select the next Audio Encoder to add to the stream.

Metadata	None	(Only available if KLV or CoT has been installed) To enable metadata, select one of the defined inputs. • (None) • Select from list of defined metadata sources, e.g., Serial:CoT or Serial:KLV (if connected), HD-SDI-BNC-1, or HD-SDI-BNC-2 **Note** To stream metadata from multiple sources, click **Add** next to the Metadata field and select the next metadata source to add to the stream. For more information, see **Configuring Metadata Capture**.
Data Carriage	Asynchronous	Selects the encapsulation type to use for the KLV metadata source, either: • Synchronous: synchronous metadata AU (ISO/IEC 13818-1) • Asynchronous: asynchronous private data (SMPTE RP 217) • Asynchronous with Sync AU: asynchronous private data carrying sync metadata AU

Content | Streaming Parameters | SAP | RTMP | General

Streaming Parameters

Streaming Setting	Default	Description/Values
Broadcasting		
Protocol	TS over UDP	Select the Protocol Type for the encoded stream. • TS over UDP: MPEG2 transport stream over UDP (no RTP header) • TS over RTP: MPEG2 transport stream over RTP • TS over SRT: Secure Reliable Transport. See Configuring Secure Reliable Transport (SRT). • Direct-RTP: RFC3984 (H.264 only) • RTMP: Streams to a Flash Media Server or Content Delivery Network. See CDN Interoperability (RTMP).
Transport Stream Settings		
Video PID	33	(Optional) Video Packet Identifier 16..8190
Audio PID	36	(Optional) Audio Packet Identifier 16..8190
Metadata PID	40	(Optional) Data (metadata) Packet Identifier. 16..8190
PCR PID	33	(Optional) (Program Clock Reference) Packet Identifier. Timestamp in the TS from which the decoder timing is derived. 16..8190
PMT PID	32	(Optional) (Program Map Table) Packet Identifier. 16..8190
Transport Stream ID	0	(Optional) Transport Stream ID. Identifies the transport stream in the Program Association table (PAT) of the TS stream. 0..65535
Program Number	1	(Optional) Program Identifier used in the Program Map Table (PMT) of the TS stream. 0..65535
Destination		
Address	n/a	Enter the destination IP address in dotted-decimal format. **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`).

(RTMP only)		**Note** For more information, see CDN Interoperability (RTMP).
Port(s)	n/a	**Note** Direct-RTP streams require different UDP ports for video and audio. You must specify the second port number.

Link Parameters		
Average Bandwidth	n/a	(Read-only) The average transmit bandwidth for the unit in kbps.
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
VF Encryption	Off	(Read-only) Indicates whether Advanced Encryption Standard (AES) encryption has been enabled through the Furnace Server interface (VF Channel Editor).
MTU	1496	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing RTP data stream. 228..1500
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `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) **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.
Pro-MPEG FEC Settings (TS over RTP only)		
Level	B	The level of Forward Error Correction (FEC) protection: • A (Column only): uses the column FEC stream. • B (Row and Column): uses both column and row FEC streams.

Columns	10	The number of columns in the FEC matrix.
Rows	5	The number of rows in the FEC matrix.
Block Aligned	Enabled	Specifies the type of FEC matrix scheme. • Check this checkbox to align the FEC blocks in the matrix structure (i.e., sequential columns within a group start on the same row). • If left unchecked, the blocks are a staggered series of FEC packets (i.e., each column starts on the row below the row on which the previous column started). **Note** The enabled Block Aligned setting corresponds to the aligned FEC discussed in Annex C of SMPTE 2022-1. The disabled Block Aligned setting corresponds to the non-aligned FEC discussed in Annex B of SMPTE 2022-1.
Traffic Shaping		
Traffic Shaping	Disabled	**Note** For some limited networks such as satellites or some dedicated network pipes, it may be necessary to enable Traffic Shaping to smooth the traffic and respect the absolute upper limit configured.
Idle Cells	Disabled	(Traffic Shaping must be enabled) When enabled, Idle TS cells will be inserted into a TS stream when necessary.
Delayed Audio	Disabled	(Traffic Shaping must be enabled) When enabled, delays the transmission of audio information to prevent MPEG-2 TS HRD main buffer overflows.
Bandwidth Overhead	15%	(Traffic Shaping must be enabled) Specifies the percentage of network bandwidth beyond the average rate that the encoder is allowed to use if needed. **Note** To configure the Bandwidth Overhead for CBR streams with metadata, see Bandwidth Overhead for CBR Streams with Metadata.
Still Image		
Still Image When Paused	n/a	Click Select to select an image from the pre-defined list. See Configuring Still Image Streaming.

Content Streaming Parameters SAP RTMP General

Session Announcement Protocol (SAP)

Streaming Setting	Default	Description/Values
Transmit SAP	Off	Check this checkbox to enable Session Announcement Protocol (SAP) network announcements.
Name	n/a	If SAP is enabled, enter a unique name for the Session.
Description	n/a	(Optional) Enter an expanded description of the Session.
Keywords	n/a	(Optional) Enter one or more keywords to associate with the Session. Keywords can serve as filters.
Author	n/a	(Optional) Enter the name of the program's author.
Copyright	n/a	(Optional) Enter the copyright information for the session.
Address	Auto-Assign	(Optional) Enter a different SAP multicast advertising IP address to override the default/selected values. The "Auto-Assign" default value means that when the stream is created and SAP is enabled, the Makito X will automatically pick the proper default advertisement address based on the stream's destination address and family (IPv4 or IPv6). After after the new stream is is started, it will display the actual selected IP address.
Port	n/a	Enter the SAP advertising UDP port. Default=9875.

Content Streaming Parameters SAP RTMP General

RTMP

Streaming Setting	Default	Description/Values
Publish Name	n/a	(RTMP only) Enter a publish name for the stream (511 characters maximum). **Note** Note that stream names must be unique, while the publish name can be reused if desired across multiple RTMP streams. See CDN Interoperability (RTMP).
Username	n/a	Enter the CDN login username.
Password	n/a	Enter the CDN login password.

Content Streaming Parameters SAP RTMP General

General

Streaming Setting	Default	Description/Values
These buttons become available to control a stream once it has started streaming (after you click Apply).		
Stop	n/a	Click **Stop** to stop an active stream. You can later restart it or clear it.
Pause	n/a	Click **Pause** to pause the stream. If a Still Image When Paused has been configured, it will be displayed. You can later resume the stream or stop it.
Start	n/a	Click **Start** to restart a stopped stream.
Statistics	n/a	Click **Statistics** to view statistics for the stream. See Streaming Output Statistics.

SRT Streaming Settings

The following table lists the SRT-specific parameters:

Connection SRT Settings

Connection

SRT Stream Setting	Description
Mode	Specifies the SRT Connection Mode: • Caller: The SRT stream acts like a client and connects to a server listening and waiting for an incoming call. • **Note** The firewall must be configured to allow incoming Caller connections to reach the Listening device. • **Note** To simplify firewall traversal, Rendezvous Mode allows the encoder and decoder to traverse a firewall without the need for IT to open a port, but requires that the firewall not remap the UDP port for the stream.
Address	**Tip** You can also enter a Fully Qualified Domain Name (FQDN).
Source Port	**Note** This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.
Destination Port	(Caller and Rendezvous modes) Specifies the UDP destination port for the SRT stream.
Port	(Listener mode only) Specifies the UDP local port for the SRT stream.

Connection SRT Settings

SRT Settings

SRT Stream Setting	Description
Network Adaptive	Check this checkbox to enable Network Adaptive Encoding. NAE directs the video encoder to adapt to changing network throughput used by the SRT stream during operational use with the goal of maximizing video quality for a given network. NAE may adjust video bitrate, frame-rate and resolution depending on measured link throughput without stream tear-down and re-build.

SRT Stream Setting	Description
(Buffering) Latency	**Note** Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices. The SRT buffer, configured as "Latency"", is the time reserved in the decoder to recover missing packets.
Encryption	Enables AES encryption and specifies the key length, either: None, AES-128, or AES-256
Passphrase	(Only required and accepted if Encryption is enabled) Specifies a string used to generate the encryption keys to protect the stream. Range = 10-79 UTF8 characters
Bandwidth Overhead (%)	Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-50% **Note** SRT streams may temporarily overshoot the defined bandwidth overhead limit.

Streaming Output Statistics

The following table lists the Streaming statistics:

Streaming SRT

Streaming

Streaming Statistic	Description/Values
State	The current operating status of the stream, either: • STREAMING • STOPPED • PAUSED
Up Time	(only available when State is STREAMING) The length of time the stream is actively streaming (e.g., 1d22h5m41s).
SSRC	(RTP only) The synchronization source.
Sent Packets	Number of RTP or UDP packets sent for that stream.
Sent Bytes	Number of Bytes sent for that stream.
Unsent Packets	Number of RTP or UDP packets not sent for that stream.
Unsent Bytes	Number of Bytes not sent for that stream.
Last Error	The last logged error (number and description).
Occurred	The time at which the last error was logged (i.e., how long ago).
Bitrate	The stream bitrate (in kbps).
Reset	Click to reset the Output statistics.

Streaming SRT

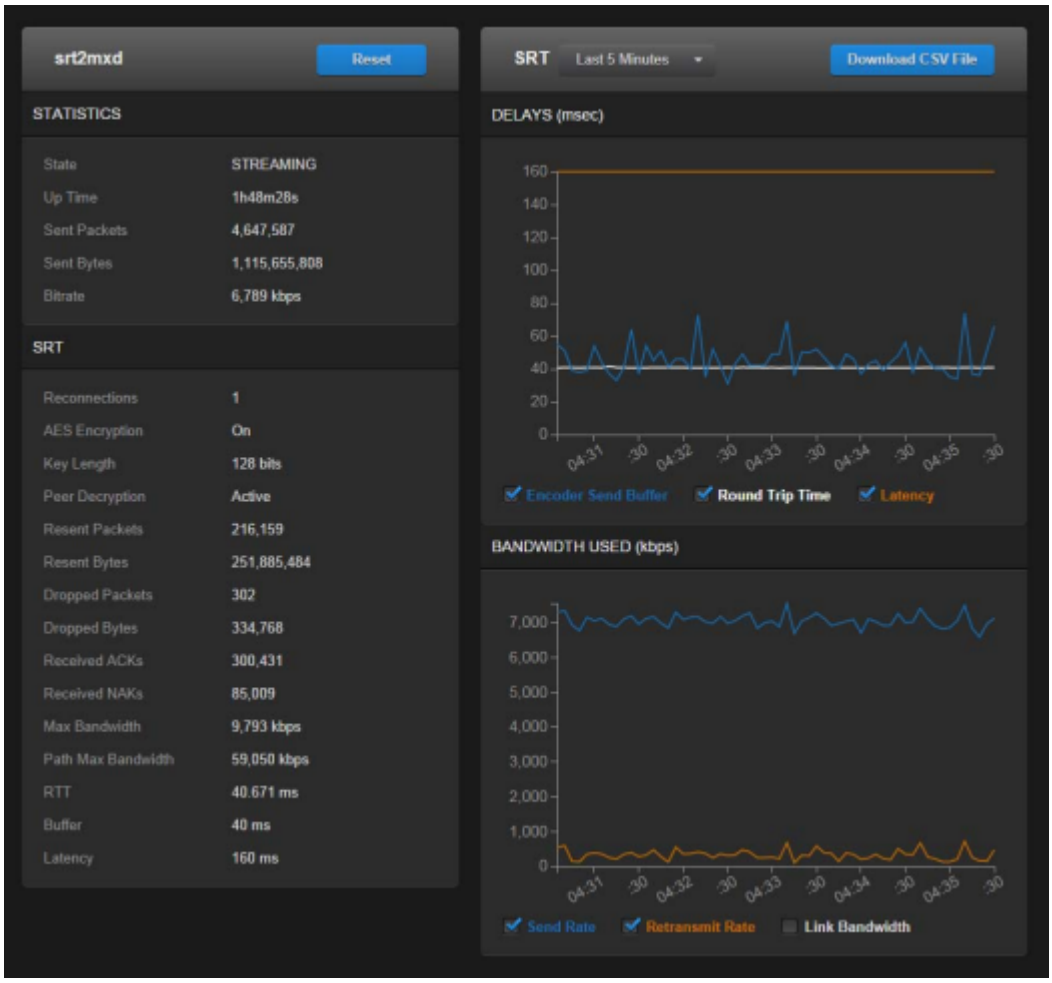
SRT

Streaming Statistic	Description/Values
Reconnections	Number of reconnections since the stream started. Severe network congestion may cause the connection to drop and automatically reconnect.
AES Encryption	Indicates whether Advanced Encryption Standard (AES) encryption has been enabled.
Key Length	The key length for AES encryption, either: None, AES-128, or AES-256
Peer Decryption	Indicates whether the decoder can decrypt the stream. Either Active, Initializing, Inactive (no passphrase), or Inactive (invalid passphrase).

Streaming Statistic	Description/Values
Resent Packets	Number of packets retransmitted following a lost report from the decoder.
Resent Bytes	Total bytes of the lost packets retransmitted.
Dropped Packets	Number of dropped packets.
Dropped Bytes	number of dropped bytes.
Received ACKs	Transmission progress acknowledgement and feedback.

Streaming Statistic	Description/Values
Received NAKs	Lost packet reports.
Max Bandwidth	Maximum bandwidth (input stream rate * (1 + overhead)).
Path Max Bandwidth	Estimated link bandwidth. This can change due to cross traffic.
RTT	Measured Round Trip Time.
Buffer	**Tip** If the Buffer goes to or above the Latency value often, then there is most likely insufficient bandwidth to support the desired bitrate. In this case, decrease your bitrate. If the Buffer occasionally goes to or above the Latency Value, then the SRT Latency should be increased.
Latency	Maximum of the decoder and encoder configured in (Buffering) Latency. For example: Encoder Configured SRT Latency = 750 Decoder Configured SRT Latency = 20 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 other side.

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



Note

The Link Bandwidth is an estimate of the actual link bandwidth.

Configuring Recording Outputs

Important

Recording is *only* available on the Makito X with Storage dual-height model (either fixed or removable SSD). For details, see Storage Options.

Setting Up Recording

Note

The Makito X with Storage can record two streams simultaneously.

When setting up a recording session, you select the file format (either .TS or .MP4) and then can optionally configure a recording limit and segmentation.

Recording segmentation subdivides the recording into segments. Segmented file creation is useful for long duration or continuous recording. You can specify either a size limit or a time limit for segments of the content recording. As each completed segment is saved, a new segment is created and any newly created content is stored in the new segment.

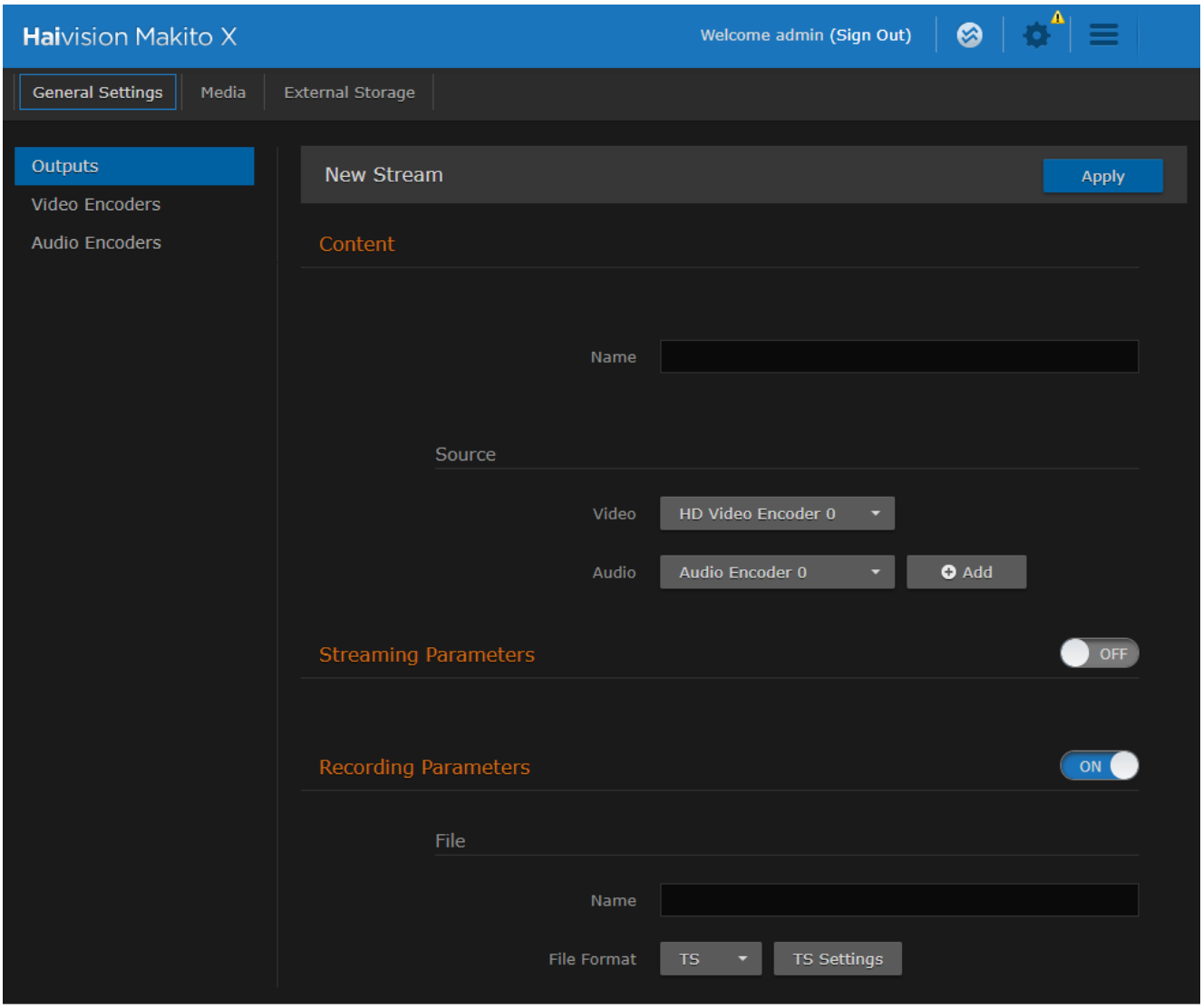
- Auto Export automatically exports completed segments to either HVC or an FTP server. Auto Export becomes available once you either set a recording limit or enable segmentation.
- Segmentation Roll-Over deletes old segments beyond the configured recording limit. As such, it is only available when a recording limit is set and segmentation is enabled.

You can play back .MP4 assets directly in the Makito X Web Interface once a segment of the recording has completed. See Managing Recordings.

Makito X recordings can be used by either HVC or Haivision Media Platform. These videos can be downloaded from the Makito X Web Interface, exported to a USB, or sent automatically to an FTP location.

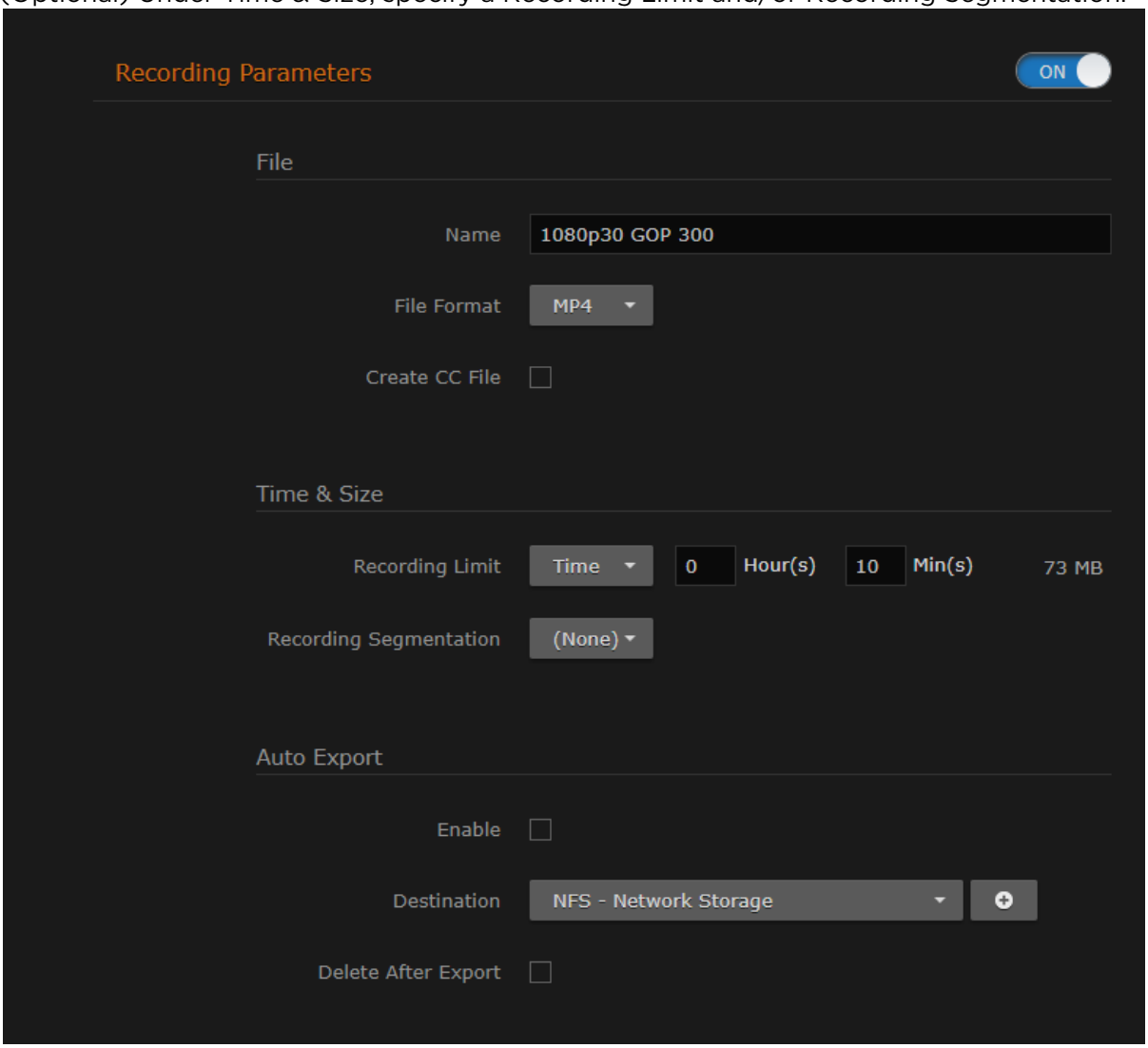
To set up a Recording session:

1. On the Streaming page, click **General Settings** on the navigation bar and **Outputs** on the sidebar.
2. From the Outputs List View, click a link in the table for an existing stream, or click **Add** to add a stream.
3. On the Outputs Detail View, if necessary, scroll down the page and toggle the Recording Parameters button to **On**.



4. Under File, enter the name and select the File Format.

5. (Optional) Under Time & Size, specify a Recording Limit and/or Recording Segmentation.



6. Click **Apply** to start recording (as well as streaming, if configured).
7. To return to List View, click **Outputs** on the sidebar.

Recording Settings

The following table lists the Recording controls and settings:

Recording Setting	Default	Description/Values
File		
Name	n/a	**Note** This name is merged with the recording start date/time of the asset segment to create the asset file name.
File Format	TS	Select the file format for the recording, saved directly into a file either: • TS (Transport Stream): MPEG-2 TS/ISO 13818-1 format. Supports audio/video & metadata. • MP4: formatted as per ISO 14496-12, 14 and 15. Only supports audio/video, no metadata.
TS Settings	Auto-Assign	Available if the File Format is TS. See "Transport Stream Settings" in Streaming Output Settings.
Create CC File	Disabled	(File Format must be MP4) Check this checkbox to create a serial file (.srt) containing the captured closed captions. This file can be used by some players to replay the captions with the recorded content.
Time & Size		
Recording Limit	None	Specifies either a size limit or a time limit for the recording: • (None) • Time: Specify the time limit in hours and minutes. • Size: Type in the size limit and select either MB, GB or TB.
Recording Segmentation	None	Specifies either a size limit or a time limit for recording segments. • (None) • Time: Hours and Minutes • Size: Type in the size limit and select either MB, GB or TB
Segmentation Roll Over	Disabled	(*Both* Recording Limit and Recording Segmentation must be enabled) Check this checkbox to delete the oldest content and continue recording new content as segments are filled. See Roll-Over and Uploading to HVC or Haivision Media Platform.
Enable	Disabled	(*Either* Recording Limit or Recording Segmentation must be enabled) Check this checkbox to configure the recording session to automatically export completed segments to either HVC or an FTP server.
Destination	None	Select from drop-down list of previously defined destinations (see "Destination" in Streaming Output Settings). Or you can click **+Add** to add an export destination from this page and then select it.

Delete After Export	Disabled	(Not available when Segmentation Roll Over is enabled) Check this checkbox to configure the Makito X to delete these files after transfer.

Roll-Over and Uploading to HVC or Haivision Media Platform

Segmentation Roll-Over becomes available when the Time & Size are set for a recording and both Recording Limit and Recording Segmentation are enabled. Segmentation RollOver allows you to leave the encoder running autonomously (for example, to record a high quality stream while streaming a low quality version of the same content for surveillance purposes, such as over 24 hours).

In such applications, operators do not intend to view the recording unless some event occurs and then they can extract just the particular segment, instead of having to go through the entire 24 hour file. To do this, you simply set up the recording in Segmented Roll-Over mode and leave it alone.

The recording may also be configured to upload completed segments to the Haivision Video Cloud (HVC), Haivision Media Platform (via FTP), or a NAS drive.

As of Version 1.5, you can auto-export a segment of an asset that has completed recording to a NAS drive in order to automate asset ingest from a Makito X with storage to a NAS-mounted watch folder.

Managing Recordings

Important

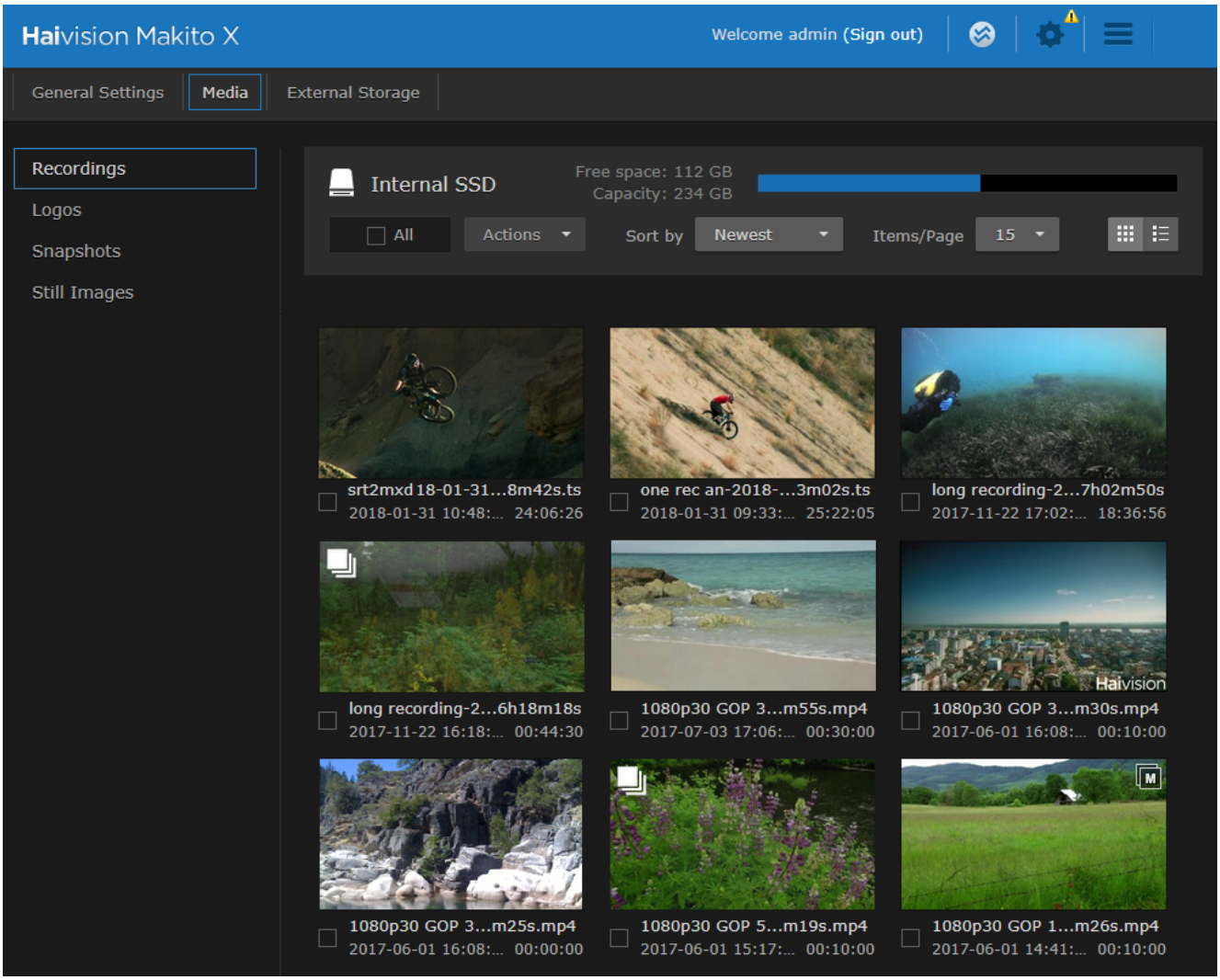
The Asset Browser is only available on the Makito X with Storage dual-height model. For details, see Storage Options.

From the Recordings (Asset Browser) page, you can manage the recordings created from Makito X encoded stream content. For setup details, see Configuring Recording Outputs.

From here, you can copy, move, download, export, and delete recordings. You can also select and play back .MP4 recordings directly in the Makito X Web Interface once a segment of the recording has completed.

To manage recordings:

1. On the Streaming page, click **Media** on the navigation bar and **Recordings** on the sidebar.
2. The Recordings page opens, displaying the list of files that have been recorded by the encoder, as shown in the following example.



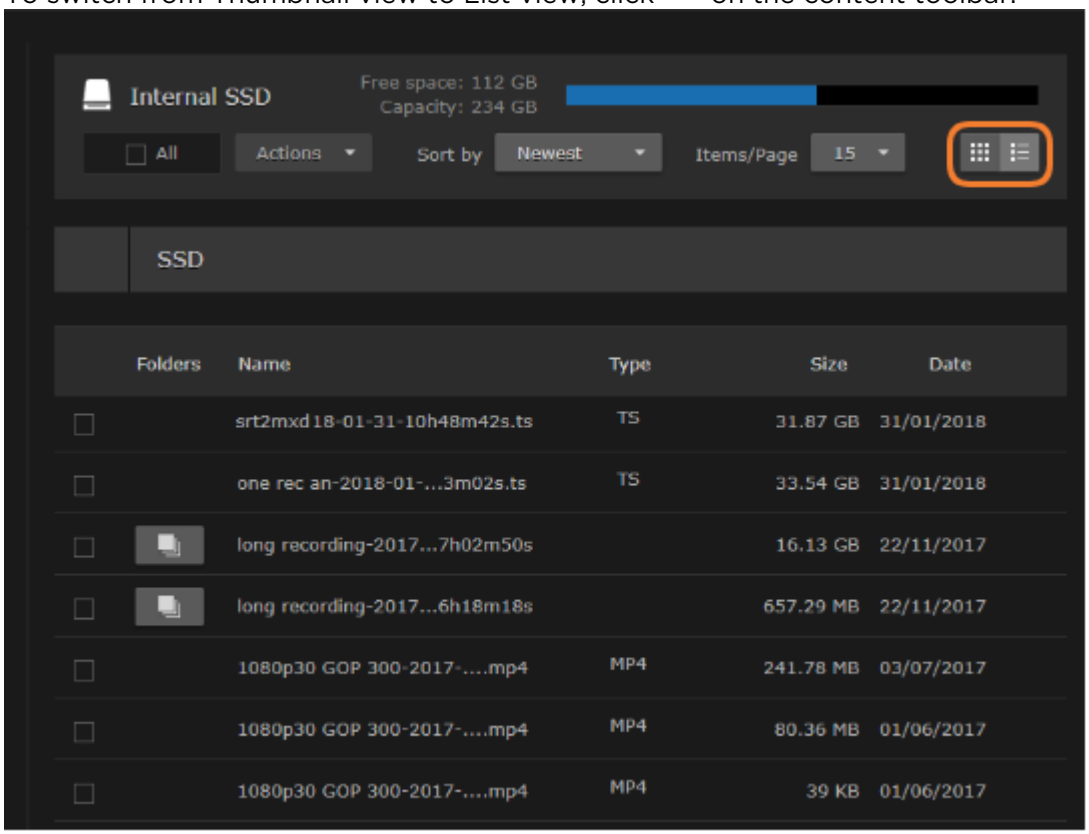
Tip

If you have a Removable SSD Storage option, you can review the contents from a removable drive on a PC (Windows 7 to 10) or MAC OS. For details, see Viewing Recordings from a Removable Drive on a Computer.

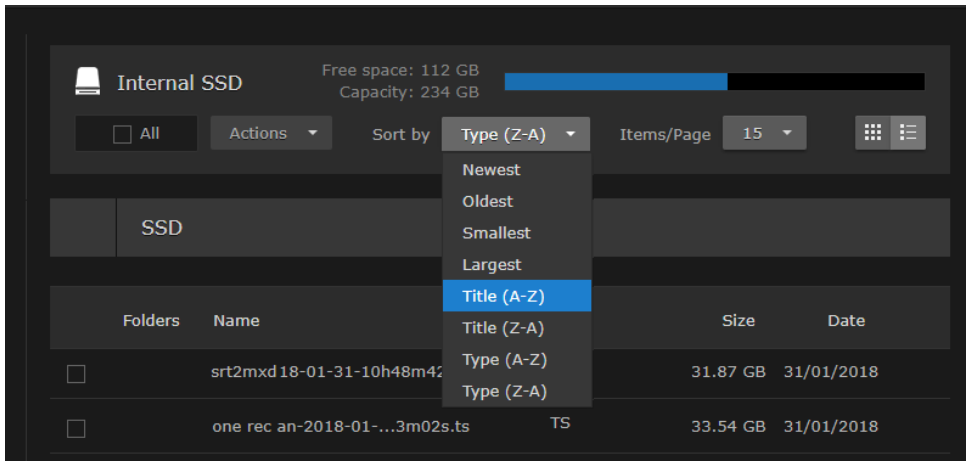
Viewing Options

By default, the Recordings (Asset Browser) page opens with the list displayed in Thumbnail view, showing the newest assets first. In Thumbnail view, each asset is represented with a thumbnail image. You can adjust the display to List view, which displays the assets in horizontal rows of information. You can also change the sort order of the list and change the number of items to display per page.

1. To switch from Thumbnail view to List view, click on the content toolbar.



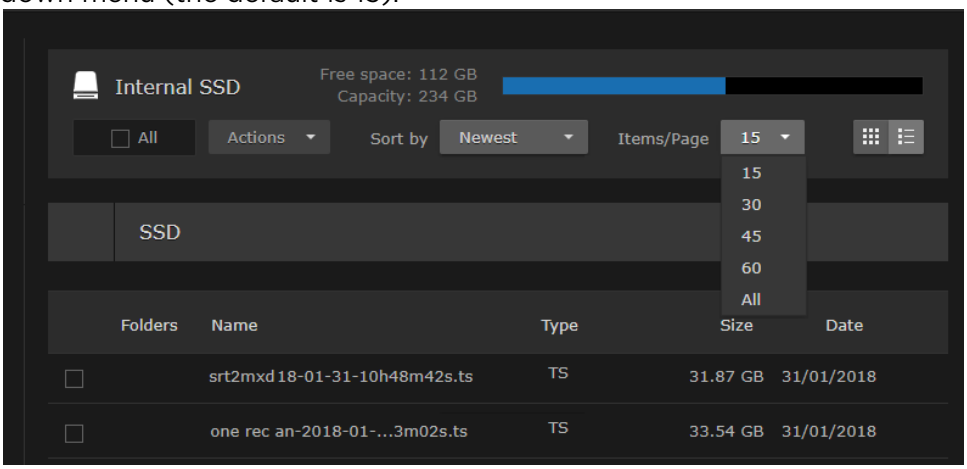
2. To sort the list by a different metadata field or change the sort order, select from the **Sort by** drop-down menu.



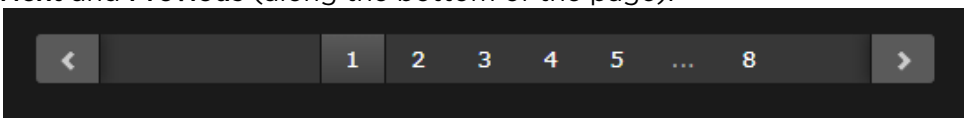
The **Sort by** options include creation date (Oldest or Newest), file size (Smallest or Largest), title

(A-Z or Z-A), and type (A-Z or Z-A).

3. To change the number of items to display per page, select the number from the **Items/Page** drop-down menu (the default is 15).



4. If the list is more than one page, you can page forward and backward through the list by clicking **Next** and **Previous** (along the bottom of the page).



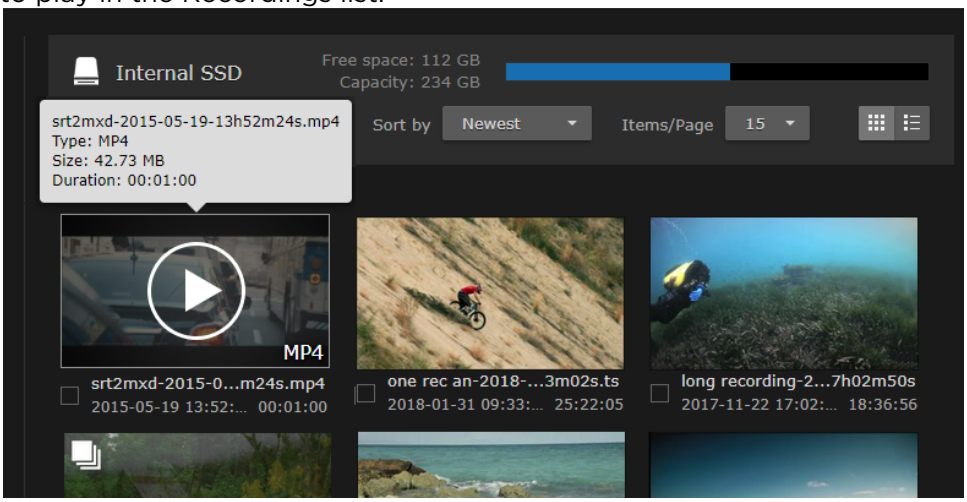
Playing Back .MP4 Recordings

Note

If you have a removable storage drive, you can play back either .MP4 or .TS files on a PC. See Viewing Recordings from a Removable Drive on a Computer.

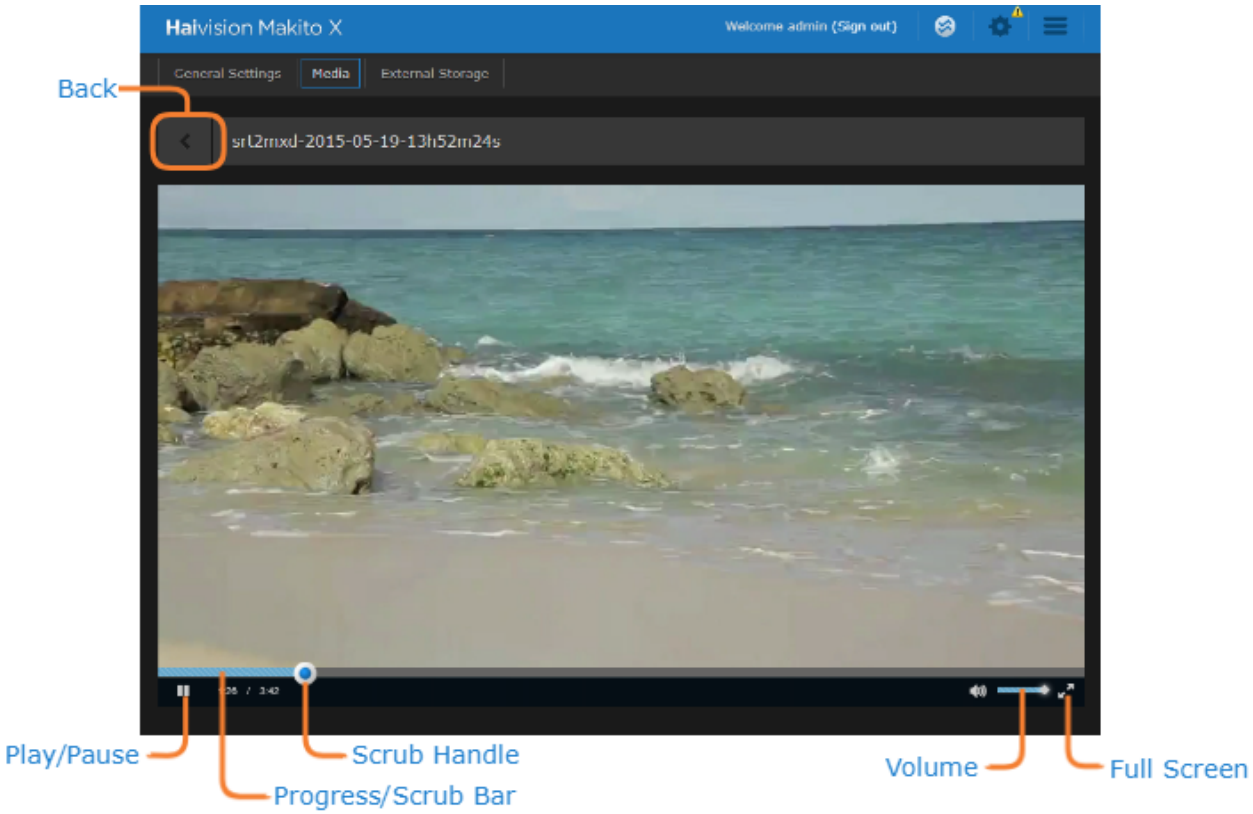
To play back .MP4 recordings:

1. On the Recordings page, click the thumbnail (anywhere except the name or time) of the recording to play in the Recordings list.



2. Click the arrow in the player to start playback.

The Recording opens and starts to play in the player (as shown in the following example).



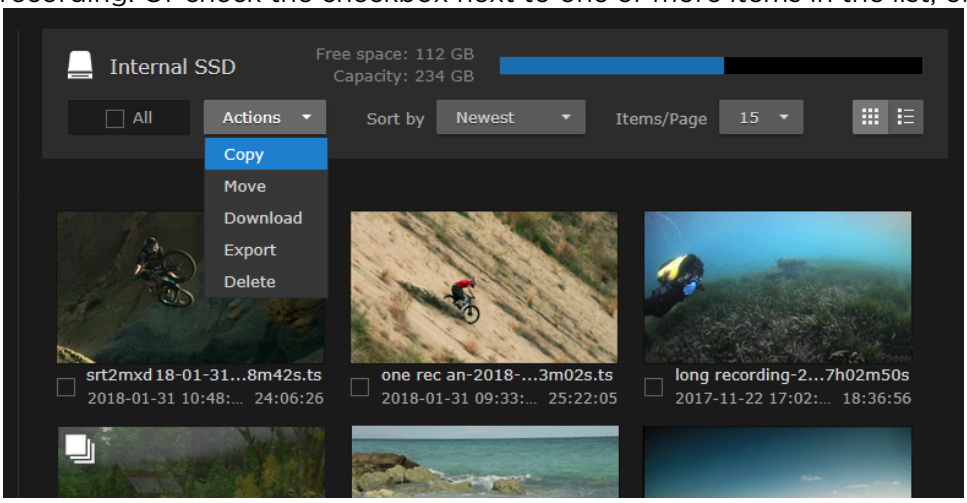
3. From here you can pause and restart playback and adjust the volume.
4. To move forward or backward through the video, drag the scrub handle along the progress/scrub bar.
5. To switch to full-screen mode (i.e., to fill your entire screen and remove the player controls), mouse over the viewer and click (in the bottom right corner). To exit full-screen mode, press ESC or click again.
6. To return to the Recordings list, click the icon.

Managing Recorded Content

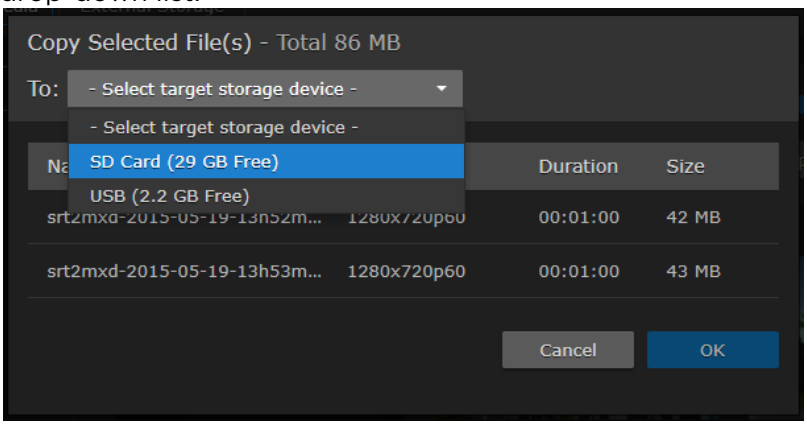
From the Recordings page, you can copy or move one or multiple recordings to a storage location. The difference is that moving deletes the recordings from the Recordings page. You can also download recordings as MP4 or TS files, export files to an FTP/FTPS server or the Haivision Video Cloud (HVC), and delete recordings.

To copy or move recordings:

1. On the Recordings page, click the name or time information (*not* the thumbnail) to select the recording. Or check the checkbox next to one or more items in the list, or check All.



2. Select Copy or Move from the Actions drop-down menu (this menu is selectable when one or more items are checked).
3. On the Copy or Move Selected File(s) dialog, select the (destination) storage location from the drop-down list.



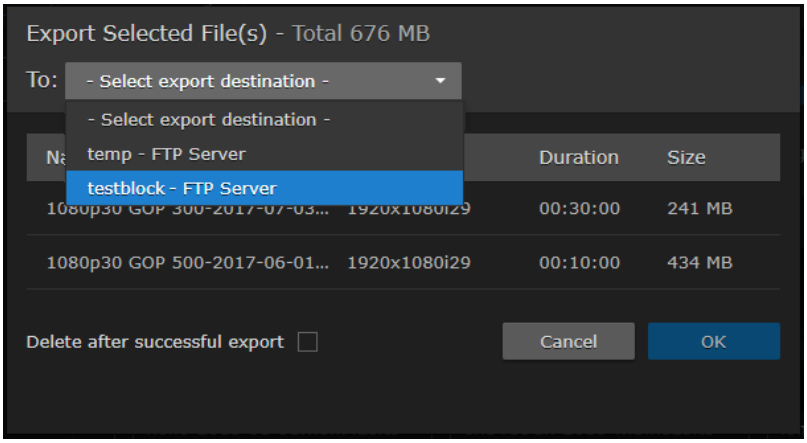
4. Click **OK**.

To download recordings:

1. Select one or more recordings from the Recordings list.
2. Select Download from the Actions drop-down menu.
3. Type in the file name in the Save As window and click **Save**.

To export recordings:

1. Select one or more recordings from the Recordings list.
2. Select Export from the Actions drop-down menu.
3. On the Export Selected File(s) dialog, select the (destination) server location from the drop-down list.



4. (Optional) Check the "Delete after successful export" checkbox.
5. Click **OK**.

To delete recordings:

1. Select one or more recordings from the Recordings list.
2. Select Delete from the Actions drop-down menu.
3. Click **Confirm** (or where applicable, select **Delete** from the warning dialog). The selected recording(s) will be removed from the list.

Viewing Recordings from a Removable Drive on a Computer

The Makito X with Removable Storage will record either .TS or .MP4 on a SATA drive formatted for EXT4. This section explains how to review the contents from a removable drive on a PC (Windows 7 to 10) or MAC OS.

Prerequisites:

- USB2-3 uSATA dock
- ExtFS disk utility (from Paragon) installed on computer http://www.paragon-software.com/home/extfs-windows-pro/eshopbusiness.html?affChecked=1

To view recordings on a MAC OS X computer:

1. Download the ExtFS for MAC OS X and install it.
2. Remove the SAT A drive from the Makito X and insert it into a SATA dock on your computer.
3. You will see the EXT4 file system mounted automatically on the desktop.
4. You can view MP4s using VLC.
5. You can view TS files using VLC or another TS player such as Haivision's InStream.

To view recordings on a PC (Windows Professional):

1. Download the ExtFS for Windows Professional and install it.
2. Remove the SAT A drive from the Makito X and insert it into a SATA dock on your computer.
3. You will see the EXT4 file system.
4. You can view MP4s using VLC.
5. You can view TS files using VLC or another TS player such as Haivision's InStream.

Configuring Logo Overlays

> **Note**
>
> The maximum file size for logo and still image files is 10 MB.

You can configure the Makito X to display a graphic file as a logo overlay in the encoded video. One logo may be configured for each physical video input interface, i.e.:

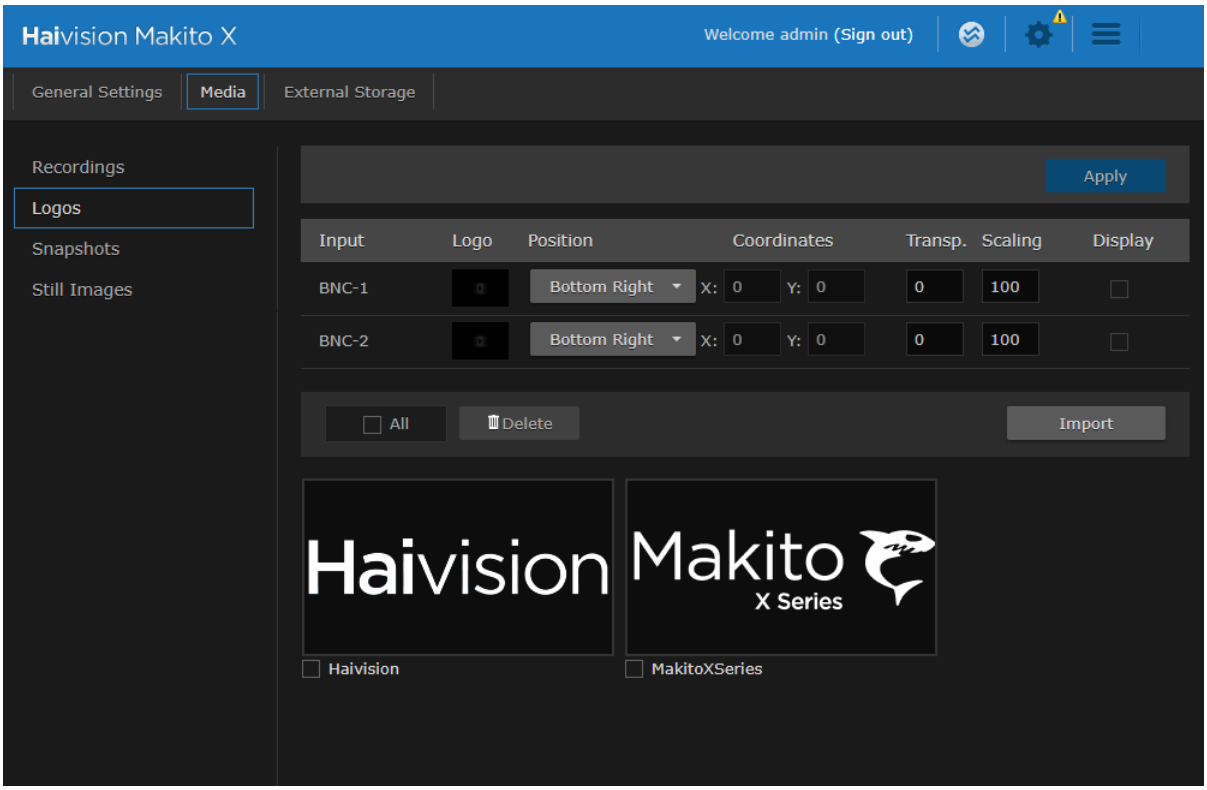
- Two logos on the Makito X SDI dual-channel #S/B-292E-HDSDI2 (BNC1 and BNC2);
- One logo on the Makito X DVI #S/B-292E-DVI or the Makito X SDI single-channel #S/B-292E-HDSDI1.

The image file can be uploaded in either BMP, JPEG, PNG, or GIF format. The image file will be converted to Haivision's image overlay (.oly) format.

The logo position can either be relative (top left, top right, centered, etc.) or absolute (positioned at the exact X and Y coordinates specified).

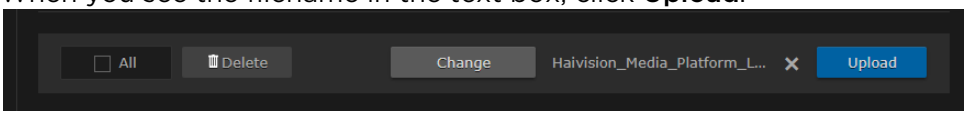
To configure a logo overlay:

1. On the Streaming page, click **Media** on the navigation bar and **Logos** on the sidebar.
2. The Logos page opens, displaying the list of logo image files that have been uploaded for the encoder.



3. To upload a new image file in either BMP, JPEG, PNG, or GIF format, click **Import** and select the file in the Open File dialog box.

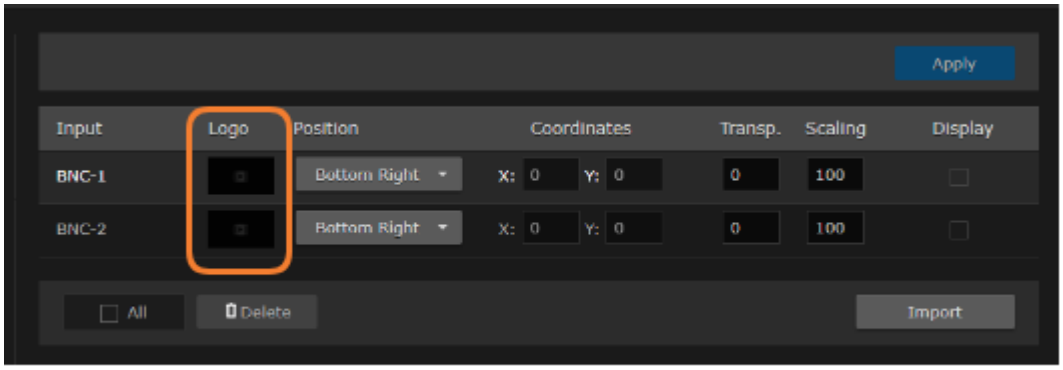
4. When you see the filename in the text box, click **Upload**.



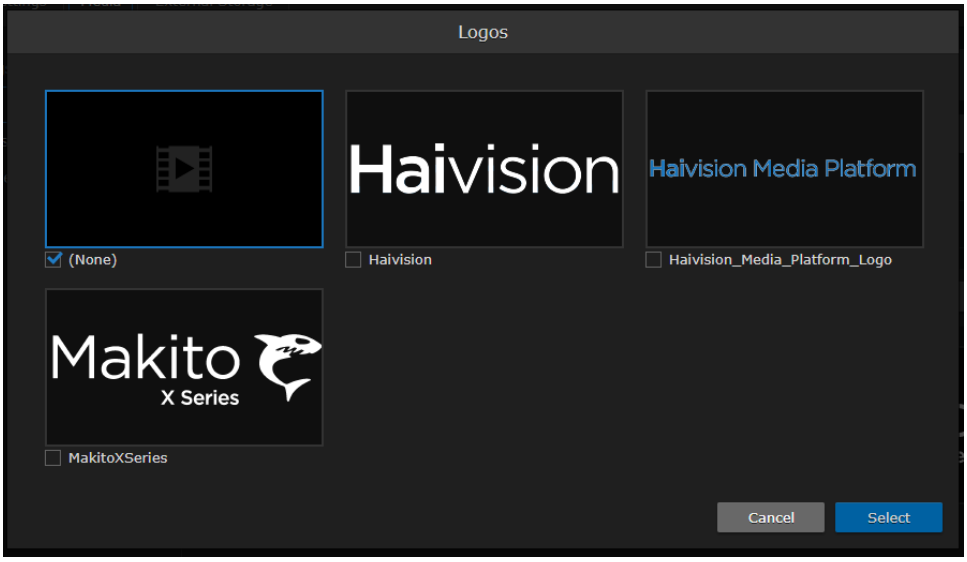
> **Tip**
>
> To select a different logo file, click **Change**. To remove the selection, click the ✕ icon.

The image file will be converted to Haivision's image overlay (.oly) format and will be added to the Logos list.

5. To select the image file to display as a logo overlay, in the channel row, click the area below **Logo**.



The **Logo Selection** dialog opens, with the currently selected logo or None highlighted and checked.



6. To select the image for the logo overlay, click the image or check the checkbox next to the image filename and click **Select**.
7. To configure the position, transparency, and scaling for the logo overlay, select or enter value(s) in the appropriate field(s). See Logo Settings.
8. To delete one or more image files from the Logos list, check the checkbox next to one or more filenames (or check **All**) and click **Delete** on the Content toolbar.
9. To apply your changes, click **Apply**.

Note

Logos are stored on the Makito X file system in the folder `/usr/share/haivision/logos`.

Related Topics:

- Logo Settings
- logo (CLI Command)

Logo Settings

The following table lists the Logo controls and settings:

Logo Setting	Default	Description/Values
Input	n/a	On the Makito X SDI dual channel, the video input is either BNC-1 or BNC-2. On the Makito X-DVI or SDI single channel, there is only one video input.
Position	Bottom Right	Select the position for the logo overlay: • Bottom Right • Top Right • Bottom Left • Top Left • Centered • Absolute • Relative **Note** In Absolute mode, the logo will be positioned at the exact X and Y coordinates specified.
Coordinates	0, 0	**Note** Only takes effect if Position is set to Absolute.
Transparency	0	Specifies the percentage of transparency for the logo: • 0 = no transparency (i.e., a completely solid/ opaque logo) • 100 = fully transparent (i.e., a completely transparent/invisible logo)
Scaling	100	Specifies the scale factor (percentage) for the logo: • 25% = 1/4 size • 100% = no scaling • 400% = 4x
Display	Disabled	Check this checkbox to display the selected file as a logo overlay.

Capturing Image Snapshots

> **Note**
>
> Snapshot Capture is an optional H.264 feature which may be disabled at the factory. The following section is only applicable if snapshots are enabled.

From the Snapshots page, you can take a snapshot of the current video input and save it to either JPEG or YUV image format. With JPEG snapshots, you can also specify the image quality. On the Makito X SDI, you can select the video input, either BNC-1 or BNC-2.

The snapshot feature may be used to create still images, for example, to record a person's image or a scene from an event for identification purposes or for future reference.

When you take a snapshot, a unique snapshot name will be generated based on the current time.

Thumbnails of the snapshots are displayed on the Snapshots page for you to view and optionally save to an external location.

Note that the encoder must have a valid Input Format. To verify the Input Format detected by the system, see Configuring Video Encoders.

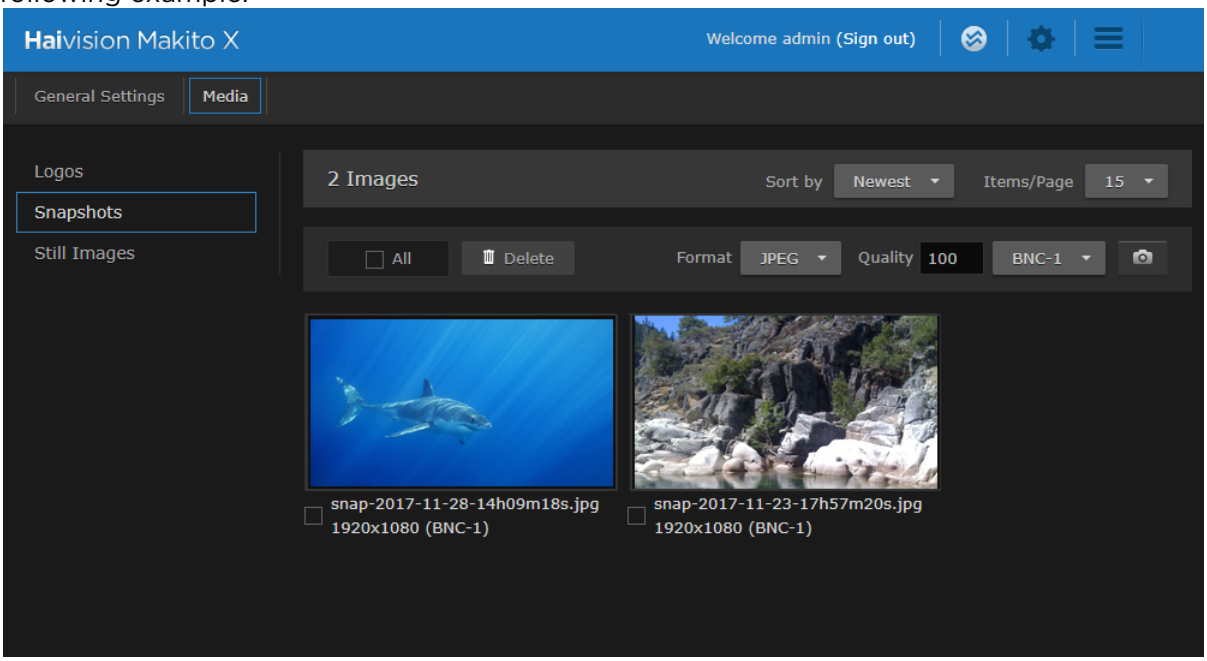
> **Note**
>
> Snapshot files are stored on the Makito X file system under `/usr/share/haivision/snapshots`.

> **Tip**
>
> You can also take snapshot of each video input from the Video Encoders List View.

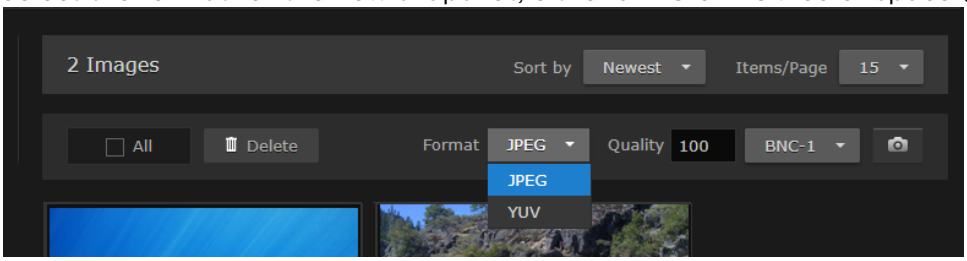
To take an image snapshot:

1. On the Streaming page, click **Media** on the navigation bar and **Snapshots** on the sidebar.

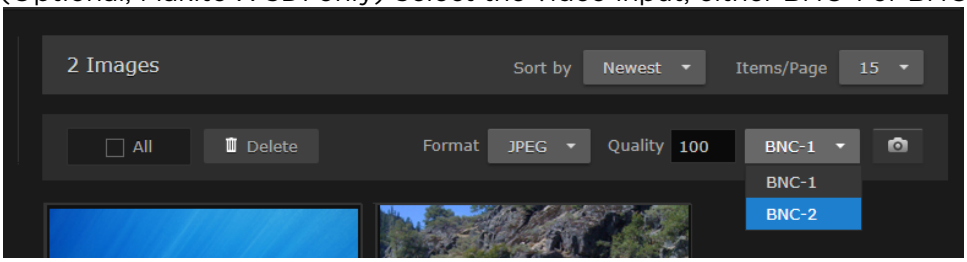
2. The Snapshots page opens, displaying the snapshots taken for the encoder, as shown in the following example.



3. To toggle the sort order of the list from newest to oldest, select the order from the **Sort by** drop-down list.
4. Select the format for the new snapshot, either JPEG or YUV color space (color model).



5. (JPEG only) To adjust the image quality, either type in a value between 1 and 100 in the Quality field.
6. (Optional, Makito X SDI only) Select the video input, either BNC-1 or BNC-2.



To take the image snapshot, click the icon. Once a snapshot has been taken, a new thumbnail is displayed.

7. (JPEG only) To view a full-size image of a snapshot, click the thumbnail.
8. To save the snapshot to an external location, right-click either the thumbnail or the full-size image (JPEG only), and select Save image as...
9. To delete one or multiple snapshots, check the checkbox beside the snapshot (or click **Check All**) and click **Delete**.

Related Topics

- Configuring Video Encoders
- Configuring Still Image Streaming

Configuring Still Image Streaming

When creating a stream, you can specify a static image that will be used to replace the encoded video stream when the stream is paused. This feature may be used, for example, to block out sensitive content or deliver announcements and other messages. See Selective Video Mute.

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

Note

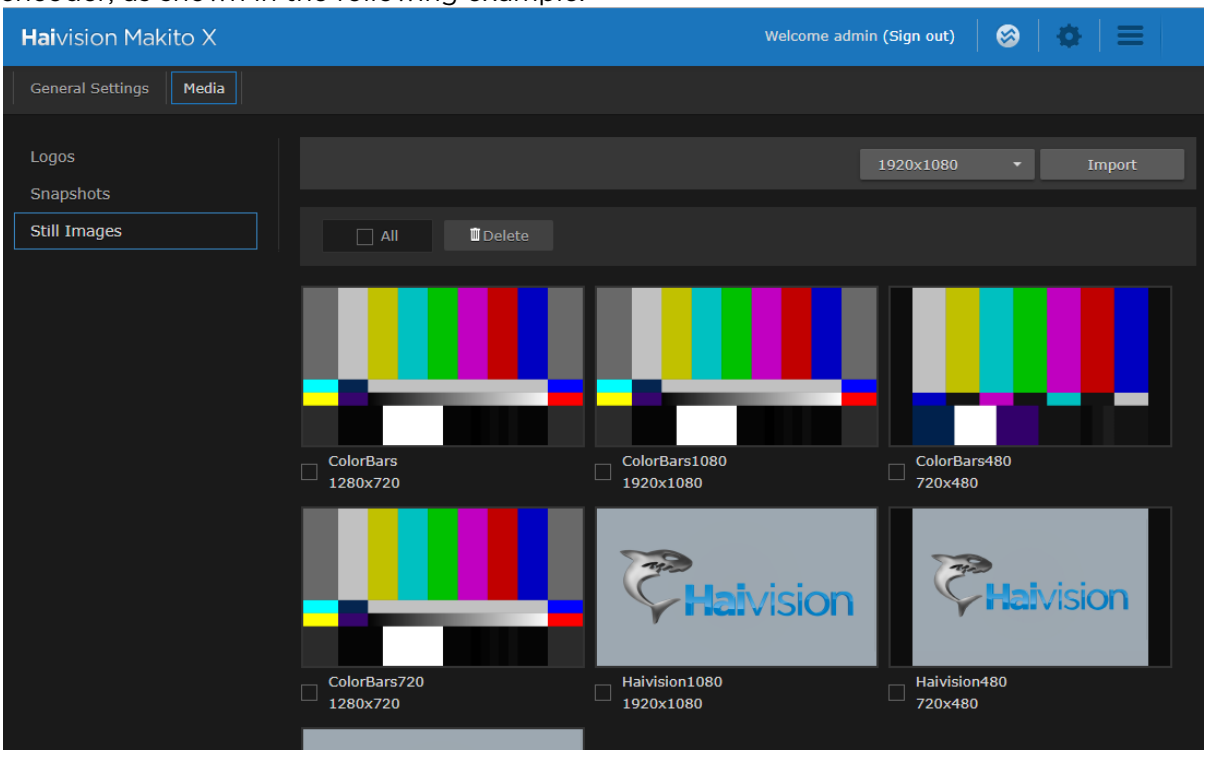
Still Image insertion when pausing a stream is *not* supported when a HEVC/H.265 video encoder is selected as a content source.

Tip

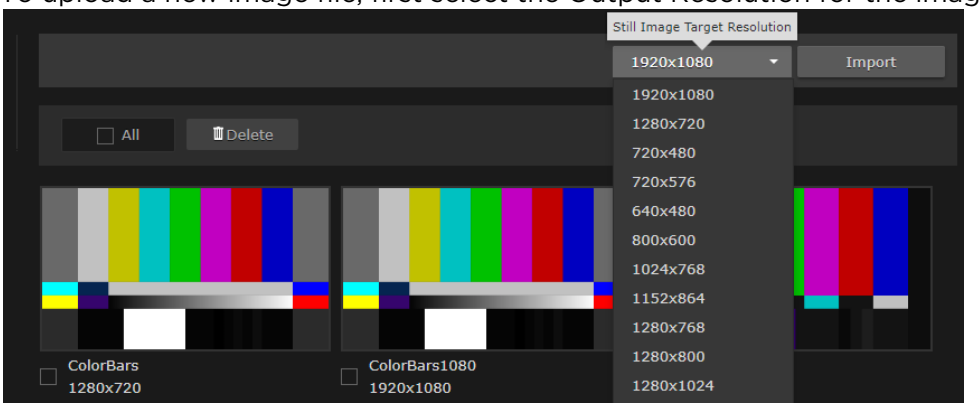
For best results, the input file resolution must be the same or greater than the output resolution.

To upload a static image:

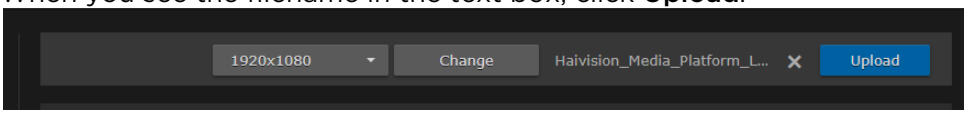
1. On the Streaming page, click **Media** on the navigation bar and **Still Images** on the sidebar.
2. The Still Images page opens, displaying the list of still images that have been uploaded for the encoder, as shown in the following example.



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



4. Click **Import** and select the file in the Open File dialog box.
5. When you see the filename in the text box, click **Upload**.



> **Tip**
>
> To select a different image file, click Change. To remove the selection, click the ✕ icon.

The static image is encoded into a single H.264 GOP sequence and will be used to replace the “real” video stream when the stream is paused.

6. 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 External Storage

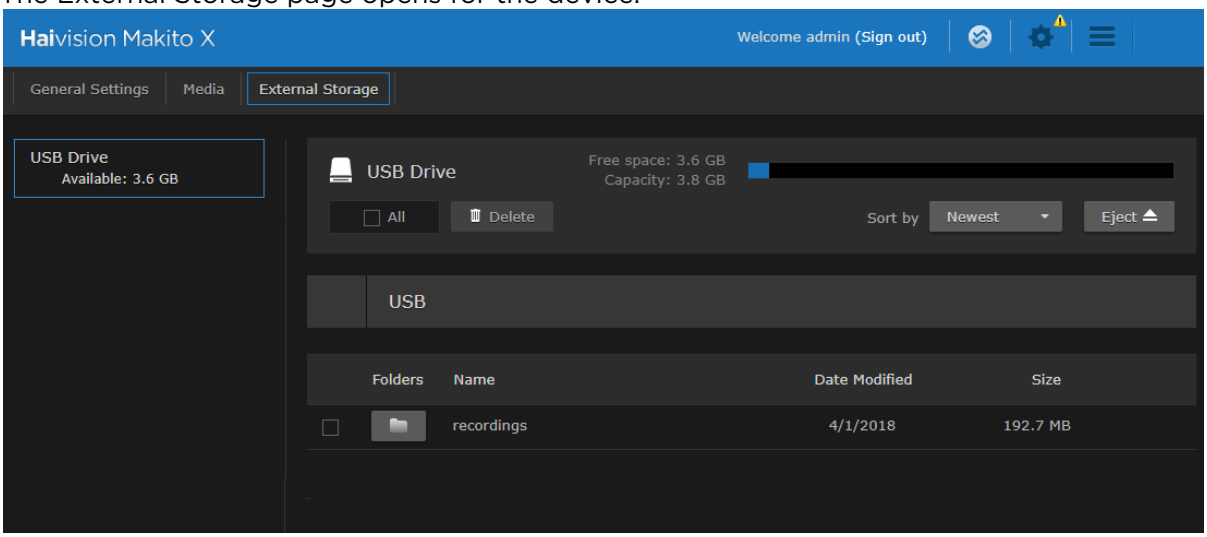
Important

The External Storage page is *only* available on the Makito X with Storage dual-height units with face-plate accessible USB 2.0 and SD card interfaces. For details, see Storage Options.

The External Storage pages list all installed external storage devices for the encoder. There is a separate page for each device, which shows the available space and capacity. From here, you can view the list of folders (and sub-folders) on each device, as well as delete folders or files and eject devices.

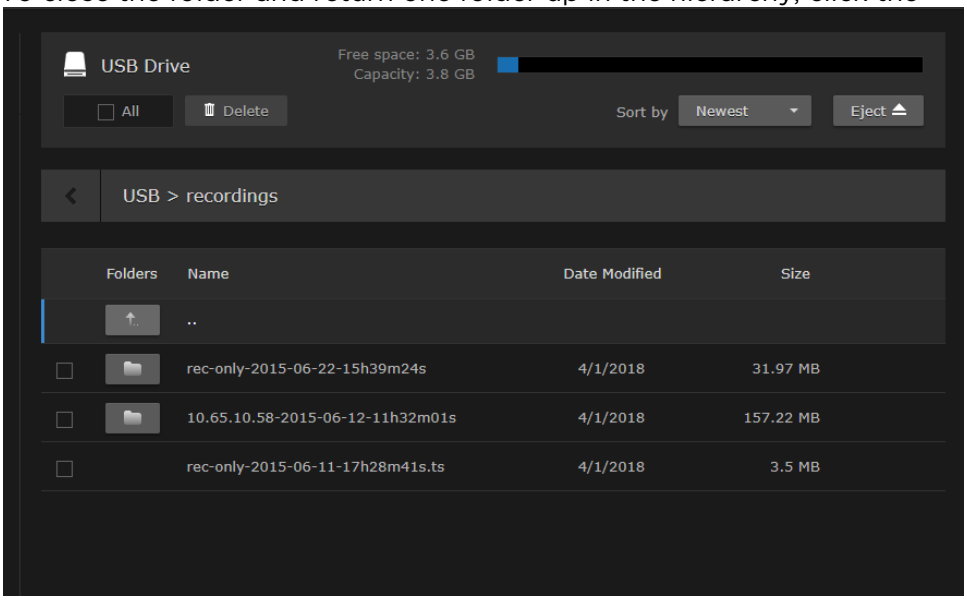
To manage external storage:

1. On the Streaming page, click **External Storage** on the navigation bar. If more than one storage device is available, select the device (for example, **SD Card** or **USB Drive**) on the sidebar. The External Storage page opens for the device.



   This page displays the name, date modified, and size for each folder.
2. To display the contents of a folder, click the ? Unknown Attachment icon.

3. To close the folder and return one folder up in the hierarchy, click the .. icon.



4. To change the sort order of the list of folders, select the order from the **Sort by** drop-down menu.
5. To delete one or multiple folders or files, check the checkbox beside the folder (or check **All**) and click **Delete**.
6. To unmount one or multiple removable devices (i.e., SD or USB or removable SSD), check the checkbox beside the device (or check **All**) and click **Eject**.
7. Remove the device from the interface port.
8. Install the device on a computer to view the assets on the device. (See Viewing Recordings from a Removable Drive on a Computer.)

System Administration and Storage

Note

Unless otherwise indicated, the Administration Settings and Storage pages are only accessible to administrators.

Topics in This Chapter

- Viewing System Status Information
- Saving and Loading Presets
- Installing Firmware Upgrades
- Configuring Network Settings
- Configuring Date and Time
- Enabling and Disabling Network Services
- Managing Licenses
- Managing the COM Port
- Managing Storage Drives
- Managing Network Storage
- Configuring Export Destinations
- Managing Snapshot Storage Locations
- Managing File Transfer History

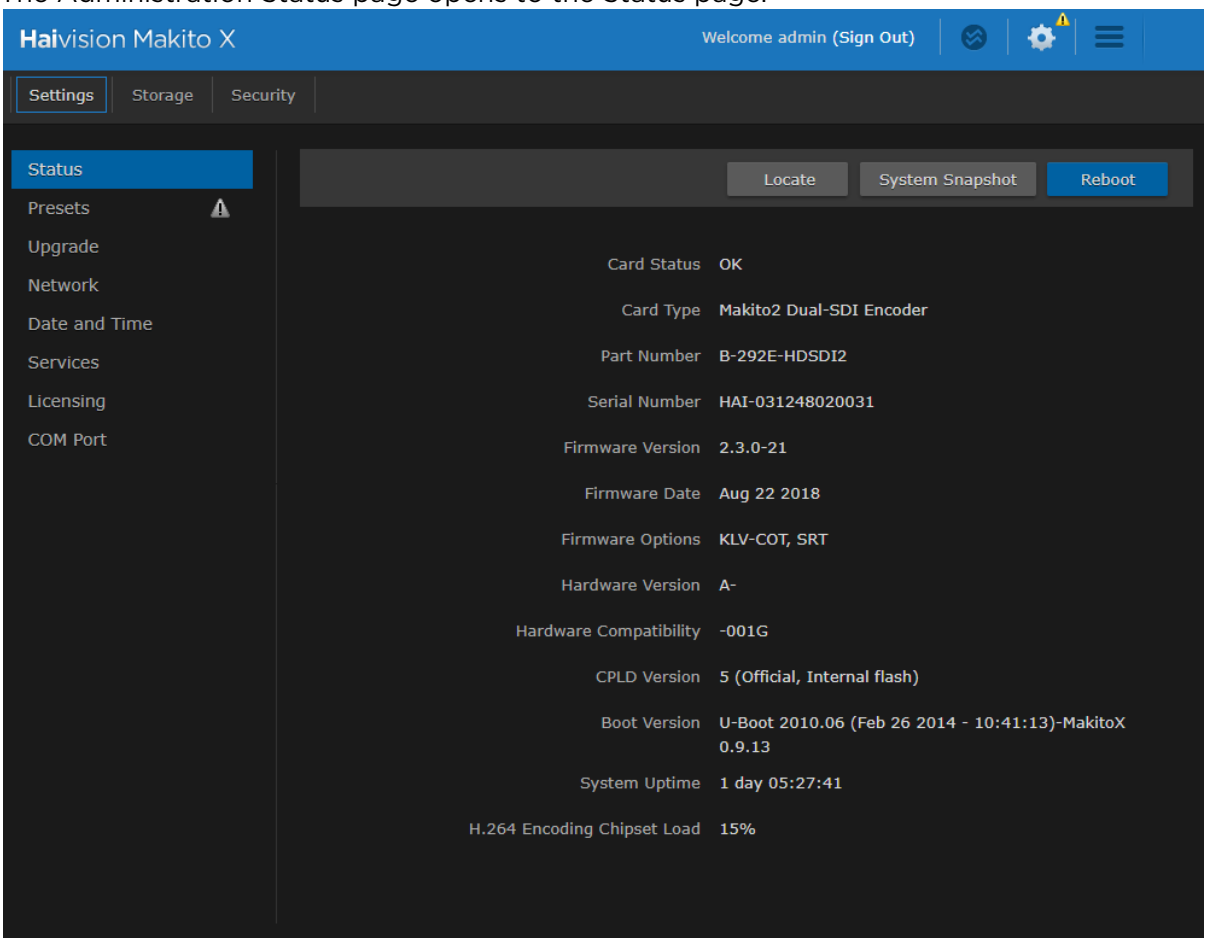
Viewing System Status Information

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 initiate blinking of the Status and TX LEDs (to help locate particular encoders in a lab or rack), as well as take a system snapshot and reboot the encoder.

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

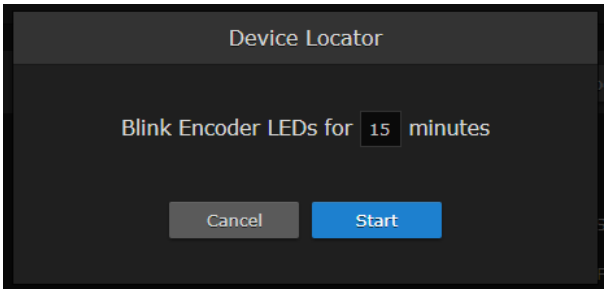
To view status information:

1. Click the **Administration** icon on the toolbar.
   The Administration Status page opens to the Status page.



   The Status settings are read-only. For details, see Status Settings.
2. To display a snapshot of system information, see Taking a System Snapshot.

3. To initiate blinking of the status and TX leds, click **Locate**. On the Device Locator dialog, adjust the time allowed to blink the encoder LEDs and click **Start**.



> **Note**
>
> The blinking can last from 1 minute to 1 hour; the default is 15 minutes.

4. To reboot the encoder, see Rebooting the Encoder.

Status Settings

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

Status Setting	Description/Values
Card Status	OK (or error message if applicable).
Card Type	The type of device, e.g., Makito2 Dual-SDI Encoder or Makito2 Decoder.
Part Number	The Haivision part number for the encoder or decoder, e.g., B-292E-HDSDI2
Serial Number	The serial number for this appliance or card.
Firmware Version	The firmware version of the device, e.g., v2.2-47
Firmware Date	The firmware release date.
Firmware Options	(If applicable) Firmware options installed, e.g., KLV-COT (Metadata Capture KLV & COT) or SRT.
Hardware Version	The hardware version of the device.
Hardware Compatibility	-001G (basic card assembly).
Mezzanine	(applicable hardware only) Indicates whether the mezzanine board is present.
Mezzanine Type	(applicable hardware only) The type of mezzanine board, e.g., HEVC Encoder.
CPLD Version	The CPLD version of the device.
Boot Version	The Boot version of the device.
System Uptime	The length of time the encoder or decoder has been "up" and running (e.g., 1 day 03:42:03).

Status Setting	Description/Values
Encoding Chipset Load	(Encoder only) The combined video encoding processor usage in percentage% (combining both Hi and Lo streams).
Temperature	The current board temperature in degrees Celsius.

Rebooting the Encoder

To reboot the Encoder:

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

Tip

You can also reboot the encoder from the Network Settings page. See Configuring Network Settings.

Taking a System Snapshot

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

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

To take a system snapshot:

1. From the Status page, click **System Snapshot**.
   The system will generate a snapshot of system information in a new window, as shown in the following example:

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

--------------------------------------------------------------------------------
Credentials:
--------------------------------------------------------------------------------
uid=500(admin) gid=511(haiadmin) groups=510(haisecur),511(haiadmin),512(haioper)

--------------------------------------------------------------------------------
Local Time:
--------------------------------------------------------------------------------
Wed Mar  7 15:36:08 EST 2018

--------------------------------------------------------------------------------
Universal Time:
--------------------------------------------------------------------------------
Wed Mar  7 20:36:08 UTC 2018

--------------------------------------------------------------------------------
System UP Time:
--------------------------------------------------------------------------------
 15:36:08 up 9 days,  5:21,  0 users,  load average: 0.15, 0.07, 0.05

--------------------------------------------------------------------------------
Manufacturing Information:
--------------------------------------------------------------------------------
MAC Address   : 5c:77:57:00:32:97
Serial Number : HAI-031304010042
Boot Revision : U-Boot 2010.06 (Feb 26 2014 - 10:41:13)-MakitoX 0.9.13
Nand          : MT29F16G08ABABAWP

--------------------------------------------------------------------------------
Card Temperature:
--------------------------------------------------------------------------------
Temperature Status:
  Current Temperature   : 62 Celsius measured 1s ago
  Maximum Temperature   : 63 Celsius measured 9d5h1m26s ago
  Minimum Temperature   : 59 Celsius measured 8d2h3m13s ago
Debug Statistics:
  Invalid Readings      : 0
  Discarded Deltas      : 0

--------------------------------------------------------------------------------
System Information:
--------------------------------------------------------------------------------
Card Type              : "Makito2 Dual-SDI Encoder"
Part Number            : B-292E-SDI2-FS
Serial Number          : HAI-031304010042
MAC Address            : 5c:77:57:00:32:97
Firmware Version       : 2.2.1-27
Firmware Date          : "Feb 22 2018"
Firmware Time          : "16:52:01"
Firmware Options       : "KLV-COT, SRT"
Hardware Version       : A-
Hardware Compatibility : -001G
Mezzanine              : Present
Mezzanine Type         : "Storage (MSATA Fixed)"
CPLD Version           : 5 (Official, Internal flash)
Boot Version           : "U-Boot 2010.06 (Feb 26 2014 - 10:41:13)-MakitoX 0.9.13"

--------------------------------------------------------------------------------
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)
||/ Name            Version        Description
+++-===============-==============-============================================
ii  makitox-base    2.2.1-27       MakitoX Base
ii  makitox-boam    2.2.1-27       Base Operation and Management
ii  makitox-enc     2.2.1-27       MakitoX Encoder
ii  makitox-help    2.2.1-27       MakitoX on-line help
ii  makitox-prepare 2.2.1-27       MakitoX Pre-installation Checks
ii  makitox-snmp    2.2.1-27       Simple network management.
```

2. Save the file.

Tip

You can also take a system snapshot from the CLI using the system_snapshot.sh command.

Saving and Loading Presets

Each Makito X is configured by users' selecting and setting values of applicable settings, such as encoder or 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 recall these configurations settings to apply to other streams.

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

Note

Presets do not include System Administration (e.g., Network) or Security settings.

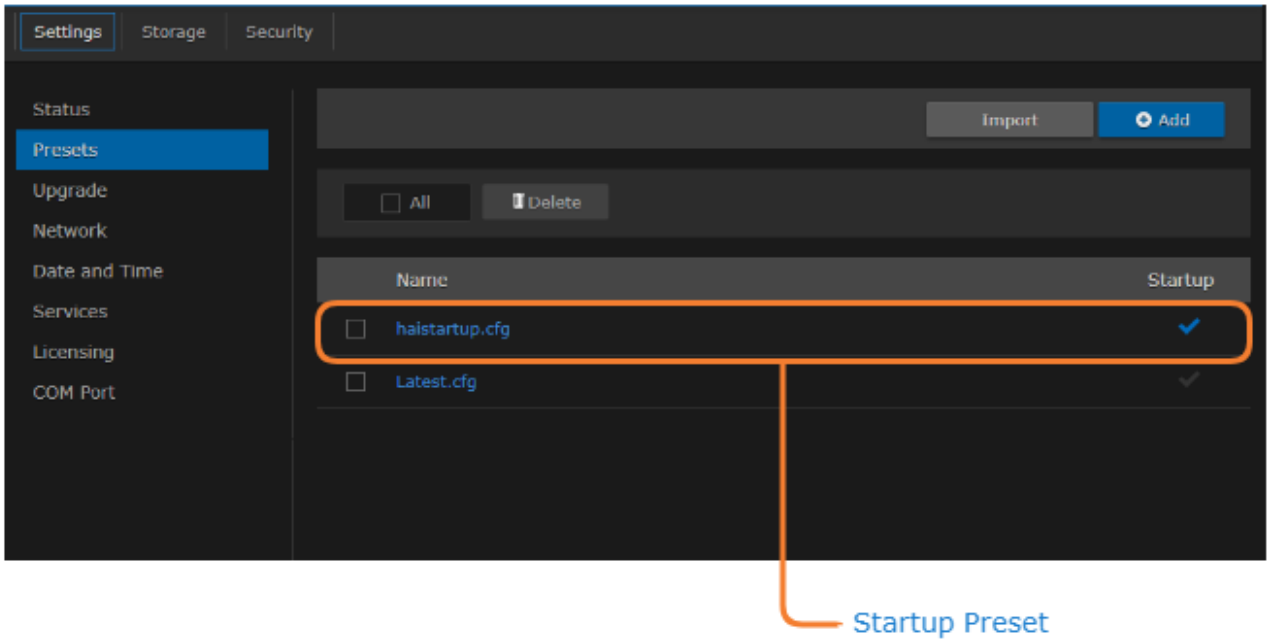
From the Presets page, you can view the list of saved presets, load a saved preset, and save the current settings as a preset. You can also view the contents of a preset file, delete a preset, and select the preset to load at startup.

Note

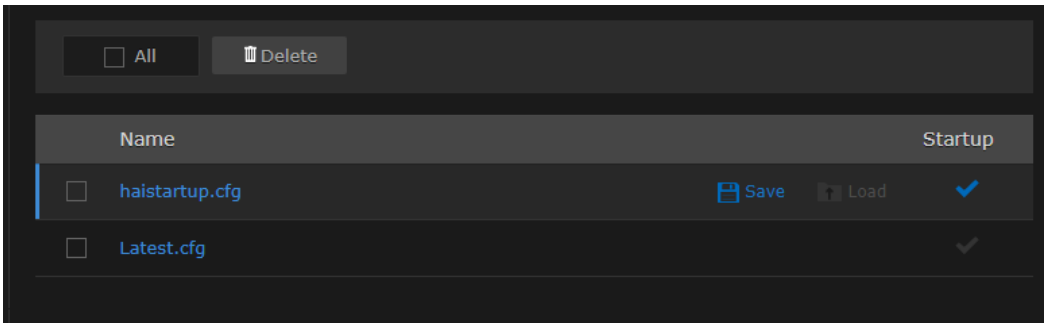
A warning indication appears in the title bar on systems with unsaved configurations. The indication is displayed when a user logs in or out of a Makito X when the current configuration has not been saved in a preset.

To view and manage presets:

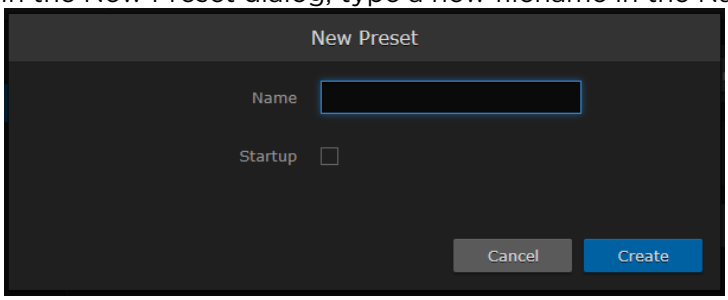
1. On the Administration page, click **Settings** on the navigation bar and **Presets** on the sidebar.
2. The Presets page opens displaying the list of saved presets for the encoder.
   The startup preset is indicated with a blue check.



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

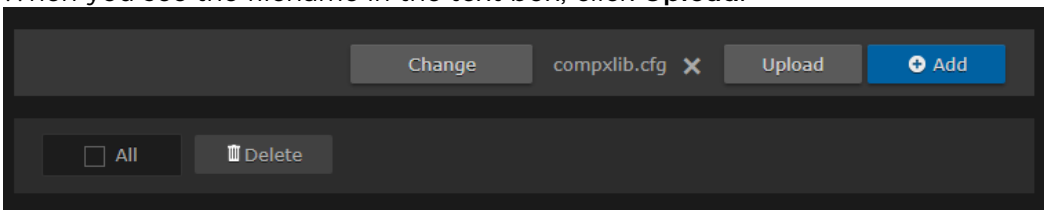


4. To select an existing preset to load at startup, hover over the preset row and click the (grayed out) checkmark under **Startup**.
5. To save the current settings as a new preset, click **Add**.
   a. In the New Preset dialog, type a new filename in the Name text box.



   b. To select this preset to load at startup, check the Startup checkbox.
   c. Click Create.
6. To save the current settings as an existing preset, hover over the preset row and click **Save**. You can (optionally) check the **Startup** checkmark.
7. To save the preset as a text file to view or export to other Makito X encoders, click the preset name and save it in the Save As dialog. Note that the file is in Unix format.

8. To import a preset, for example, from another Makito X encoder, click **Import** and select the file in the Open File dialog box.
9. When you see the filename in the text box, click **Upload**.



> **Tip**
>
> To select a different preset file, click Change. To remove the selection, click the ✕ icon.

10. To delete one or more presets, check the checkbox next to one or more preset names (or check **All**) and click **Delete** on the Content toolbar.

Installing Firmware Upgrades

Important

We recommend that upgrades to a new version occur in a stepwise fashion (i.e., 1.0.x -> 1.1.x -> 1.2.x -> 1.3.x -> 1.4.x -> 1.5.x).

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.

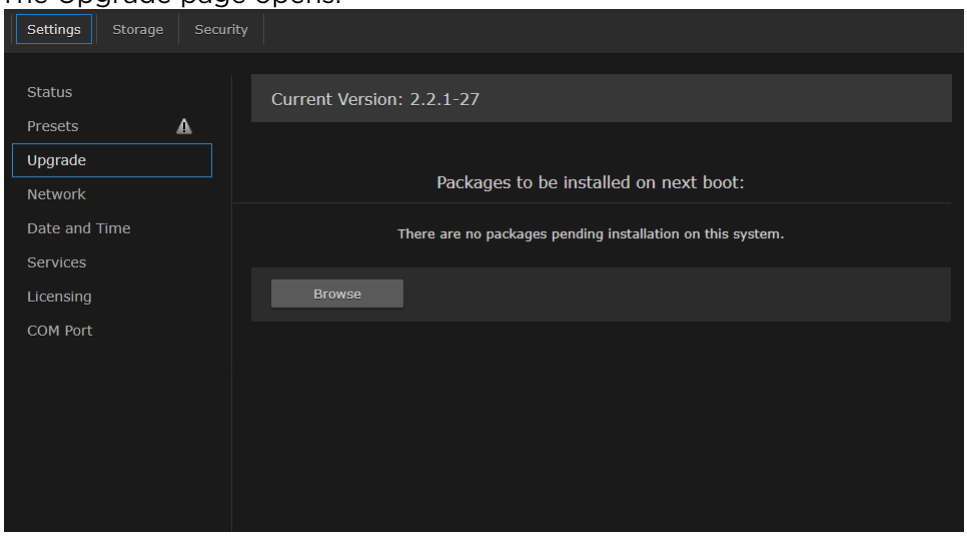
When a firmware upgrade becomes available, you can easily install it from the Web interface. You will first need to copy the upgrade file to your local computer or network.

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.

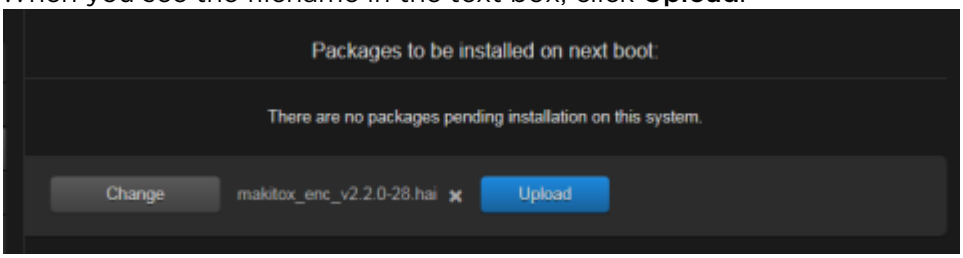
To install a firmware upgrade:

1. On the Administration page, click **Settings** on the navigation bar and **Upgrade** on the sidebar.
2. The Upgrade page opens.



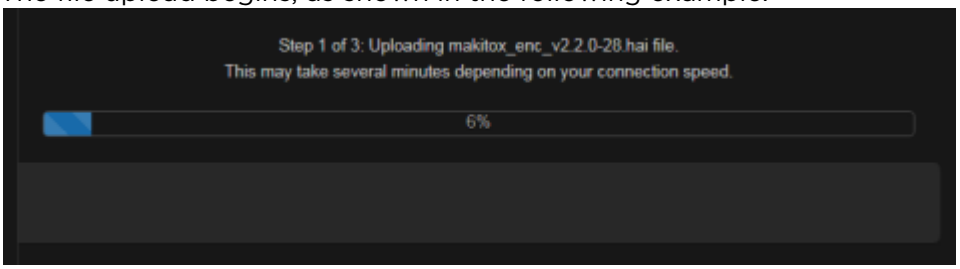
Click **Browse** and select the file in the Open File dialog box.

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



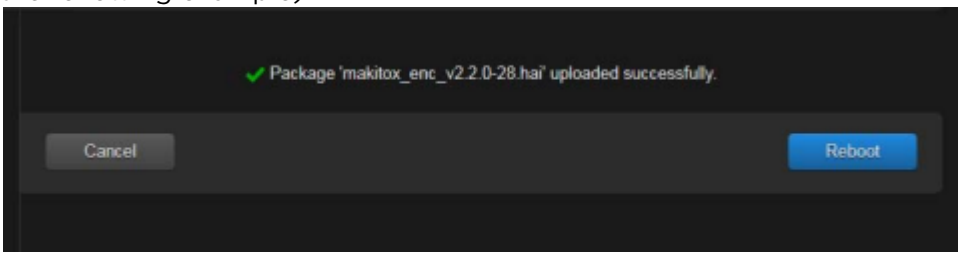
> **Tip**
>
> To select a different file, click **Change**.

The file upload begins, as shown in the following example.



> **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.

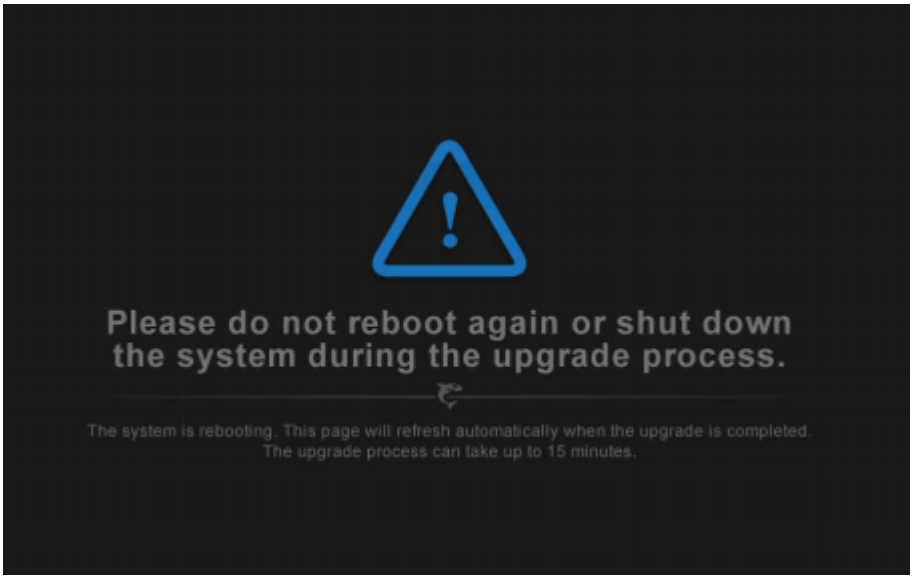
If any of the package components has been modified or is not signed by a valid certificate, the verification will fail and the downloaded package will be discarded.
When the file is uploaded and verified successfully, you will see a confirmation page (as shown in the following example).



4. Click **Reboot**. While the unit is rebooting, the Status LEDs will flash, and you will see a warning page (as shown following).

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.

5. Clear your browser cache after the firmware upgrade.
6. Sign in again in order to access the encoder. For more information, see Signing In to the Web Interface.

Note

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

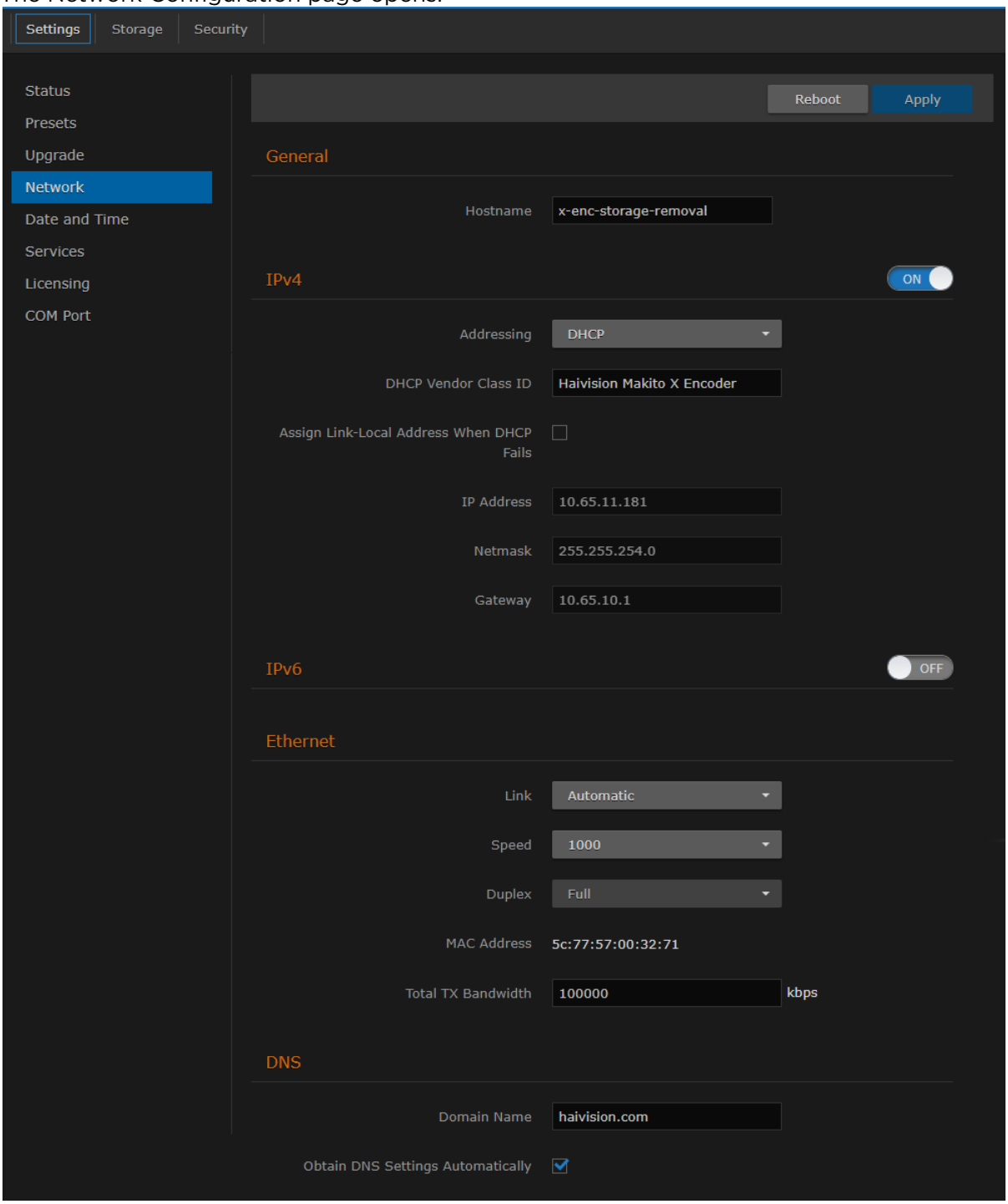
Configuring Network Settings

Caution

When you make changes to the Network settings, be sure to write down the new encoder 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 sign in again in order to access the encoder.
If you are connecting to the Makito X through an IPv4 connection, disabling the IPv4 interface will drop your connection after a reboot. You will need to reconnect using IPv6 or the serial interface (if available).

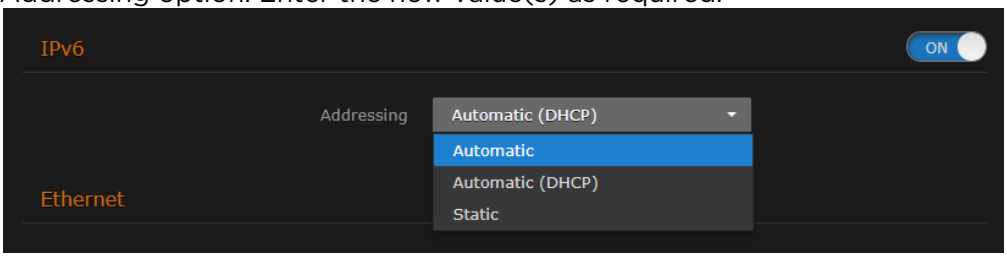
To view and configure the Network settings:

1. On the Administration page, click **Settings** on the navigation bar and **Network** on the sidebar. The Network Configuration page opens.



2. Select or enter the new value(s) in the appropriate field(s). For details, see Network Settings.

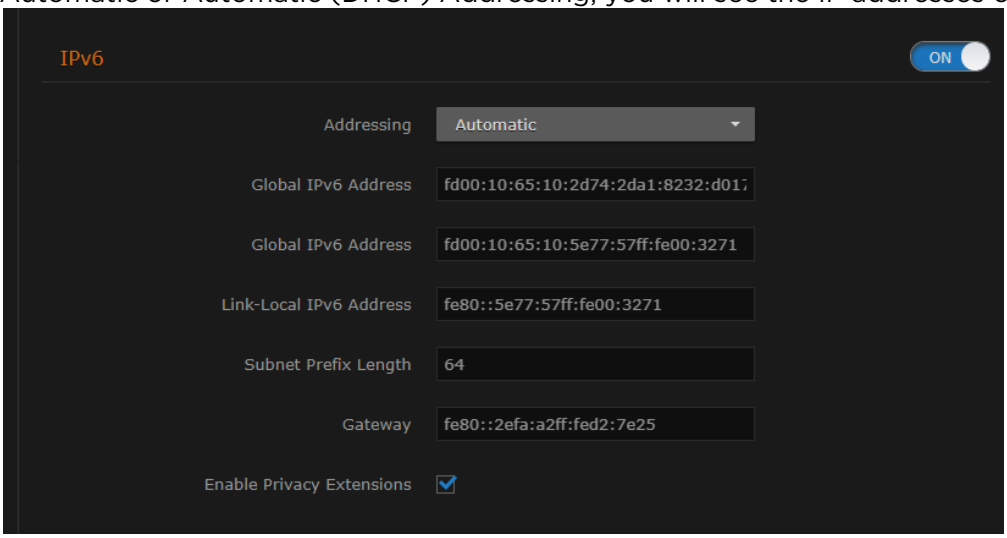
3. To configure IPv4 or IPv6 addressing, toggle the IPv4 or IPv6 button to **On** and select the Addressing option. Enter the new value(s) as required.



4. Click the **Apply** button.
5. Click the **Reboot** button.

> **Note**
>
> You must reboot the system for the changes to take effect.

After the encoder reboots, you will be returned to the Sign-In page.
When you open the Network Configuration page again, if you configured the unit using either Automatic or Automatic (DHCP) Addressing, you will see the IP addresses obtained by the system.



Network Settings

The following table lists the shared Encoder-Decoder Network settings:

General

Setting	Description/Values
Hostname	Enter a unique name for the Makito X.
IPv4	When set to On, configures the network to use IPv4 addressing.
IPv6	When set to On, configures the network to use IPv6 addressing.

IPv4

Setting	Description/Values
Addressing	Select DHCP or Static to enable or disable the Dynamic Host Configuration Protocol. **Note** When DHCP is enabled, the Makito X will get an IP Address from a DHCP server on the network. When it is disabled, you must manually enter the device's IP Address, Netmask & Gateway Address.
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 Encoder" or "Haivision Makito X Decoder" (as applicable).
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 Makito X 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.
Decoder-specific	

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.
Resolution	(**Enable IP Address Display** must be enabled) The resolution for the display of the IP address (default = 720p60).

IPv6

Setting	Description/Values
Addressing	Select one of the following options to obtain an IPv6 address for the unit: • Automatic: Uses SLAAC (Stateless Address Autoconfiguration) to obtain IP addresses automatically without the need for a DHCP server • Automatic (DHCP): Enables the Dynamic Host Configuration Protocol to get an IP address from a DHCP server on the network • Static: Use to manually configure the device's IP and gateway addresses.
Global IPv6 Address	Displays the IPv6 Address for the Makito X. This is a unique address that identifies the unit in the IP network. There may be multiple IPv6 addresses on a single interface. If Static Addressing is used, enter an IPv6 address in hexadecimal notation.
Subnet Preflix Length	The Prefix Length in IPv6 is the equivalent of the Subnet Mask in IPv4. However, instead of being expressed in four octets as it is in IPv4, it is expressed as an integer between 1 through 128.
Gateway	Displays the gateway address of the network (typically the address of the network router). If Static Addressing is used, enter a gateway address in hexadecimal notation.
Enable Privacy Extensions	(**Automatic** Addressing only) Check this checkbox to enable SLAAC Privacy Extensions. As documented in RFC 4941 "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", this entails using randomly generated, temporary, global scope IPv6 addresses that are regularly discarded and replaced with different addresses.
Link-Local IPv6 Address	A link-local address is an Internet Protocol (IP) unicast address intended to be used only to connect to the hosts on the same network. A link-local address starts with fe80: The link-local address is always automatically assigned; you cannot configure it.

Ethernet

Setting	Description/Values
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.
Encoder-specific	
Total TX Bandwidth Limit	(Encoder only) The maximum transmit bandwidth for the Makito X in kbps. Specifies the bandwidth "ceiling" for the Ethernet port.

DNS Settings

Setting	Description/Values
Domain Name	Enter the domain for the Makito X.
Obtain DNS Settings Automatically	(Addressing cannot be **Static**) 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.
DNS Precedence	Select either IPv4 or IPv6 to specify the priority for DNS resolution. On systems with both IPv6 and IPv4 enabled, if users use HOSTNAMES instead of specifying IP addresses when creating connections, the default behavior is to resolve to IPv6 first if it is available.
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 Makito X. mDNS is enabled on units shipped from the factory or reset to factory defaults to allow them to advertise their existence. A user can then click **Locate** (Status page) to start the Status and TX or RX LEDs flashing in order to discover the location of the device, for example, within a large server room.
mDNS Identifier	(Optional) Enter a unique name for the Makito X. By default, the system creates a unique name “MakitoXD (%HOSTNAME%)”) for the device.

Related Topics

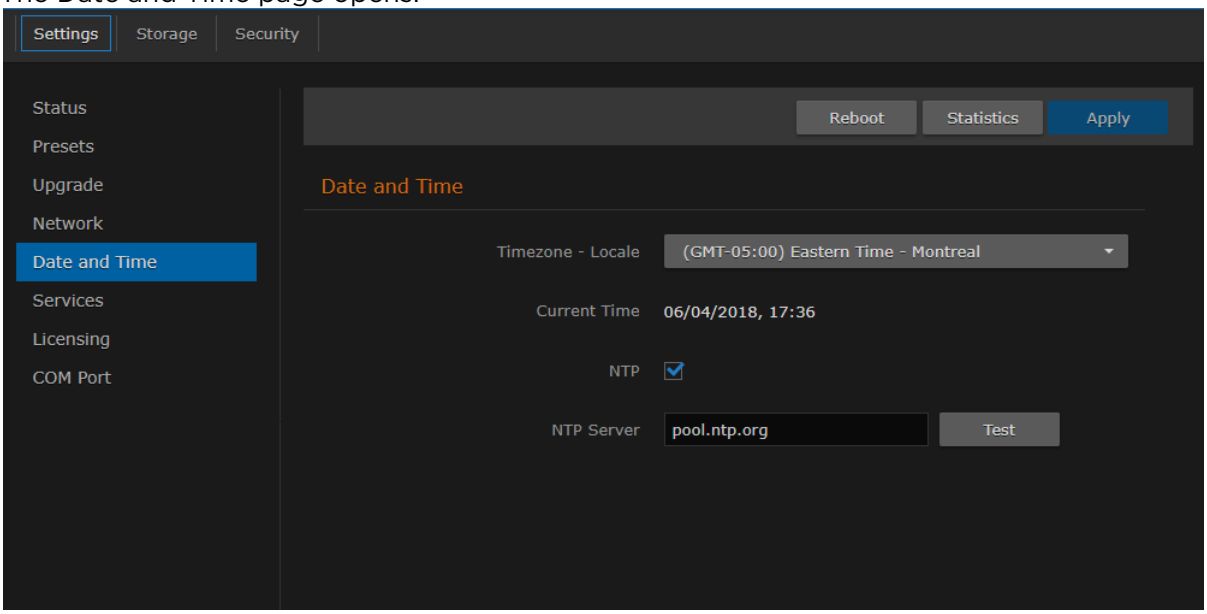
- Configuring Network Settings
- Viewing System Status Information

Configuring Date and Time

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

To view and configure the date and time:

1. On the Administration page, click **Settings** on the navigation bar and **Date and Time** on the sidebar.
   The Date and Time page opens.



2. Select or enter the new value(s) in the appropriate field(s). For details, see Date and Time Settings.
3. To apply your changes, click **Apply**.
4. To validate that the NTP server is reachable, click **Test** next to the NTP server field.
5. To view statistics for the NTP server, click **Statistics**. For details, see NTP Statistics.

Date and Time Settings

The following table lists the Date and Time settings:

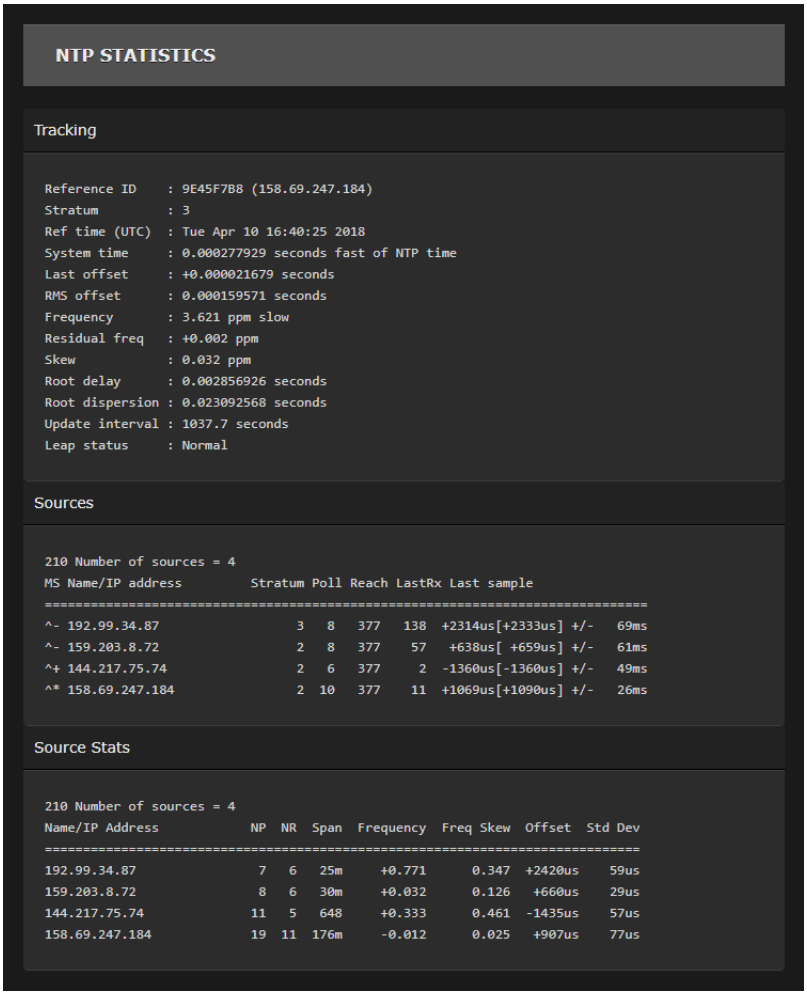
Date and Time Setting	Description/Values
Timezone-Locale	Select the desired time zone and corresponding city. **Note** The times are based on hours added to or subtracted from Greenwich Mean Time (GMT).
Current Time	(Read-only) The current local date and time.
NTP	Check this checkbox to connect to a Network Time Protocol (NTP) server to synchronize the encoder or 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.
Test	If NTP is enabled, click to validate that the NTP server is reachable.
Statistics	If NTP is enabled, click to display tracking and source information, and source statistics for the NTP server.

Related Topics

- NTP Statistics

NTP Statistics

Following is an example of the NTP Statistics:



NTP STATISTICS

Tracking

```
Reference ID    : 9E45F7B8 (158.69.247.184)
Stratum         : 3
Ref time (UTC)  : Tue Apr 10 16:40:25 2018
System time     : 0.000277929 seconds fast of NTP time
Last offset     : +0.000021679 seconds
RMS offset      : 0.000159571 seconds
Frequency       : 3.621 ppm slow
Residual freq   : +0.002 ppm
Skew            : 0.032 ppm
Root delay      : 0.002856926 seconds
Root dispersion : 0.023092568 seconds
Update interval : 1037.7 seconds
Leap status     : Normal
```

Sources

```
210 Number of sources = 4
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- 192.99.34.87                  3   8   377   138  +2314us[+2333us] +/-   69ms
^- 159.203.8.72                  2   8   377    57   +638us[ +659us] +/-   61ms
^+ 144.217.75.74                 2   6   377     2  -1360us[-1360us] +/-   49ms
^* 158.69.247.184                2  10   377    11  +1069us[+1090us] +/-   26ms
```

Source Stats

```
210 Number of sources = 4
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
==============================================================================
192.99.34.87                7   6   25m     +0.771      0.347  +2420us    59us
159.203.8.72                8   6   30m     +0.032      0.126   +660us    29us
144.217.75.74              11   5   648     +0.333      0.461  -1435us    57us
158.69.247.184             19  11  176m     -0.012      0.025   +907us    77us
```

Enabling and Disabling Network Services

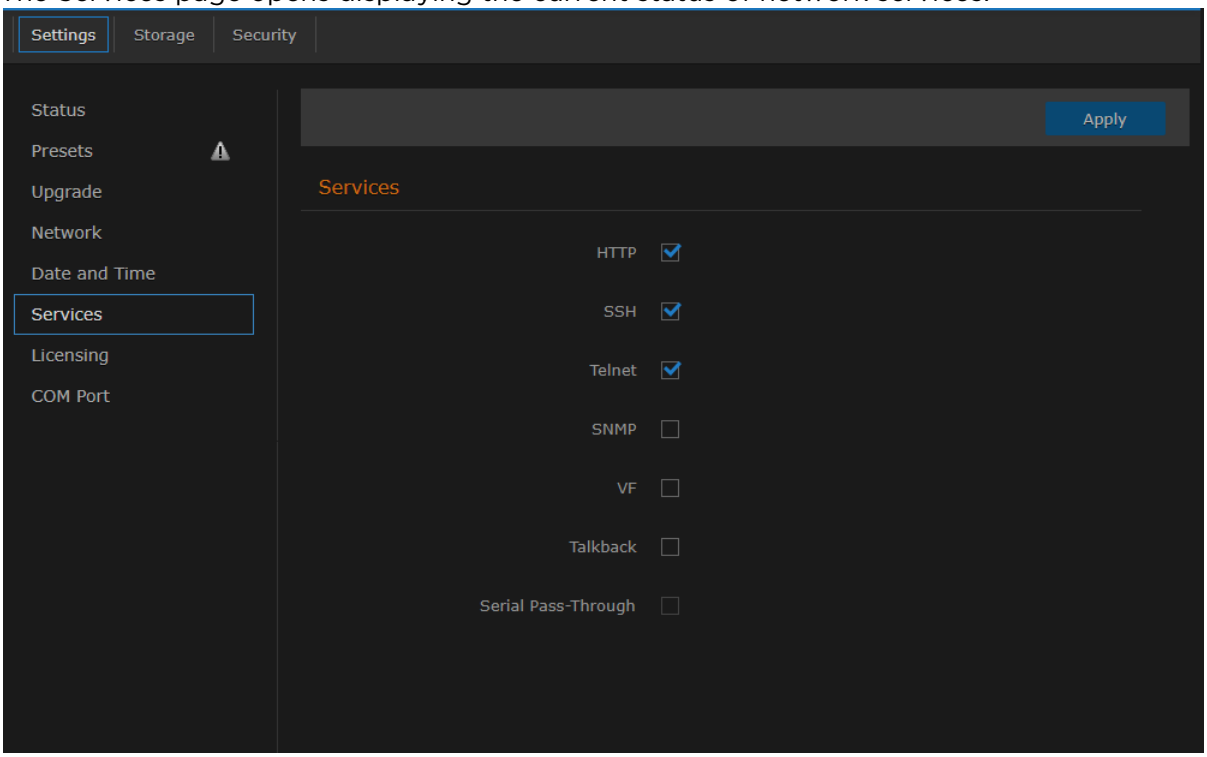
For security purposes, an administrator may need to stop one or more network services from accessing the Makito X. From the Services page, you can enable and disable network services, including HTTP, SSH, Telnet, SNMP, VF, and Talkback.

Important

In order to optimize your encoder's performance, it is recommended that *only* the required network services be enabled. Please review the network services to make sure services used for your application are enabled or disabled as appropriate. For encoders integrated within a Furnace environment, "VF" must be enabled.

To enable or disable network services:

1. On the Administration page, click **Settings** on the navigation bar and **Services** on the sidebar. The Services page opens displaying the current status of network services.



2. To enable or disable a service, check or clear the associated checkbox. For details, see Service Settings.
3. To apply your changes, click **Apply**. The service(s) will be stopped or started immediately.

Important

If the COM1 serial port is used for metadata capture, and all remote management interfaces (HTTP, telnet, SSH, and SNMP) are disabled, the only way to re-enable these services will be by a Factory Reset. (For details, see Resetting the Encoder.) Once the serial port is dedicated for metadata capture, it is no longer usable for CLI management.

Related Topics

- service (CLI command0

Service Settings

The configurable Services are as follows:

Network Services

Service	Description/Values
HTTP	Hypertext Transfer Protocol, used for Web browsers acting as a client. **Note** Only secured HTTP (HTTPS) is supported. See Managing Certificates (Encoder) or Managing Certificates (Decoder) 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 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.
Haivision EMS	EMS (Element Management System) allows simple management of Haivision-only devices.

Encoder-specific

Service	Description/Values
VF	Protocol used for communication between the encoder and Furnace servers. Note that VF Pilot provides access to encoder configuration settings.
Talkback	Audio Talkback (a Makito X feature) allows end users monitoring a streaming session to "talk back" to individuals at the video source, via a speaker or headphones connected to the encoder. For details, see Audio Talkback.

Service	Description/Values
Serial Pass-Through	Bi-directional serial pass-through for controlling serially attached devices such as PTZ controlled cameras. Both RS-232 and RS422 are supported. **Note** The COM Port Mode must first be set to Pass-Through (see **Managing the COM Port**).
Port	(Serial Pass-Through must be enabled) Specifies the TCP port that the Makito X will listen on for remote commands.
RTSP	Enables streaming of video feeds from the Makito X encoder to a Milestone server for archiving and analysis using the RTSP protocol.
ONVIF	Enables the ONVIF management API to send commands from the Milestone XProtect video management software (VMS) to the Makito X encoder.

Decoder-specific

Service	Description/Values
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.
SAP only	
IPv4 Listening Address	Specifies the multicast IPv4 address on which the SAP service will listen (as defined in RFC 2974). **Note** The Makito X decoder listens for SAP on three different addresses when Automatic is selected: • 224.2.127.254 (IPv4 global scope announcement multicast address) • 239.255.255.255 (IPv4 local scope announcement multicast address) • 239.195.255.255 (IPv4 organization local scope announcement multicast address) The standard IP addresses and ports for multicast SAP announcements are defined in RFC 2974.
IPv6 Listening Address	Specifies the multicast IPv6 address on which the SAP service will listen (as defined in RFC 2974). **Note** The Makito X decoder listens to `FF0X::2:7FFE` where X is the 4-bit scope value.
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

- License File Errors

Feature licensing allows you to add new functionality to already deployed systems. For example, you may add features such as the following to a base Makito X.

Feature	SKU
KLV	SWO-292E-KLV
KLV&CoT	SWO-292E-KLV-COT

To acquire a new license, please contact your Authorized Reseller or Haivision at: **https://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.

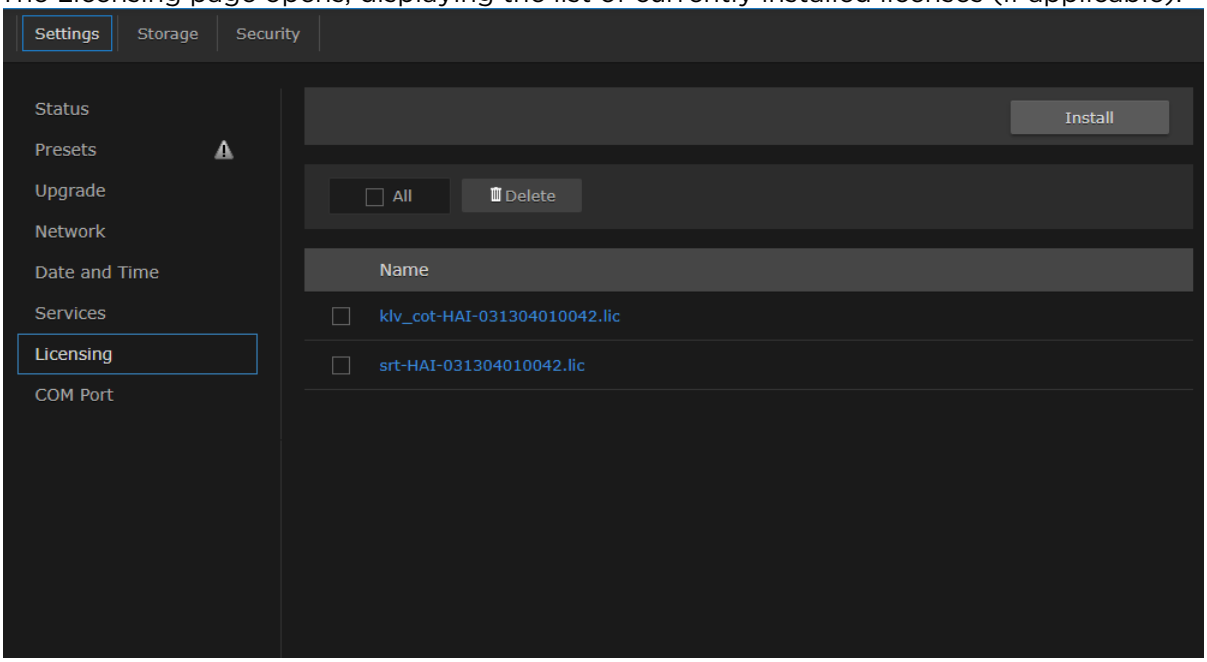
This section provides instructions to install a license from the Web interface as well as view current licenses on your system.

Caution

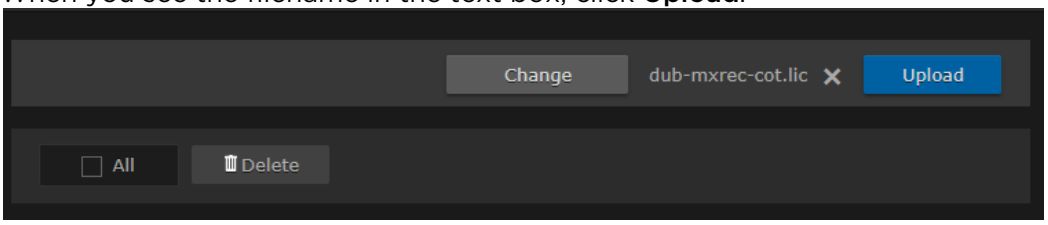
- Do not delete existing licenses before uploading the new license.
- New licenses are typically add-ons to complement the base license. You should only delete existing licenses if instructed to do so by Haivision.

To install a license file:

1. On the Administration page, click **Settings** on the navigation bar and **Licensing** on the sidebar. The Licensing page opens, displaying the list of currently installed licenses (if applicable).



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**.



4. To apply your changes, click the **Reboot** button. The encoder 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.

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.

Related Topics

- license (CLI command)

Managing the COM Port

> **Note**
>
> The COM Port page only accessible to administrators. However, operators can configure the COM port settings from the Metadata page when the COM port is in Metadata mode.

The Makito X with SDI provides a serial interface that you can use to connect to a computer for management of the encoder. The COM Port page displays the serial COM port settings and provides the option to switch from Metadata to Management mode.

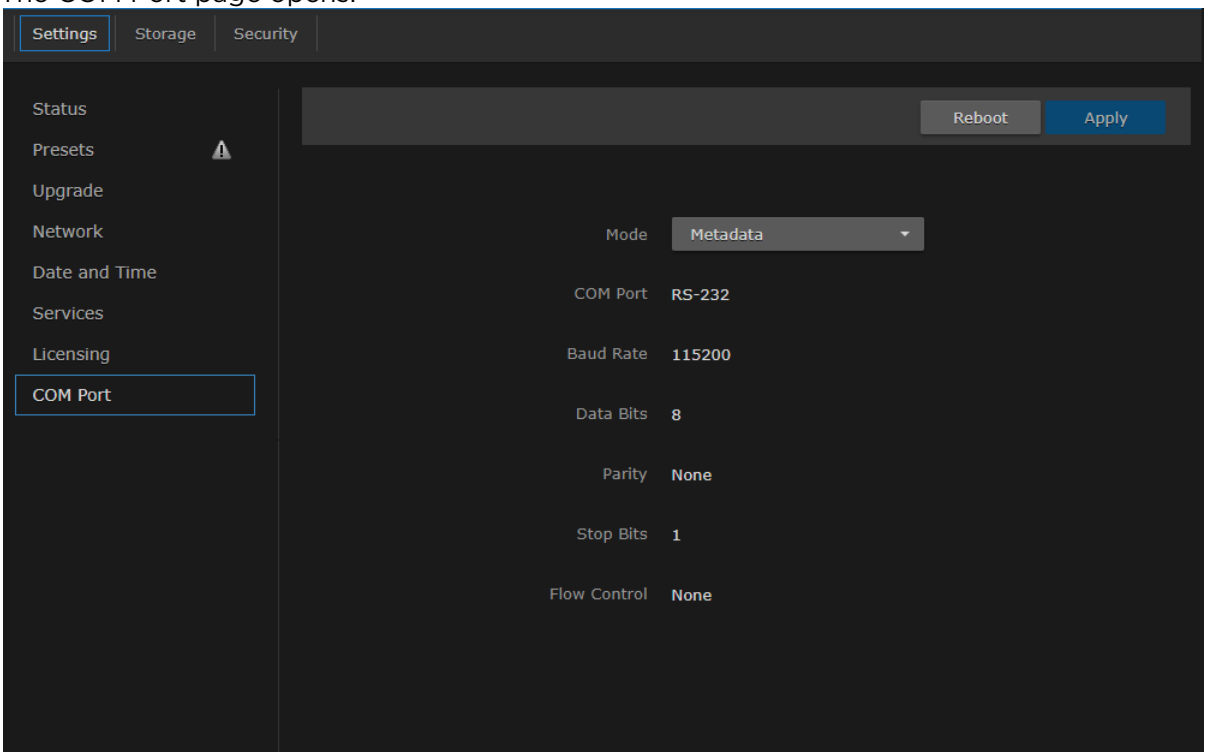
On systems with the Metadata Capture option installed, you can use the serial COM port interface to capture either KLV or CoT metadata. For more information, see Configuring Metadata Capture.

In order to configure the COM port settings to capture metadata, you need to set the COM Port Mode to Metadata and then reboot the encoder. You can then configure the COM port settings from the Metadata page.

In order to configure serial pass-through to control devices such as PTZ cameras, you need to set the COM Port Mode to Pass-Through and then reboot the encoder.

To manage the COM Port settings:

1. On the Administration page, click **Settings** on the navigation bar and **COM Port** on the sidebar. The COM Port page opens.



2. (If applicable) Select **Metadata** from the COM Port **Mode** drop-down list.
3. To apply your change, click **Apply**.
4. Click **Reboot**. The changes will take effect after the reboot has completed.

Related Topics

- For information on connecting a computer to the COM1 port, see **Connecting the Encoder to the Network and a Computer**.

COM Port Settings

Note

With the exception of the COM Port Mode, the COM Port settings are read-only. For information on modifying the COM Port settings, see Metadata Settings.

COM Port Setting	Default	Description/Values
Mode	Management	Selects the type of activity: • Management • Metadata (required in order to configure the Metadata settings) • Pass-Through (required to control serially attached devices such as PTZ controlled cameras). **Note** You must reboot the encoder when you change the Mode.
COM Port	RS-232	(Read-only) The type of Serial interface: • RS-232 or • RS-422
Baud Rate	115200	(Read-only) The COM Port bitrate.
Data Bits	8	(Read-only) The COM Port databits: 8
Parity	None	(Read-only) The COM Port parity: None
Stop Bits	1	(Read-only) The COM Port stopbits: 1
Flow Control	None	(Read-only) The COM Port flow control: None

Managing Storage Drives

Important

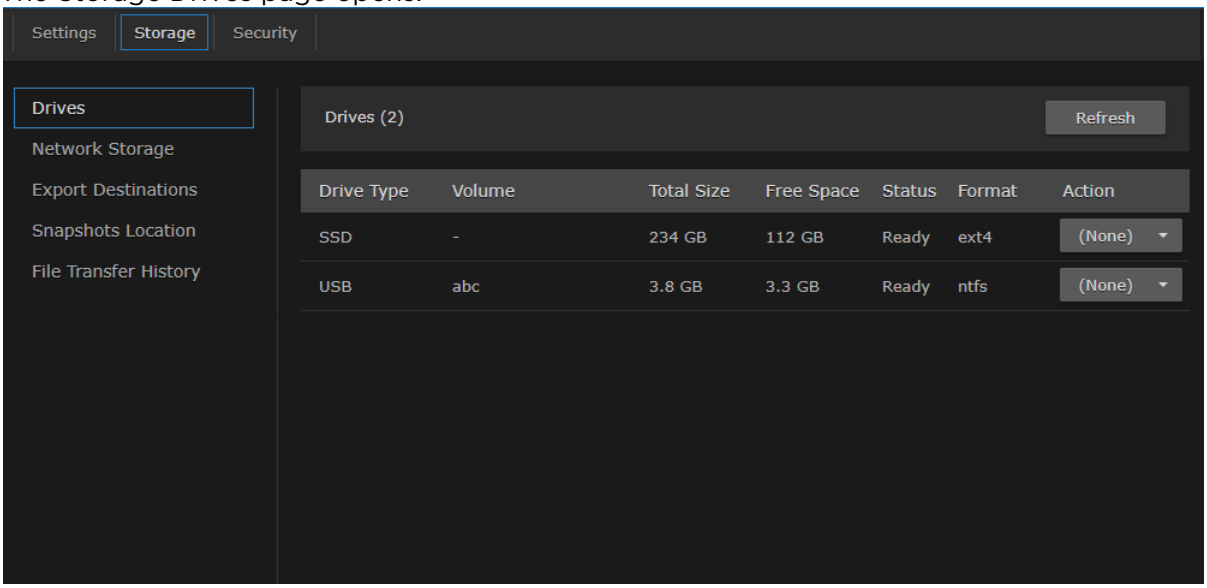
The Drives page is only available on the Makito X with Storage dual-height model.

From the Drives page, you can view and manage storage media for the encoder. This includes removable devices such as SD cards, USB thumb drives, or removable SSDs. From here you can format, mount or unmount storage drives.

- Formatting a drive initializes the file structure and removes all existing data.
- Mounting makes the drive available to the system (e.g., to store data).
- Ejecting unmounts the drive in order to allow it to be removed (physically) from the unit.

To manage storage drives:

1. On the Administration page, click **Storage** on the navigation bar and **Drives** on the sidebar. The Storage Drives page opens.



2. To change the status for a storage drive, click the drop-down list under **Action** and select either Format, Mount or Eject (as applicable).

Note

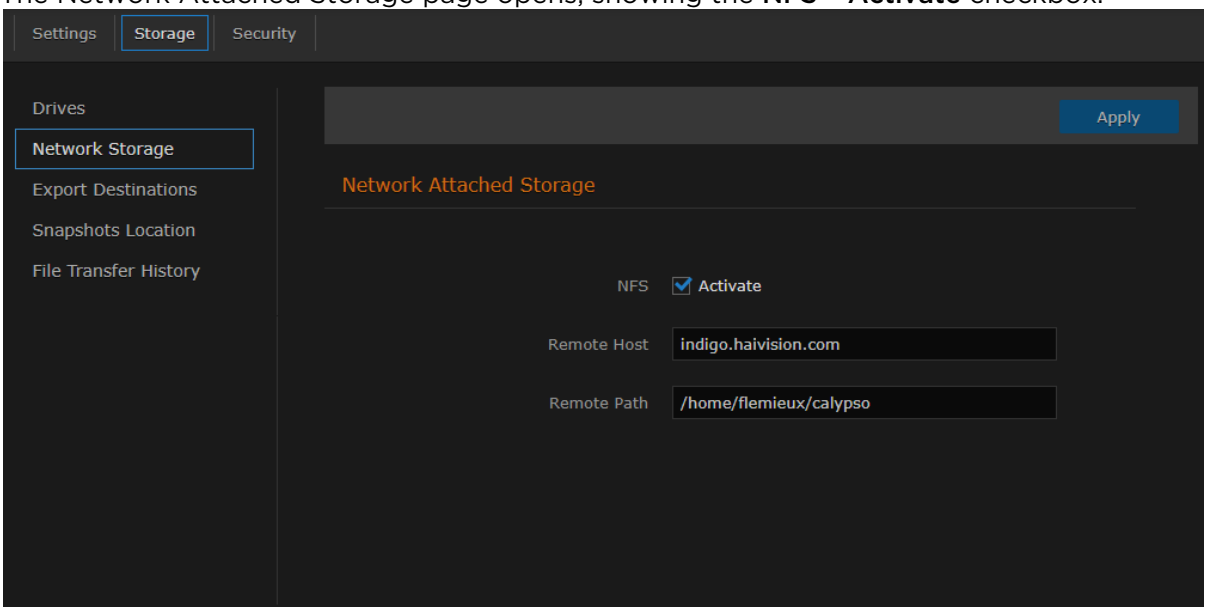
The Makito X does not support formatting of SD drives.

Managing Network Storage

Network Storage enables you to move video storage from your Makito X to NetworkAttached Storage through an NFS connection. This is useful for storing snapshots or (with the Makito X with Storage) for copying recordings after they are completed.

To configure network attached storage:

1. On the Administration page, click **Storage** on the navigation bar and **Network Storage** on the sidebar.
   The Network Attached Storage page opens, showing the **NFS – Activate** checkbox.



2. To connect to an NFS server, check the checkbox.
3. Fill in the remote host IP address and path.
4. To apply your changes, click **Apply**.
   The Network-Attached Storage is now available.

Network Storage Settings

The configurable Network Attached Storage settings are as follows:

Network Storage Setting	Description
NFS – Activate	Check this checkbox to activate Network Attached Storage.
Remote Host	Enter the NFS server hostname or its IP address in dotteddecimal format.
Remote Path	Enter the NFS server path.

Configuring Export Destinations

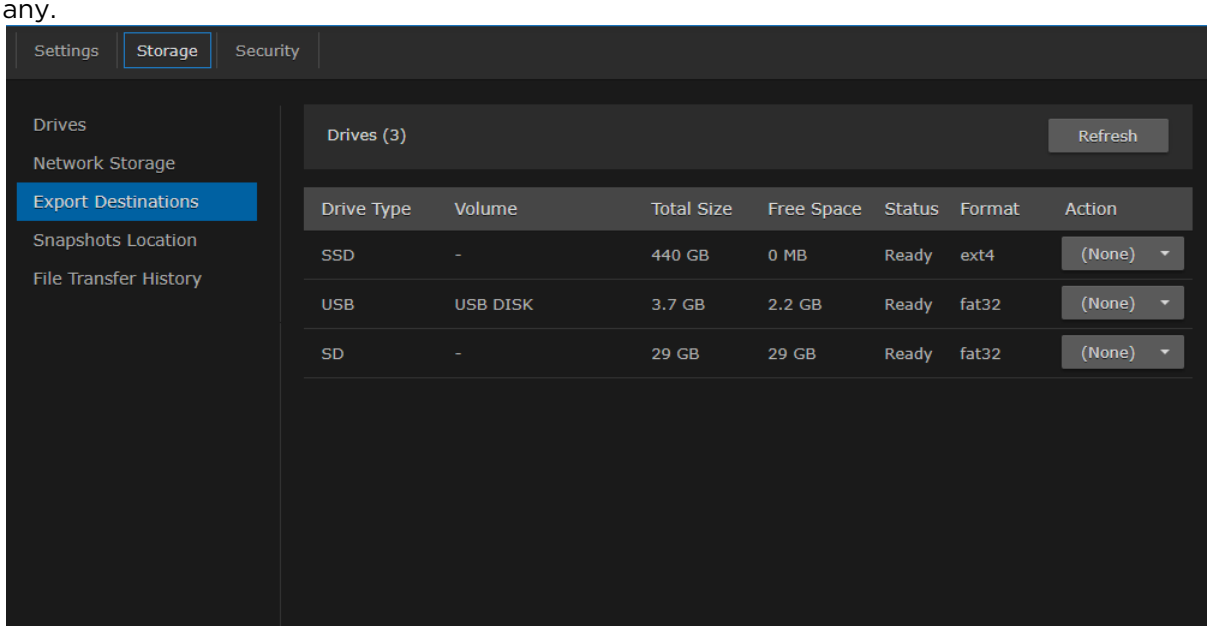
Important

Export Destinations is only available on the Makito X with Storage dual-height model.

When setting up Makito X, you can add export destinations to be available to transfer video and metadata to FTP/FTPS servers and the Haivision Video Cloud (HVC) platform. From the Export Destinations page, you can add destinations, edit settings for destinations, and delete destinations.

To view and manage export destinations:

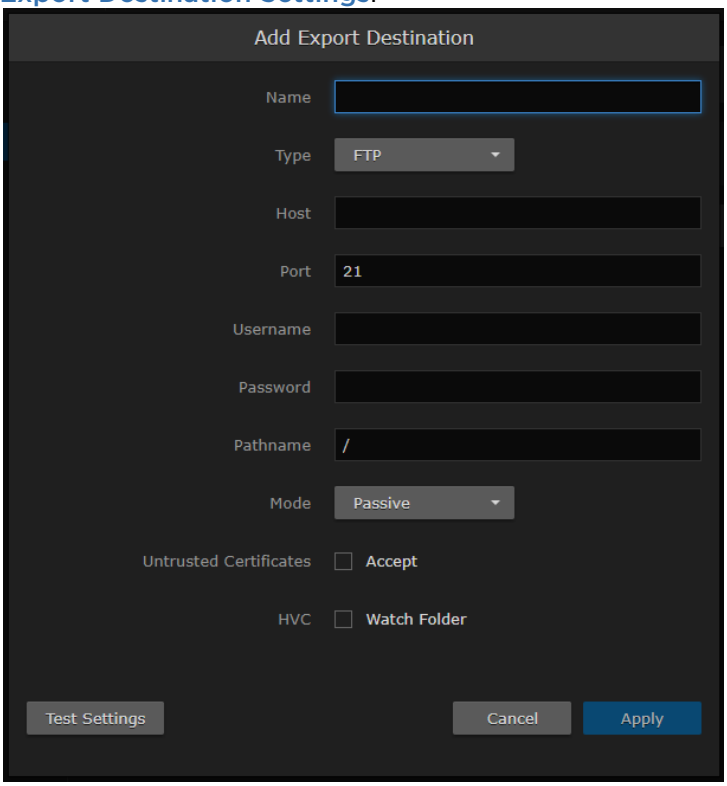
1. On the Administration page, click **Storage** on the navigation bar and **Export Destinations** on the sidebar.
   The Export Destinations page opens, displaying the list of defined destinations for your platform, if any.



To add an export destination:

1. From the Export Destinations page, click **Destinations**.

2. On the Add Export Destination dialog, enter or select the value(s) to define the destination. See Export Destination Settings.



3. To test the connection, click **Test Settings**.

> **Note**
>
> You do not need to save in order to test settings.

4. Click **Add Destination**. The new export destination will be added to the list.

Export Destination Settings

The following table lists the Export Destination configuration settings:

Export Destination Setting	Default	Description/Values
Name	n/a	Enter a name for the destination. This name will be selectable on the Export Video list.
Type	FTP	Select the protocol type, either: • FTP: File Transfer Protocol • FTPS: FTP with explicit Transport Layer Security (TLS)
Host	n/a	Type in the server's DNS host name or IP address for the destination.
Port	21	Type in the port number for the destination server.
Username	n/a	Type in your login username for the site.
Password	n/a	Type in your password.
Pathname	n/a	(Optional) Type in the file path to use on the server, or leave blank for the server's default path.
Mode	Passive	Select the FTP data connection mode provided by your FTP administrator, either: • Active: The client tells the server what port it is listening on, and the data connection is established by the server with the client via the specified port. For this to work, there either needs to be no firewalls or the firewalls defined must understand the FTP protocol. • Passive: The client opens two random ports. One port issues a PASV command to inform the server that it is in Passive mode. The server opens a random port and responds to the client. The client uses the second port to establish the data connection with the server via the port specified by the server.
Untrusted Certificates	Do not Accept	Check this checkbox to allow Makito X to connect to an FTPS server that is using an untrusted SSL certificate.
HVC - Watch Folder	Disabled	**Note** This file contains information about recording used by platforms to process files. When files show up here, HVC starts processing.

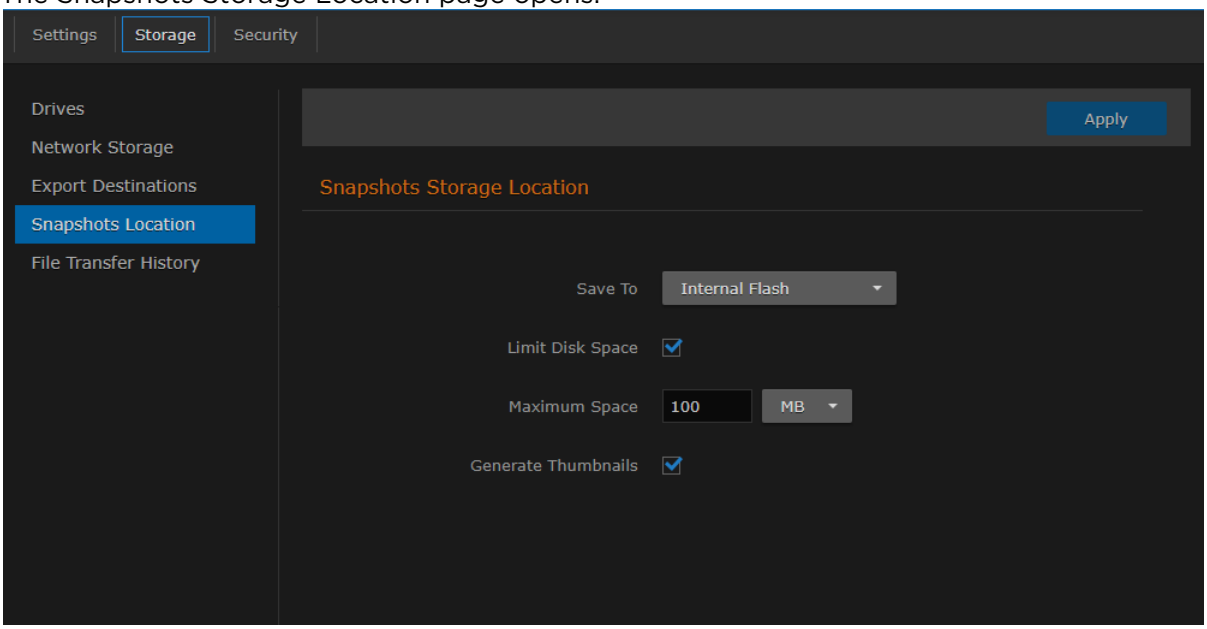
Managing Snapshot Storage Locations

From the Snapshots Storage Location page, you can specify the location where image snapshots are stored. You may choose to store snapshots on removable storage media (if available) as well as define the number and size of snapshots recorded in order to limit or increase the space allocated for snapshot storage.

Snapshots may be stored on the internal NAND storage, or on mSATA/SATA SSD, SD, USB, or NAS-configured storage devices. The snapshot storage destination control is a global parameter.

To view and manage snapshot storage locations:

1. On the Administration page, click **Storage** on the navigation bar and **Snapshots Location** on the sidebar.
   The Snapshots Storage Location page opens.



2. Enter or select the value(s) to define the location. See Snapshots Location Settings.
3. To apply your changes, click **Apply**.

Snapshots Location Settings

The configurable Snapshots Storage Locations settings are as follows:

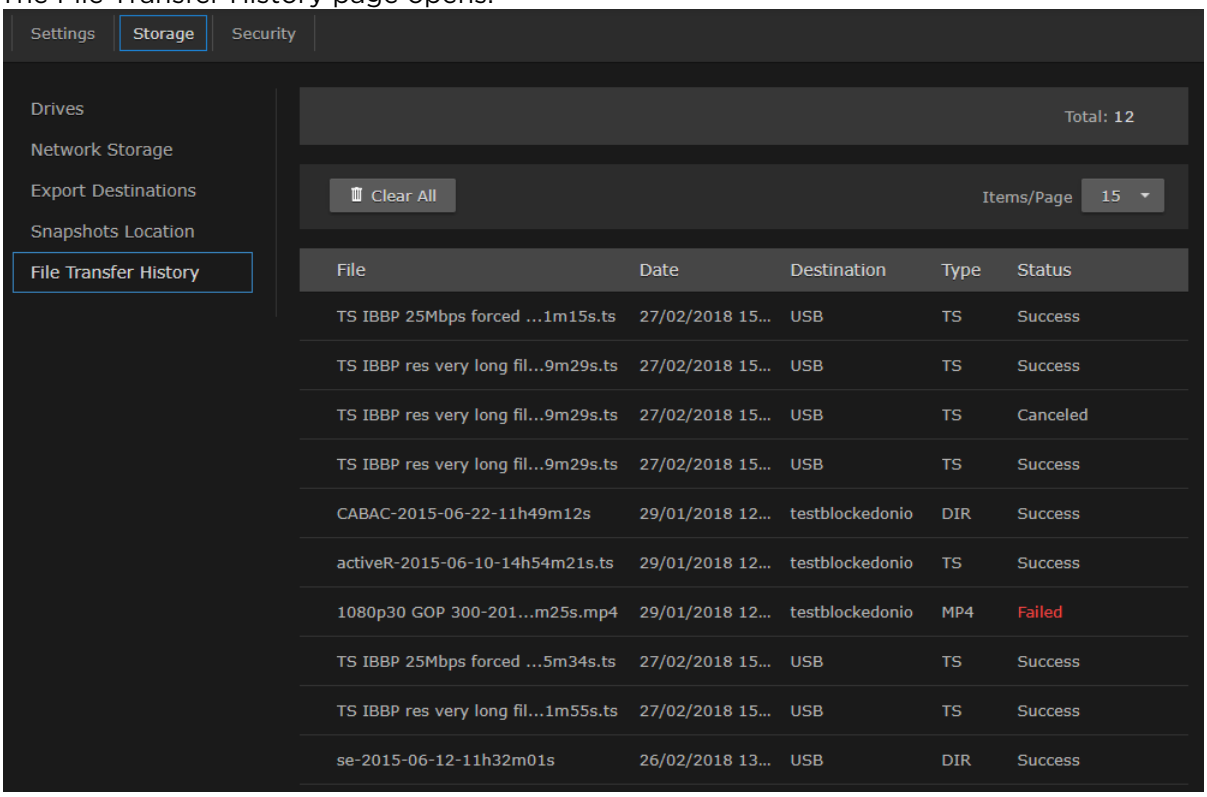
Snapshots Location Setting	Description
Save to	Select the location for snapshot storage: • Internal Flash • Internal SSD (if installed) • USB Drive (if installed) • Network Storage
Limit Disk Space	Check this checkbox to limit the disk space for snapshot storage.
Maximum Space	**Note** For USB or SD cards, you cannot configure a space limit; instead the space available on these devices will be the effective limit.
Generate Thumbnails	Check this checkbox to disable thumbnail generation to speed up snapshot acquisition and storage time.

Managing File Transfer History

> **Note**
>
> File Transfer History is only available on the MakitoX with Storage dual-height model.

To view and manage file transfer history:

1. On the Administration page, click **Storage** on the navigation bar and **File Transfer History** on the sidebar.
   The File Transfer History page opens.



2. To clear the list, click **Clear All**

Managing Users and Security

Note

Unless otherwise indicated, the Administration Security pages are only accessible to administrators.

Topics in This Chapter

- Managing User Accounts
- Managing Messages
- Managing Banners
- Managing Security Policies
- Managing Certificates
- Managing Audits

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**.

Important

Makito X Series devices ship from the factory with only the `admin` account enabled. For security reasons, the two default user accounts (`user` and `operator`) are locked at the factory as well as after a factory reset. An administrator must unlock them and change the passwords to use them for the first time.

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**.

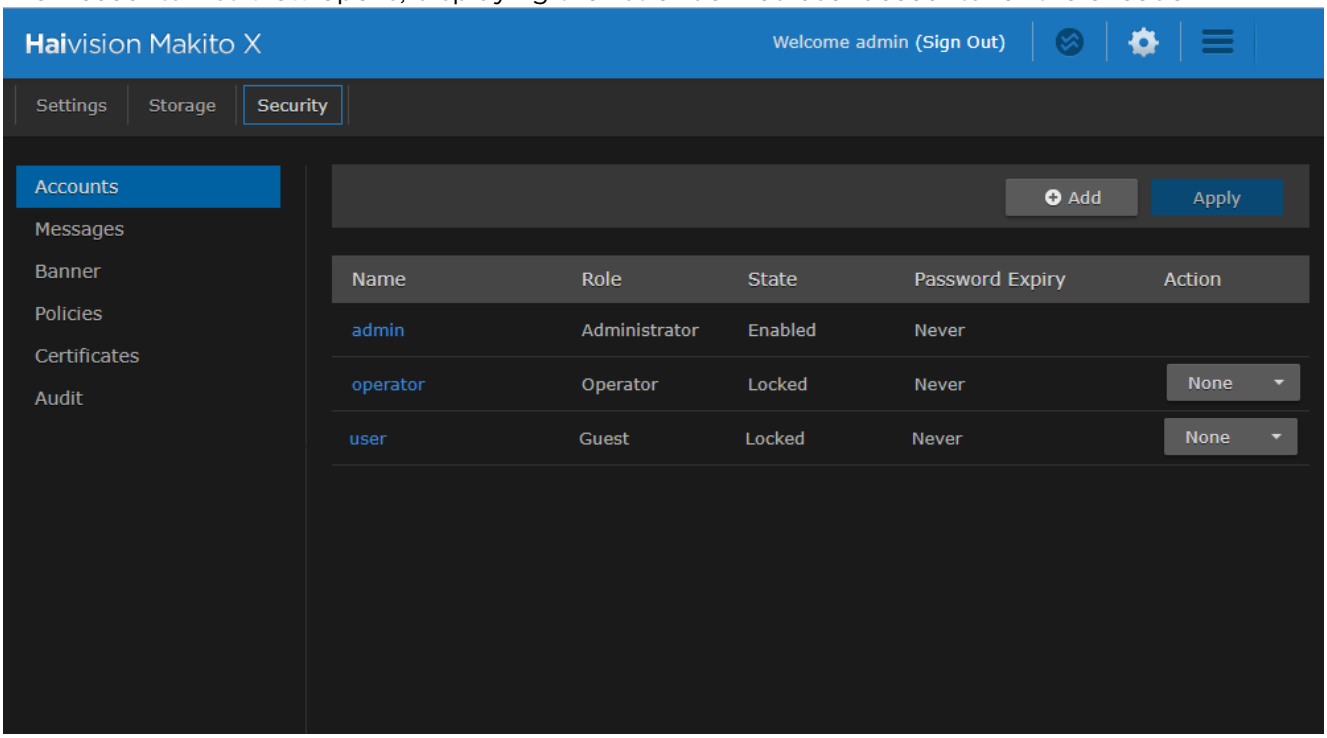
Using system-wide parameters, administrators can configure the allowable password strength and composition (i.e., to force the selection of strong passwords), as well as the periodic change of passwords. The Makito X can also be configured for Web interface and CLI account sessions to log out after an idle session timeout period. The session timeout period is selectable via a system-wide parameter. For details, see **Managing Security Policies**.

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 encoder.

To open the Accounts List View:

1. On the Administration page, click **Security** on the navigation bar.

2. The Accounts List View opens, displaying the list of defined user accounts for the encoder.



   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.
3. 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.
4. To add a new account, click **Add**. For details, see Account Management.
5. 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).
6. To delete an account, click the drop-down menu under **Actions** and select Delete.
7. To apply your changes, click **Apply**. The changes will take effect immediately.

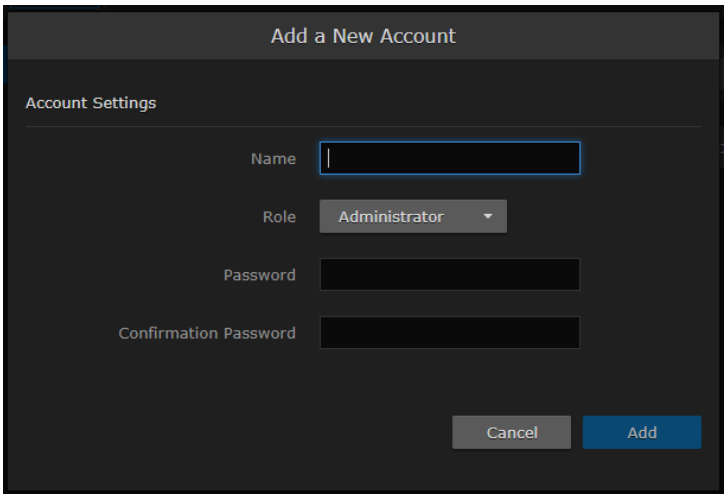
Account Management

> **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:

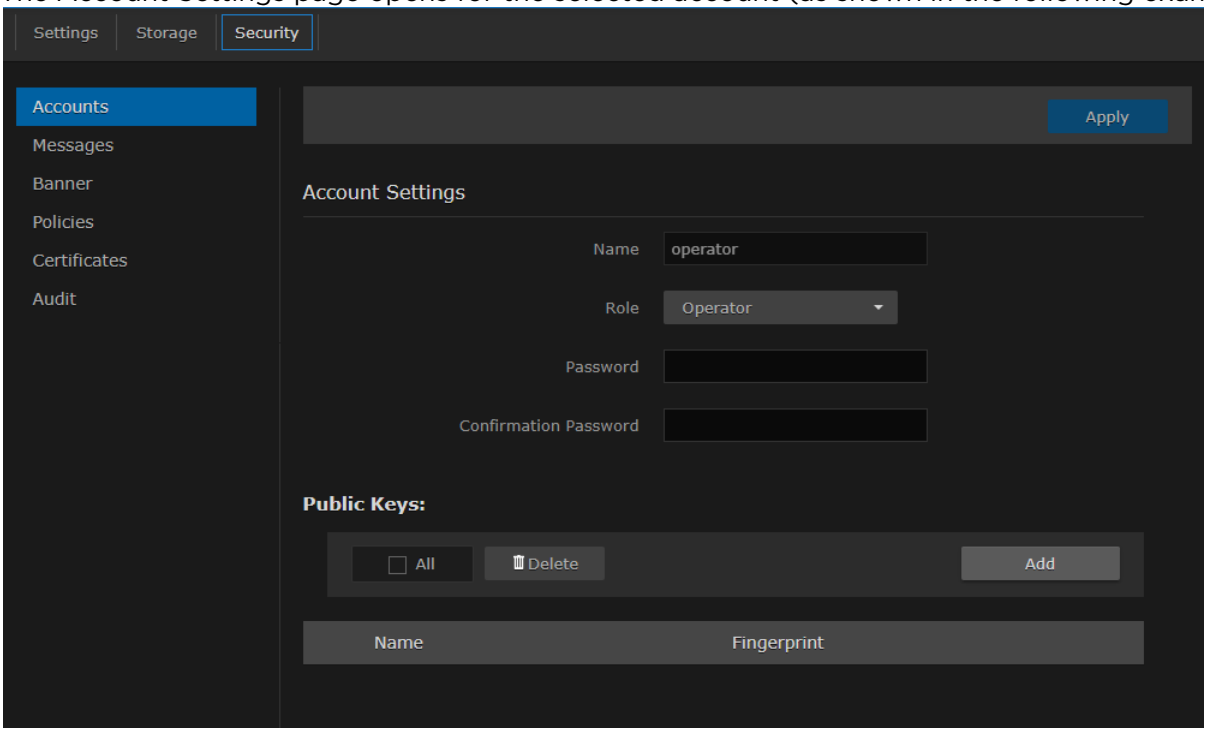
1. From the Accounts List View, click **Add**.
2.
> **Tip**
>
> The user name must comply with Unix restrictions (lower case letters a-z, numbers 0- 9, hyphen and underscore).



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

   New users must change their passwords the first time they sign in as well as when the administrator resets the password of an existing account. When you change your password, the new password takes effect immediately.
4. To upload a public key for the account, follow the steps in Managing Public Key Authentication.
5. To get the fingerprint for a public key, select the public key in the list. For more information, see Account Settings.
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; must 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
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.
Confirmation password	n/a	Re-type the new password.
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**.
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.

Related Topics

- Role-based Authorization.
- "Password Requirements" in Changing Your Password
- Managing Public Key Authentication

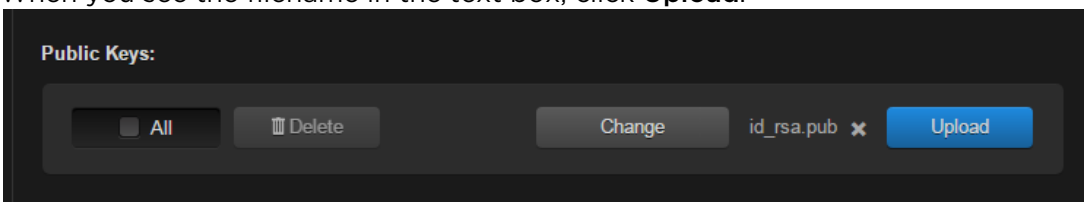
Managing Public Key Authentication

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 Makito X.

To upload a public key file for an account:

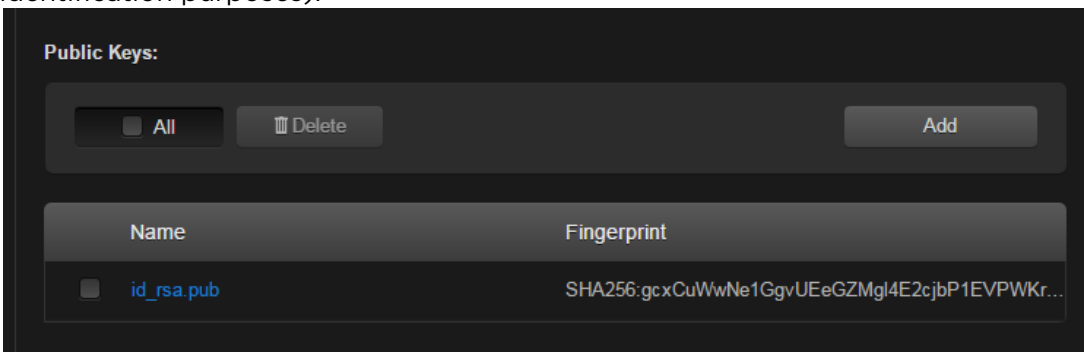
1. From the Accounts List View, click a link in the table for an existing account.
2. On the Account Settings page, under Public Keys, click **Add** and select the file in the Open File dialog box.

   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 Public Keys list of along with the fingerprint for the key (e.g., for identification purposes).



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 your 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 sign-in.

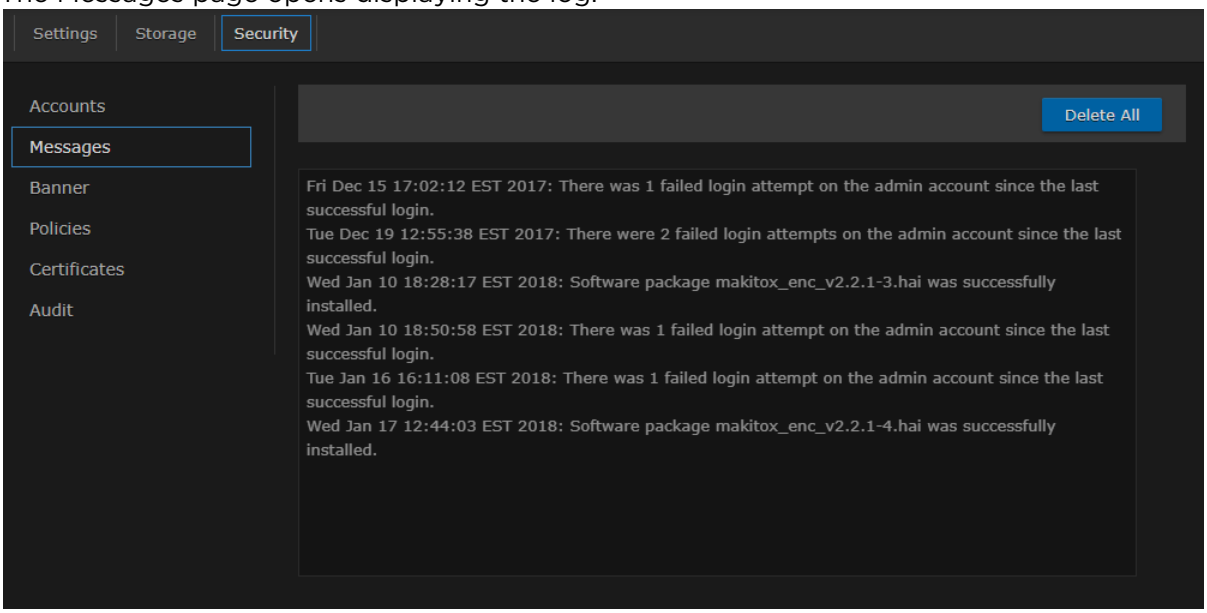
The log of the actions recorded includes the following:

- 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 encoder or decoder may be compromised, and it is recommended to re-installed the firmware.**

To view the messages:

1. On the Administration page, click **Security** on the navigation bar and **Messages** on the sidebar. The Messages page opens displaying the log.



2. To delete the messages, click **Delete All**. The messages will be deleted immediately.

Managing Banners

The `banner` command is used to manage the Advisory Notice and Consent Banner. This is a single text file that is displayed to users who sign in for interactive sessions on Makito X Series devices. The banner is typically an advisory/warning notice to be displayed before the Sign-in page.

Only ASCII file format is supported for the banner file; the maximum file size for the banner is 4KB.

Note

The `banner` command can only be used by an administrator.

Synopsis

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

Actions

Action	Description
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 encoder and locally stored in the current (administrative) user's directory before it can be installed from the CLI. The Makito X Series 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.

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 encoder.

Examples

```
# banner get
The Advisory Notice and Consent Banner is disabled.
Unable to display banner: No banner file.
```

If enabled, the following banner is displayed upon user login:

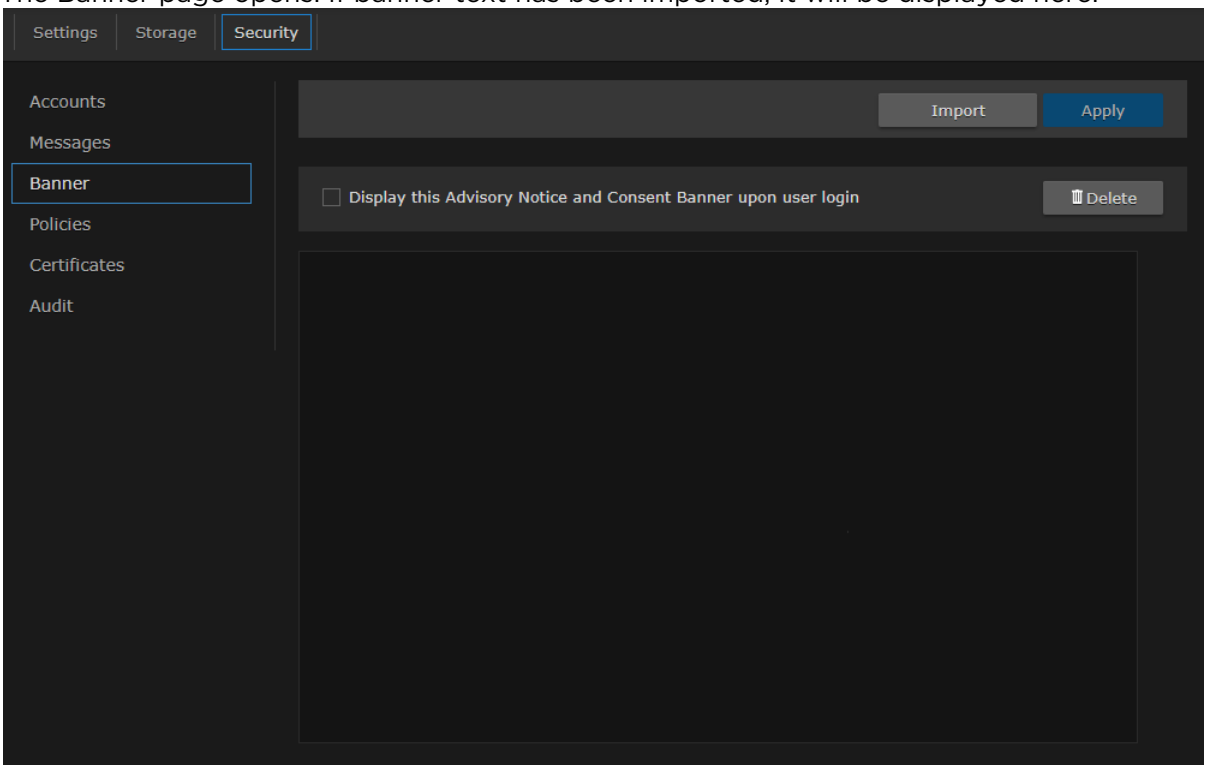
```
----------------------------------------------------------------------
**********************************************************************
                            * WARNING *
**********************************************************************

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 QA *
**********************************************************************
```

To upload a text file for the Banner page:

1. On the Administration page, click **Security** on the navigation bar and **Banner** on the sidebar. The Banner page opens. 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 the ✖ icon.

3. Click **Upload**. The banner text is now displayed in the pane.
4.

> **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.

> **Important**
>
> IP display is enabled on the serial port login prompt by default and takes precedence over a banner. If both Banner and IP display are enabled, users will see the IP, not the banner on the serial port.
> You can disable and re-enable IP display using the CLI commands `disable_ip_display_on_serial_port` and `enable_ip_display_on_serial_port`. If you disable IP display with this CLI command, the banner works.

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.

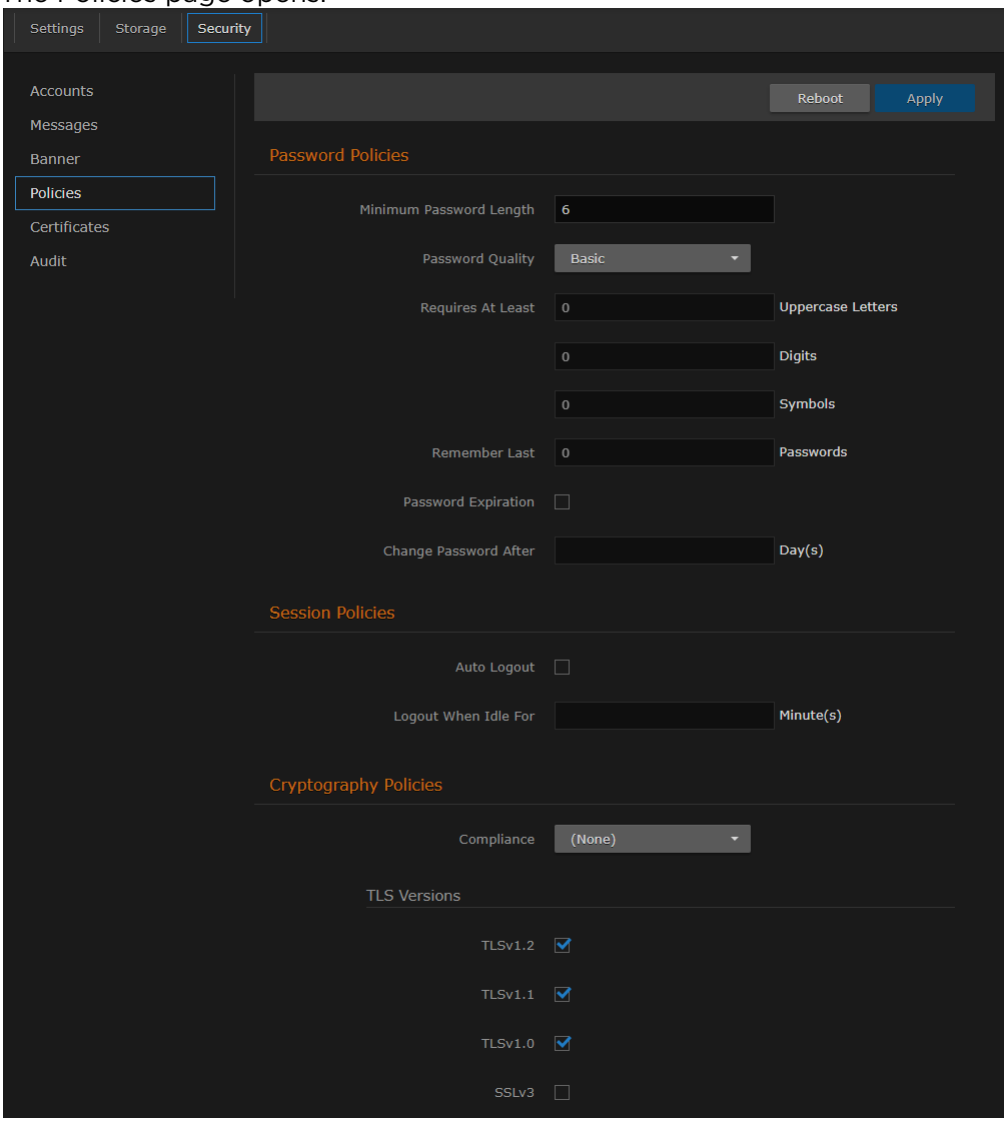
Managing Security Policies

> **Note**
>
> The Policies page provides the options to configure Makito X encoders to be "hardened". For more information, see Hardening.

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 Security policies for the encoder:

1. On the Administration page, click **Security** on the navigation bar and **Policies** on the sidebar. The Policies page opens.



2. Select or enter the new value(s) in the appropriate field(s). For details, see Policy Settings.
3. To apply your changes, click **Apply**.

Policy Settings

The following table lists the Policy settings for the encoder:

Password Policies

Policy Setting	Default	Description/Values
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.
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

Policy Setting	Default	Description/Values
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 Sign-in page.

Policy Setting	Default	Description/Values
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).

Cryptography Policies

Policy Setting	Default	Description/Values
Compliance	None	Specifies the required cryptographic compliance, either: • None • FIPS 140-2: Applies cryptographic modules accredited under the Federal Information Processing Standard (FIPS) Publication 140-2. • NDPP v1.1: Activates cryptographic security to a level compliant with the National Information Assurance Partnership (NIAP) Network Device Protection Profile, Revision 1.1. • 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** SSLv3 can be enabled only if Compliance is set to None. At least one TLS version must be enabled.

Managing Certificates

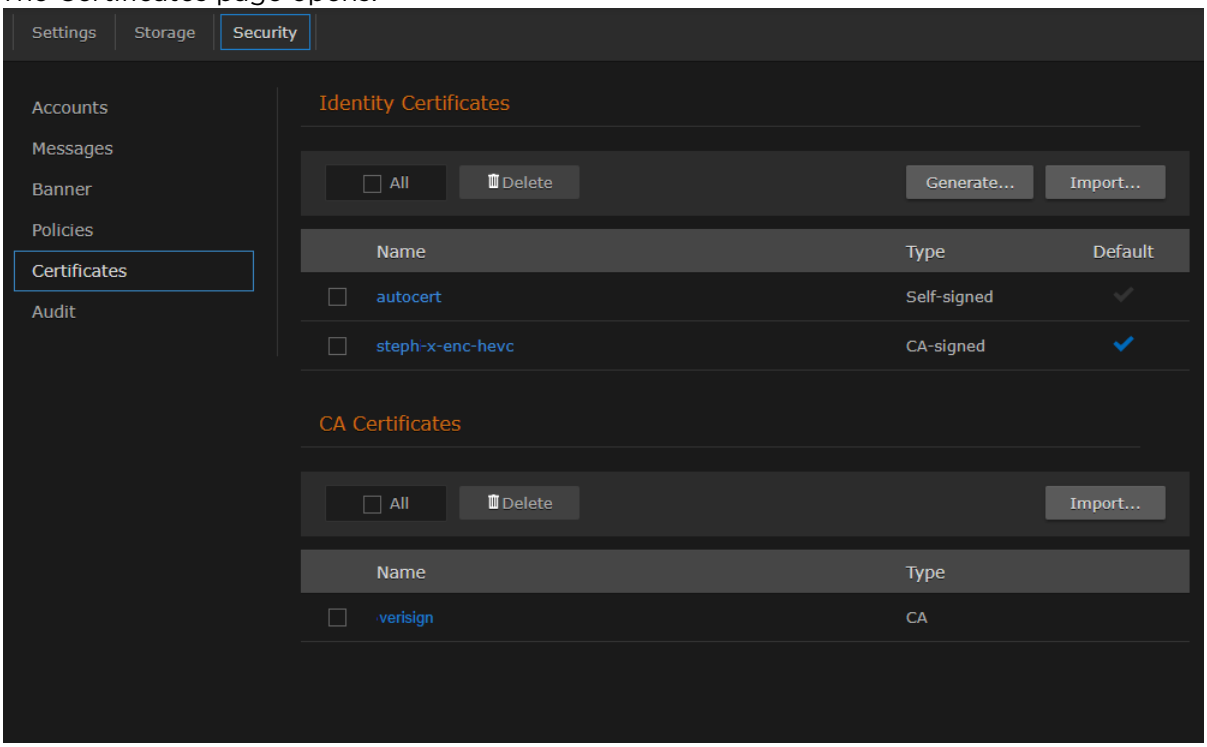
The Certificates page shows the list of Identity and CA Certificates installed on Makito X Series devices.

- **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 device's IP address and/or its FQDN (Fully Qualified Domain Name) if DNS is used.
- **CA Certificates:** A CA Certificate is normally a root certificate from a certificate authority that is generally widely known and trusted. CA Certificates are stored on the Makito X 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 (if you have one).

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:

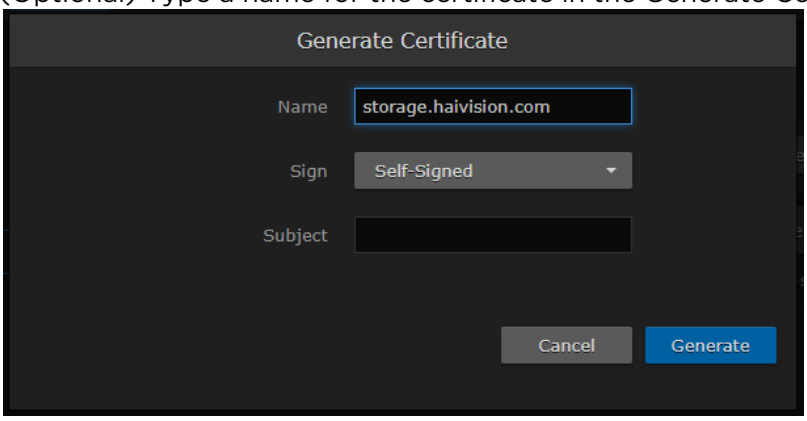
1. To generate a Self-signed Certificate or a Certificate Signing Request (CSR):On the Administration page, click **Security** on the navigation bar and **Certificates** on the sidebar.
2. The Certificates page opens.



The default Identity Certificate is indicated with a blue check.

1. On the Certificates page, click **Generate**.

2. (Optional) Type a name for the certificate in the Generate Certificate dialog.



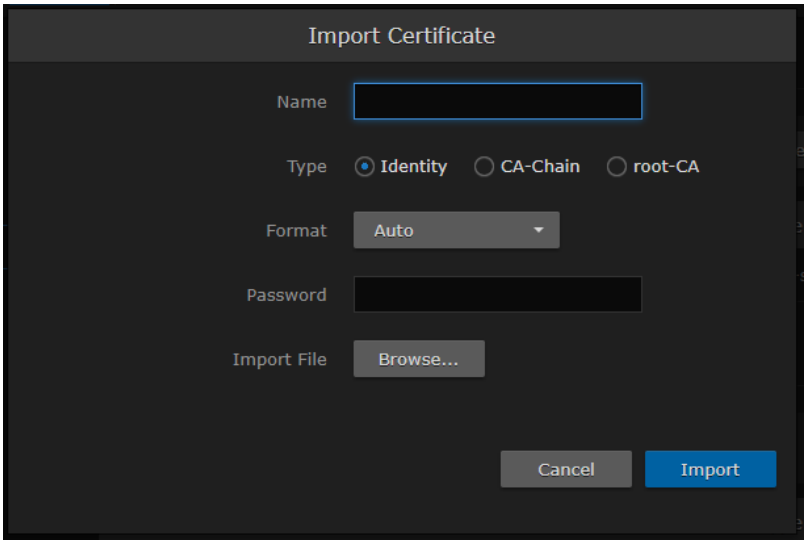
3. Select either Self-signed or Certificate Signing Request from the drop-down list. For more information, see "Sign" in Certificate Settings.
4. For the subject, type in information about the device that the Identity Certificate represents. For more information, see "Subject" in Certificate Settings.
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 the signed certificate back later by clicking on the **Import** button (using the same name as the CSR file).

Tip

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

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" in Certificate Settings.

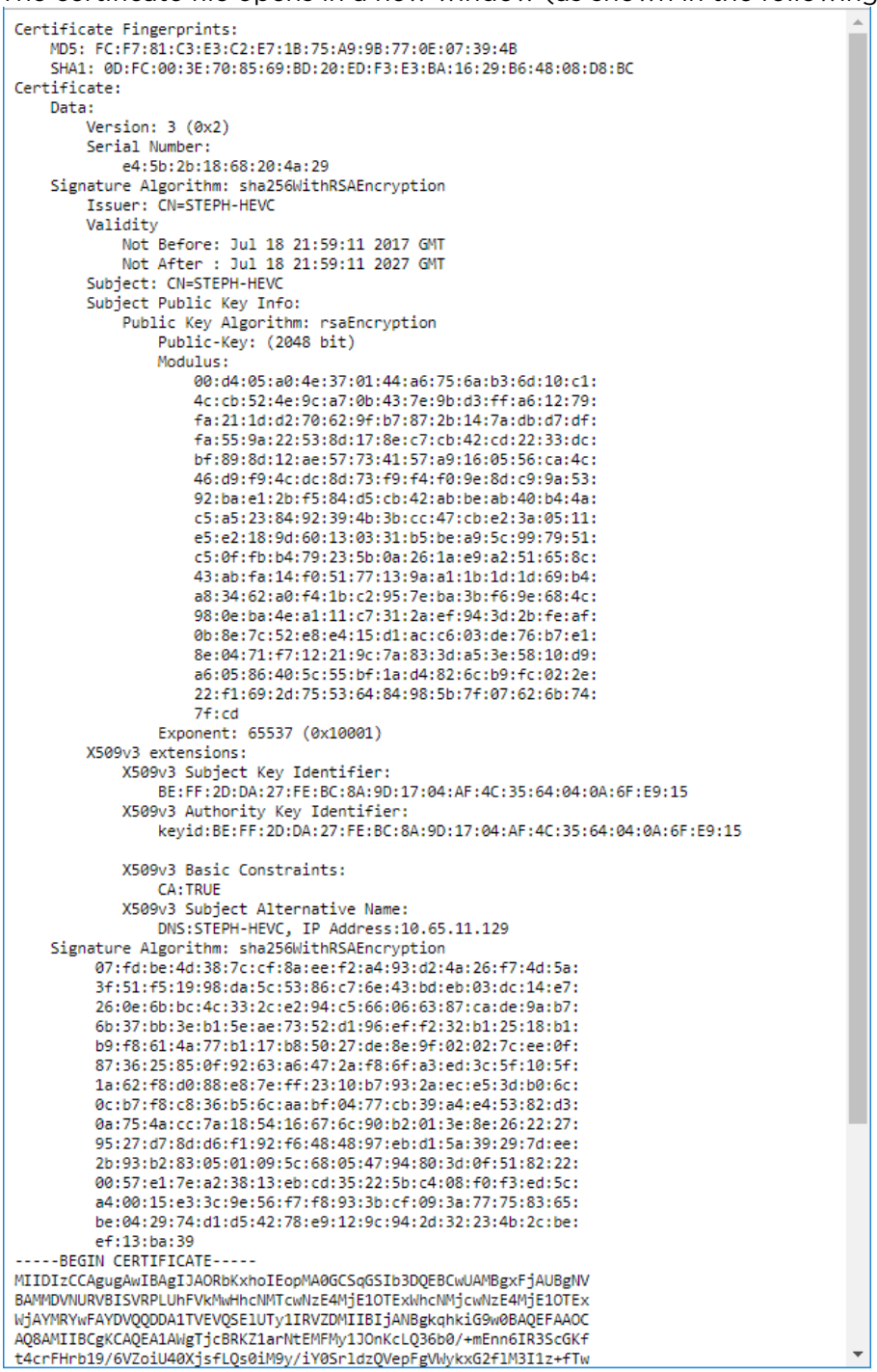
c. Click **Import**.

2. To view the details of a certificate, click 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 (grayed out) checkmark under **Default**.
   The selected certificate will be set as the default certificate. It will be immediately applied to communications with the Audit server, but will not apply to HTTP communications until the next service restart or system reboot.

Viewing Certificate Details

To view the details of a certificate file:

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



```
Certificate Fingerprints:
    MD5: FC:F7:81:C3:E3:C2:E7:1B:75:A9:9B:77:0E:07:39:4B
    SHA1: 0D:FC:00:3E:70:85:69:BD:20:ED:F3:E3:BA:16:29:B6:48:08:D8:BC
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e4:5b:2b:18:68:20:4a:29
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=STEPH-HEVC
        Validity
            Not Before: Jul 18 21:59:11 2017 GMT
            Not After : Jul 18 21:59:11 2027 GMT
        Subject: CN=STEPH-HEVC
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d4:05:a0:4e:37:01:44:a6:75:6a:b3:6d:10:c1:
                    4c:cb:52:4e:9c:a7:0b:43:7e:9b:d3:ff:a6:12:79:
                    fa:21:1d:d2:70:62:9f:b7:87:2b:14:7a:db:d7:df:
                    fa:55:9a:22:53:8d:17:8e:c7:cb:42:cd:22:33:dc:
                    bf:89:8d:12:ae:57:73:41:57:a9:16:05:56:ca:4c:
                    46:d9:f9:4c:dc:8d:73:f9:f4:f0:9e:8d:c9:9a:53:
                    92:ba:e1:2b:f5:84:d5:cb:42:ab:be:ab:40:b4:4a:
                    c5:a5:23:84:92:39:4b:3b:cc:47:cb:e2:3a:05:11:
                    e5:e2:18:9d:60:13:03:31:b5:be:a9:5c:99:79:51:
                    c5:0f:fb:b4:79:23:5b:0a:26:1a:e9:a2:51:65:8c:
                    43:ab:fa:14:f0:51:77:13:9a:a1:1b:1d:1d:69:b4:
                    a8:34:62:a0:f4:1b:c2:95:7e:ba:3b:f6:9e:68:4c:
                    98:0e:ba:4e:a1:11:c7:31:2a:ef:94:3d:2b:fe:af:
                    0b:8e:7c:52:e8:e4:15:d1:ac:c6:03:de:76:b7:e1:
                    8e:04:71:f7:12:21:9c:7a:83:3d:a5:3e:58:10:d9:
                    a6:05:86:40:5c:55:bf:1a:d4:82:6c:b9:fc:02:2e:
                    22:f1:69:2d:75:53:64:84:98:5b:7f:07:62:6b:74:
                    7f:cd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                BE:FF:2D:DA:27:FE:BC:8A:9D:17:04:AF:4C:35:64:04:0A:6F:E9:15
            X509v3 Authority Key Identifier:
                keyid:BE:FF:2D:DA:27:FE:BC:8A:9D:17:04:AF:4C:35:64:04:0A:6F:E9:15

            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Alternative Name:
                DNS:STEPH-HEVC, IP Address:10.65.11.129
    Signature Algorithm: sha256WithRSAEncryption
         07:fd:be:4d:38:7c:cf:8a:ee:f2:a4:93:d2:4a:26:f7:4d:5a:
         3f:51:f5:19:98:da:5c:53:86:c7:6e:43:bd:eb:03:dc:14:e7:
         26:0e:6b:bc:4c:33:2c:e2:94:c5:66:06:63:87:ca:de:9a:b7:
         6b:37:bb:3e:b1:5e:ae:73:52:d1:96:ef:f2:32:b1:25:18:b1:
         b9:f8:61:4a:77:b1:17:b8:50:27:de:8e:9f:02:02:7c:ee:0f:
         87:36:25:85:0f:92:63:a6:47:2a:f8:6f:a3:ed:3c:5f:10:5f:
         1a:62:f8:d0:88:e8:7e:ff:23:10:b7:93:2a:ec:e5:3d:b0:6c:
         0c:b7:f8:c8:36:b5:6c:aa:bf:04:77:cb:39:a4:e4:53:82:d3:
         0a:75:4a:cc:7a:18:54:16:67:6c:90:b2:01:3e:8e:26:22:27:
         95:27:d7:8d:d6:f1:92:f6:48:48:97:eb:d1:5a:39:29:7d:ee:
         2b:93:b2:83:05:01:09:5c:68:05:47:94:80:3d:0f:51:82:22:
         00:57:e1:7e:a2:38:13:eb:cd:35:22:5b:c4:08:f0:f3:ed:5c:
         a4:00:15:e3:3c:9e:56:f7:f8:93:3b:cf:09:3a:77:75:83:65:
         be:04:29:74:d1:d5:42:78:e9:12:9c:94:2d:32:23:4b:2c:be:
         ef:13:ba:39
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIJAORbKxhoIEopMA0GCSqGSIb3DQEBCwUAMBgxFjAUBgNV
BAMMDVNURVBISVRPLUhFVkMwHhcNMTcwNzE4MjE1OTExWhcNMjcwNzE4MjE1OTEx
WjAYMRYwFAYDVQQDDA1TVEVQSE1UTy1IRVZDMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA1AWgTjcBRKZ1arNtEMFMy1JOnKcLQ36b0/+mEnn6IR3ScGKf
t4crFHrb19/6VZoiU40XjsfLQs0iM9y/iY0SrldzQVepFgVWykxG2flM3I1z+fTw
```

2. (Optional) Save the file.

Certificate Settings

The following table lists the Certificates controls and settings:

Generate Certificate Dialog

Setting	Default	Description/Values
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 (CSR): A request will be generated, and its name will be added to the list of Identity Certificates. A copy of the request is saved in the current administrator's home directory, or it can be copied and pasted into a new file in a text editor from the CSR view. In its generated form, this certificate is still a request and cannot be used as an Identity Certificate before it is signed by a CA, and imported back.
Subject		The Subject identifies the device being secured, in this case, the Makito X. Entering the special value “auto” (or leaving the field blank) sets the Common Name to the device’s FQDN if DNS is set, or the IP address otherwise. The Subject Alternative Name extension is also set to the FQDN, hostname, and IP Address of the device (there is no other method to enter Subject Alternative Name values). Type in the subject in the form: `"/C=US/ST=Maine..."` where the most common attributes are: • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name Note that parameters with spaces should be enclosed in quotation marks.

Import Certificate Dialog

Setting	Default	Description/Values
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.

Setting	Default	Description/Values
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.

Setting	Default	Description/Values
		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
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.

Related Topics:

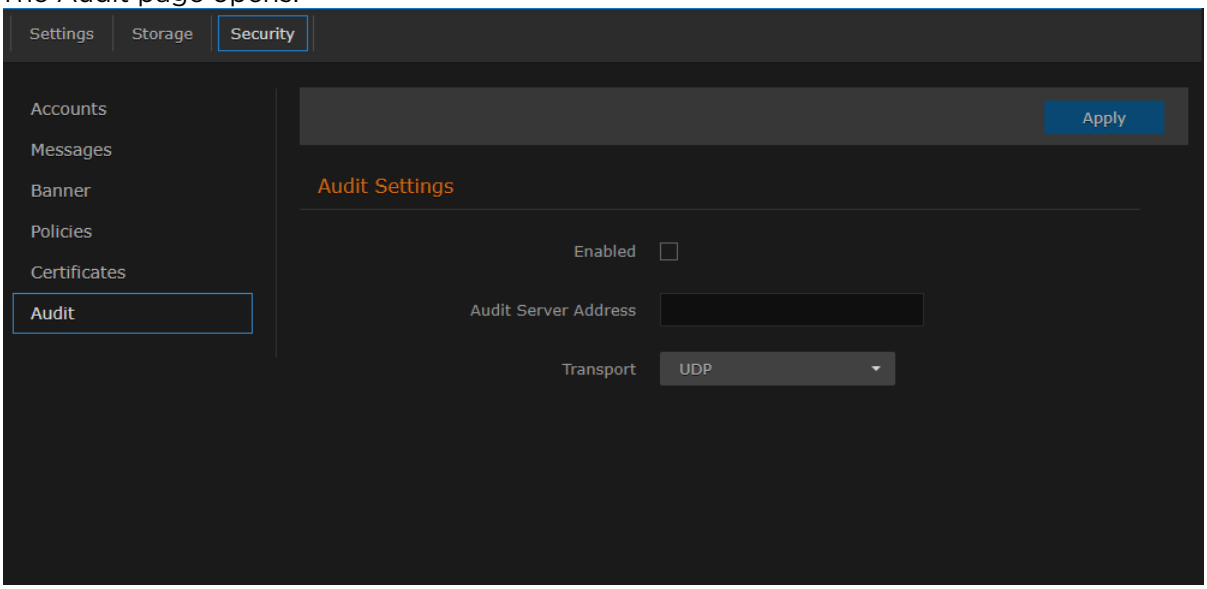
- Configuring Network Settings

Managing Audits

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

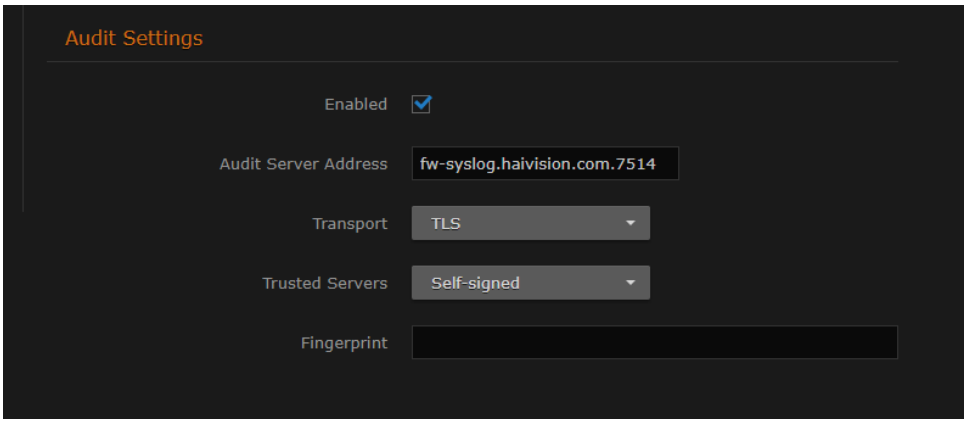
To configure an Audit server:

1. On the Administration page, click **Security** on the navigation bar and **Audit** on the sidebar. The Audit page opens.



2. Check the **Enabled** 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 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 Transport is set to TLS and Trusted Server is set to CA-Signed.
4. Set the type of transport protocol that will be used to send the logs to the audit server. See details in Audit Settings.
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 encoder (see Managing Certificates) for the TLS connection to succeed.
6. If Trusted Servers is set to Self-signed, copy the Fingerprint string from the Audit server's certificate and paste it in the Fingerprint field under Audit Settings 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]` • `ipv4_addr[:port]` • `ipv6_addr[:port]` • `hostname[:port]` If the port is not provided, the default port for the chosen Transport will be used:
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 an audit. The encoder will only accept a connection with the specified audit server if the certificate it presents 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. A connection with the specified audit server will be accepted if its certificate is self-signed, and its fingerprint matches the one configured on the Makito X.

Audit Setting	Default	Description/Values
Fingerprint	n/a	(Only appears if Self-signed is selected for Trusted Servers) Enter the fingerprint of the audit server's self-signed 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.

Configuring A/V Services Using SNMP

This section provides information required to manage the Makito X through the Simple Network Management Protocol (SNMP). 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 through the exchange of SNMP messages.

Note

This content 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.

Tip

To develop new SNMP applications, see the list of Supported MIBs.

Topics in This Chapter

- SNMP Overview
- Supported MIBs
- SNMP Agent Components
- SNMPv3
- SNMP Utilities
- SNMP Syntax for Setting Up Streams

SNMP Overview

To support management of the Makito X 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.

> **Note**
>
> **The Makito X uses Net-SNMP Version 5.5.2 and supports SNMP v1, v2c, and v3.**

The Makito X 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 IP networks.

Supported MIBs

The Makito X 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).
• IPV6-MIB.txt	RFC-2465	Management Information Base for IP Version 6.

• HAI-VISION-MIB.txt • HAI-AVT-STREAM-MIB.txt • HAI-HDC-MIB.txt	Haivision Enterprise	Supports configuration, status, and statistics.
Encoder-specific		
• HAI-MAKITO-X-ENC-CAPS.txt	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X Series (encoder) 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.

Decoder-specific		
• `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.

Note

You can download the MIBs directly from your Makito X under: `/usr/share/snmp/mibs/HAI-*.txt`, or access them in a zip file here: Makito X Encoder 2.3 MIBs.zip.

SNMP Agent Components

This section presents key components used to set up SNMP management on the Makito X.

- snmpd
- snmpd.conf
- snmpd.local.conf
- nmcfg

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 Series device 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 in `/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). However, for most settings, it is preferable to use the `nmcfg` configuration script.

On a Makito X Series device, the `snmpd.conf` file includes:

- access control setup (i.e., community and user privileges),
- system information setup (e.g., system location, services and contact).

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

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

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 Series 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` (readonly) 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 Series MIBs.

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

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/netsnmp/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           guest             auth           guest                -
usm           administrator     priv           johndoe              -
v2c           administrator     noauth         admin                localhost
v2c           administrator     noauth         admin                localnet
v2c           guest             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} [{noauh|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>
```

SNMPv3

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

The following command creates the user "johndoe" and defines its authentication protocol and password, and its privacy (encryption) protocol and password.

These examples use MD5 for authentication and DES for privacy. They provide broader compatibility but if your SNMP client supports SHA (authentication) and AES (privacy), use these as they provide better security. (Note that you can type `nmcfg user help` to view the supported protocols and pass phrase restrictions.)

```
# nmcfg user define johndoe MD5 "password" DES "pass phrase"
```

The new user has no permissions until its access rights are defined. The command below assigns the operator role to the user.

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

Note that the Makito X administrative user roles are preferred over the read-only or read-write permissions (to the whole MIB). These roles provide to SNMP v1/v2c communities and SNMPv3 users access privileges modeled on the Makito X Accounts roles.

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 MD5 -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 MD5 -A "password" -x DES -X "pass phrase" -l authPriv localhost
haiAvtStreamEncapsulation.1 i directRtp
HAI-AVT-STREAM-MIB::haiAvtStreamEncapsulation.1 = INTEGER:
directRtp(1)
```

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 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
`haiAvtStreamPgmTable`	`Stream ID` `Program Index`	Transport Stream programs. Only SPTS (Single Program Transport Stream) supported. Not present for non Transport Streams (directRTP, QuickTime).

`haiAvtStreamContentTable`	`Stream ID`
	`Program Index`
	`Content Index`
		Contents (video, audio, and/or metadata).
		Elementary Streams (ES) for Transport Stream. Only one entry for non-TS in which case Program Index is 1. One to three entries exist for Transport Streams.

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

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`).

Objects from the `haiAvtStreamPgmTable` and `haiAvtStreamContentTable` cannot be set before the corresponding `haiAvtStreamTable` row is created and can only be set when the stream entry is not active (`haiAvtStreamRowStatus` is not active).

Examples

The following example, using `netsnmp` CLI commands on the Makito X encoder, creates a streaming session to IP Address `198.51.100.106` at port 2000, and starts streaming immediately. 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 haiAvtStreamAddrType.0 = ipv4 haiAvtStreamAddr.0 d 198.51.100.106
 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 AddrType = ipv4 Addr d 198.51.100.106 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.ipv4.4.198.51.100.106.2000
HAI-AVT-STREAM-MIB::haiAvtStreamInverseID.ipv4."198.51.100.106".2000 = HaiAvtStreamID: 5
```

To create a Stream with a known ID, the `haiAvtStreamNewID.0` object reports the next available Stream ID. In the example below, the Transport Stream Program number is set to `7` and the video encoder `1` is selected for the video content. Note that `createAndWait` is used so the program and 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 AddrType = ipv4 Addr d 198.51.100.106
Port u 2000 Encapsulation i tsUdp RowStatus i createAndWait
>snmpset -v2c -c admin -IS haiAvtStream localhost PgmNumber.5.1 i 7 PgmNbContents.5.1 i 2 ContentType.5.1.1
 i video ContentToolID.5.1.1 i 1 ContentType.5.1.2 i audio ContentToolID.5.1.2 i 0
>snmpset -v2c -c admin localhost haiAvtStreamRowStatus.5 i active
```

CLI Command Reference

Management via the CLI is possible through a telnet session, SSH, or (if applicable) RS-232. This alphabetical command reference lists and describes the available Command Line Interface (CLI) commands to configure and manage the Makito X encoder.

Accessing the CLI

To access the encoder CLI:

1. Open a telnet session to the encoder (for the default encoder IP address, see **Accessing the Web Interface**).
2. At the login prompt, type the username and password (see **Role-based Authorization**).

Syntax Conventions

The following syntax conventions are used in this appendix:

Convention	Description
`Monospaced font`	Indicates command names and options, filenames and code samples.
italic font	Indicates variables or placeholders 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.

Command Summary and Access Control

The Makito X CLI commands are divided in two main groups: operation and administration:

- **Operation Commands** are used to manage the Audio/Video data path, processing, and features, including audio/video/metadata content selection, logo, audio/video encoding, H.264 streaming, and image snapshots. Operation command effects are immediate but not persistent (i.e., between reboots) unless the current operating configuration is explicitly saved (using the config command).
- **Administration Commands** address the security and network configuration. Their effects are persistent but not always immediate; some require system reboot to take effect.

Note

A warning appears when you sign in or out of a Makito X, or reboot, when the current configuration has not been saved in a preset. See config.

Below is a list of CLI commands and other functionalities supported by the system, the privileges for each role, and their descriptions.

Operation Commands | Administration Commands | Access | Other/Utilities

Operation Commands

Command	Role			Description
	Admin	Operator	Guest	
General				
audenc	Yes	Yes	"get" only	Manage encoder audio acquisition settings, including starting and stopping encoding of the audio input.
leds	Yes	Yes	"get" only	Initiate blinking of the Status and TX LEDs on the Makito X face-plate in order to help locate the device.
metadata	Yes	Yes	"get" only	Manage metadata sources to capture metadata (either KLV or CoT) and then incorporate data information within the MPEG Transport Stream.
passthrough	Yes	Yes	"get" only	Enable bi-directional serial passthrough for controlling serially attached devices such as PTZ controlled cameras.
record	Yes	Yes	"get" only	Manage recording of streams, including starting and stopping recording.
roi	Yes	Yes	"get" only	Enhance the quality of the encoded video for a region within the video frame (i.e., a region of interest).
session	Yes	Yes	"get" only	Manage SAP multicast advertising sessions.
stream	Yes	Yes	"get" only	Create and manage audio/video streams.

talkback	Yes	Yes	"get" only	Manage audio talkback settings to allow two-way audio communication using the encoder's Audio Output.
temperature	Yes	Yes	Yes	Display the current temperature of the unit.
videnc	Yes	Yes	"get" only	Manage video encoding parameters, including starting and stopping encoding of the video input.
vidin	Yes	Yes	"get" only	View and manage video input settings.
Media				
logo	Yes	Yes	"get" and "list" only	Manage logo overlays (i.e., a graphic file to display as a logo overlay in the encoded video).
mklogo	Yes	Yes	—	Convert a graphic file to Haivision's overlay image format (.oly) in order to display the image as a logo overlay.
mkstill	Yes	Yes	—	Convert a static picture into a file containing an encoded single H.264 GOP sequence. This is required in order to configure a Makito X stream with a static image that will replace the "real" video stream when streaming is paused.
snapshot	Yes	Yes	"get" and "list" only	Take and manage snapshots from the video input.
still	Yes	Yes	"list" only	Manage still image files on the Makito X file system. Static images are used to replace the "real" video stream when streaming is paused.

Operation Commands | Administration Commands | Access | Other/Utilities

Administration Commands

Command	Role			Description
	Admin	**Operator**	**Guest**	
Network and Management				
bist	Yes	—	—	Perform Built-in self-tests (BIST) and Power-ON Selftests (POST).
config	Yes	Yes	"list" only	Manage configurations on the Makito X.
date	Yes	Yes	Yes	Display the current date.

dest	Yes	Yes	"get" only	(with storage only) Manage recording export destinations.
dtconfig	Yes	—	—	Set the date and time on the encoder.
ethercfg	Yes	—	—	View, manually control, and save the Ethernet configuration parameters.
haiversion	Yes	Yes	Yes	Display the Firmware Build ID, Build Time, and serial number for the Makito X.

hdcp	Yes	Yes	"get" only	(Makito X DVI systems only) Manage HDCP settings.
ipconfig	Yes	—	—	View and set the parameters that specify the networking context for the Makito X, including the IP settings, hostname, and DNS.
ipv6config	Yes	—	—	View and set the parameters that specify the IPv6 network configuration.
license	Yes	—	—	Manage licensed features.
nmcfg	Yes	—	—	Used by system administrators or GUI/Web interface applications in the configuration of SNMP for the Makito X.
package	Yes	—	—	View and manage software packages, including firmware upgrades.
passwd	Yes	operator password only	user password only	Change the password for a user account.
personality	Yes	—	—	(Makito XR only) Set the personality to either the two or four-port variant (X2R or X4R).
reboot	Yes	—	—	Halt and restart the Makito X.
service	Yes	—	—	Enable and disable network services, including HTTP, passthrough, snmp, ssh, talkback, telnet, and vf.
system_snapshot.sh	Yes	Yes	Yes	Take a system snapshot for the purpose of troubleshooting, which may be forwarded to Haivision Technical Support if you are requesting technical support.
tzconfig	Yes	—	—	Configure the timezone on the encoder.
Storage				
nas	Yes	—	—	Set an NFS mount point on the Makito X.
storage	Yes	Yes	—	Manage storage devices on the Makito X with Storage dual-height model.
transfer	Yes	Yes	—	Use to manage the export of files from the encoder.

Security				
account	Yes	—	—	Use to manage user accounts for the encoder.
audit	Yes	—	—	Use to enable remote logging of security and administrative events and configure the remote audit (syslog) server connection.
banner	Yes	—	—	Use to manage the Advisory Notice and Consent Banner.
certificate	Yes	—	—	Use to manage the TLS certificates for the Web interface HTTPS server and the secured TLS connection to the remote audit server.
messages	Yes	—	—	Use to view and manage administrative login messages.
policy	Yes	—	—	Use to manage security policy settings.
pubkey	Yes	Yes	Yes	Use to manage the user's own authorized SSH public keys.

Operation Commands | Administration Commands | Access | Other/Utilities

Access

Command	Role		
	Admin	**Operator**	**Guest**
Web access	Yes	Yes	Yes
Telnet to/from encoder	Yes	Yes	Yes
Serial access to encoder	Yes	Yes	Yes

Operation Commands | Administration Commands | Access | Other/Utilities

Other Commands and Utilities

Command	Role			Description
	Admin	**Operator**	**Guest**	
iperf	Yes	Yes	Yes	Measure and tune network performance.
ping	Yes	Yes	Yes	Send packets to network hosts to test a network connection.

Command	Role			Description
	Admin	Operator	Guest	
tcpdump	Yes	—	—	Display TCP/IP and other packets being transmitted or received over a network interface.
traceroute	Yes	Yes	Yes	Display the route (path) and measure transit delays of packets across an IP network.

For an overview of system access control on the Makito X, see **Role-based Authorization**.

Operation Commands

audenc

The `audenc` command is used to manage encoder audio acquisition settings. The `audenc start` and `audenc stop` commands can be used to start and stop encoding of the audio input. ID is either the encoder ID or all.

- On the Makito X-DVI, the encoder ID is 0, 1, 2, or 3.
- On the Makito X-SDI, the encoder ID is 0, 1, 2, 3, 4, 5, 6, or 7.

For details, see Configuring Audio Encoders.

Synopsis

```
audenc ID start
audenc ID stop
audenc ID mute
audenc ID unmute
audenc ID set parameter=value [parameter=value...]
audenc ID get [config, stats, all]
audenc ID clear
```

Actions

Action	Description
start	Activates encoding of the audio input
stop	Stops encoding of the audio input.
mute	**Tip** This may be used when you do not wish to encode the audio but the decoder being used does not support decoding of video-only streams.
unmute	Resumes encoding of the audio input (when muted)
set	Configures encoder audio parameters. A series of one or more `parameter=value` pairs can be specified at once. See Parameters below.
get	**Tip** To display a summary of all the encoders in a table format, you can use `audenc all get table`.
clear	Clears the encoder's statistics.
help	Displays usage information for the audenc command

Parameters

Parameter	Default	Description/Values
`input`	Analog	The Audio Input for the encoder. The available values depend on your Makito X device. For Makito X DVI devices: • Analog • DVICH12 For Makito X SDI devices: • Analog • SDI1CH1+2, SDI1CH3+4, SDI1CH5+6, SDI1CH7+8, SDI1CH9+10, SDI1CH11+12, SDI1CH13+14, SDI1CH15+16 • **Note** The SDI2 audio inputs are only available on dual-BNC systems.
`language`		The language used for input. Enter a 3-character long ISO639-2 code or none. If you don't know the code for a language, you can directly enter one of the languages below in full or abbreviated form: • Albanian, Arabic, Armenian, Bulgarian, Chinese, Croatian, Czech, • Danish, Dutch, English, Estonian, Finnish, French, German, Greek, • Hebrew, Hindi, Hungarian, Indonesian, Irish, Icelandic, Italian, • Japanese, Khmer, Korean, Latvian, Lithuanian, Malay, Maltese, • Mongolian, Norwegian, Punjabi, Persian, Polish, Portuguese, • Romanian, Russian, Slovak, Slovenian, Spanish, Swahili, Swedish, • Turkish, Ukrainian, Vietnamese.
`level`	6	**Note** Only applies to Analog Audio Input.
`mode`	stereo	The number and type of audio channels to encode. • mono (left) • monoright • stereo
`algorithm`	[mpeg2]adts	The audio compression algorithm: • [mpeg2]adts - Encodes audio using the ISO/IEC 13818-7 MPEG-2 AAC-LC algorithm with an ADTS header. • loas - Encodes audio using the ISO/IEC 14496-3 MPEG-4 AAC-LC algorithm with a LOAS/LATM header.
`bitrate`	128 kbps	**Note** The available bitrate range depends on the current mode. • For mono, the bitrate range is 56 to 160 kbps. • For stereo, the bitrate range is 80 to 320 kbps.

Parameter	Default	Description/Values
`stcif`	Auto	Selects the video input from which the audio STC (System Time Clock) is derived. The available values depend on your Makito X device. For Makito X DVI devices: • Auto • digital • analog For Makito X SDI devices: • Auto • BNC1 • BNC2 **Note** When configuring the audio, in some cases, it may be necessary to specify the video input from which to derive the audio clock. An example would be if both SDI and Analog audio inputs are connected and you create two streams that share video input but each stream uses a different audio input. For more information, see **System Time Clock Interface (Video Input Selection)** below.

System Time Clock Interface (Video Input Selection)

When configuring the audio, you have to specify the video input from which to derive the audio clock so that it "runs" in lockstep with the video input and its STC (System Time Clock) moves forward at the same rate. This helps decoders with the playback and lip sync.

When audio encoders are configured to use an SDI input (SDI1ch*x* or SDI2ch*y*), it is expected and recommended that the source of the video for that encoder is the exact same SDI input. However, when audio encoders are configured to use an Analog input, the encoder has no way to know from which video input this particular audio encoder should derive its clock and STC.

When you set stcif to Auto selection of the STC source, when a new stream is created or started, if the stream contains audio and is using Analog for an input, the encoder checks if the stream also has video. If it does, it checks the currently configured input for that video encoder and sets the STC source of the audio encoder to match it.

Examples

```
# audenc 0 set input=SDI1CH1+2
```

For Makito X SDI, sets the Audio Input to SDI1CH1+2

```
# audenc 0 set input=DVICH12
```

For Makito X DVI, sets the Audio Input to DVICH1+2

```
# audenc 0 set bitrate=128
```

Sets the Audio Bitrate to 128. You will receive the following confirmation:

```
Audio encoder configured successfully
```

```
# audenc 0 get
```

or

```
# audenc 0 get config
```

Returns audio configuration information for the encoder, such as:

```
Encoder ID                : 0
  Name                    : "Audio Encoder 0"
  Configuration:
    Audio Input             : SDI1CH1+2
    Audio Bitrate           : 128 kbps
    Audio Samplerate        : 48 KHz
    Audio Mode              : Stereo
    Audio Algorithm         : ADTS
```

```
# audenc 0 get stats
```

Returns audio status information for the encoder, such as:

```
Encoder ID          : 0
Name                : "Audio Encoder 0"
Statistics:
  State             : WORKING
  Encoded Frames          : 881,906
  Encoded Bytes           : 301,024,128
  Encoded Bitrate         : 128 kbps
  Encoder Errors          : 0
  Encoder PTS             : 0x06503e698
  STC Source Interface    : BNC-1
```

Related Topics

- Configuring Audio Encoders

leds

The `leds` command may be used to help locate a Makito X by initiating blinking of the Status and TX or RX LEDs on the Makito X face-plate. This allows easy location of the device in large server room deployments, for example, to help identify a specific blade in a rack.

Synopsis

```
leds get
leds start [duration=15]
leds stop
```

Actions

Action	Description
start	Initiates blinking of the Status and TX or RX LEDs on the Makito X Encoder or Decoder face-plate.
stop	Cancels blinking of the Status and TX or RX LEDs on the Makito X Encoder or Decoder face-plate.
get	Displays LED status information for the Makito X.

Parameters

Parameter	Default	Description/Values
`duration`	n/a	The blinking duration can be set from 1 to 60 minutes. If no duration is set, blinking will last for 15 minutes.

Examples

```
# leds start duration=2
```

Initiates blinking of the Status and TX or RX LEDs, provides the following confirmation:

```
LEDs set to blink for 2 minutes.
```

```
# leds get
```

1. Displays current LED status (Makito X Encoder, blinking initiated above):
   LED States:
   Status LED : Green-Blinking
   TX1 LED : Green-Blinking
   TX2 LED : Green-Blinking
   Blinking will stop in 1m50s

2. Displays current LED status (Makito X Decoder, LEDs not blinking):
   LED States:
   Status LED : Green
   RX1 LED : Green
   RX2 LED : Green

```
# leds stop
```

Cancels blinking of the LEDs.

```
LEDs no longer blinking.
```

Related Topics

- Viewing System Status Information

logo

The `logo` command is used to manage logo overlays. You can configure the Makito X to display a graphic file as a logo overlay in the encoded video. One logo may be configured for each physical video input interface, i.e.:

- Two logos on dual channel encoders (Makito X SDI #S/B-292E-HDSDI2);
- One logo on single input encoders (Makito X DVI #S/B-292E-DVI or Makito X SDI #S/B-292E-HDSDI1).

ID is used to select the video input on dual channel encoders (either 0 for BNC-1 or 1 for BNC-2 on #S/B-292E-HDSDI2).

ID is optional on single input encoders such as the #S/B-292E-HDSDI1 and the #S/B292E-DVI. If entered, only 0 will be accepted.

The logo position can either be relative (top left, top right, centered, etc.) or absolute (positioned at the exact X and Y coordinates specified). You can also specify the scaling and transparency display settings.

Note

You can upload the graphic file either using the mklogo command, or from the Web interface (Logos page, see Configuring Logo Overlays).

Synopsis

```
logo ID enable
logo ID disable
logo ID set parameter=value [parameter=value...]
logo ID get
logo list
logo delete name
logo delete all
```

Actions

Action	Description
enable	Displays the logo when configured properly.
disable	Hides the logo.

Action	Description
set	Configures logo settings. A series of one or more `parameter=value` pairs can be specified at once. See **logo** below.
get	Displays information on the logo.
list	Lists the available logo files. Logos are stored on the Makito X file system in the folder `/usr/share/haivision/logos`.
delete name	Deletes a logo file from the list.
delete all	Deletes all logo files from the list.

Parameters

Parameter	Default	Description/Values
`filename`	n/a	The name of the `.oly` file to display as a logo overlay. **Note** The file must be in Haivision's overlay image (`.oly`) format. See **mklogo**.
`display`	Off	Enables the display of the specified file as a logo overlay. `On,Off`
`opacity`	100	Specifies the opacity percentage of the logo. • 0 — an invisible logo • ... • 100 — a solid logo
`transparency`	0	Specifies the visibility of the logo by its transparency percentage. • 0 — no transparency (solid/opaque logo) • ... • 100 — fully transparent (invisible logo)
`scaling`	100	Specifies the scale factor (percentage) for the logo: • 25 — logo is 1/4 its original size • 100 — no scaling • 400 — logo is 4 times its original size
`relative`	Off	If enabled, keeps the logo in proportion to the display area regardless of the input resolution. `On,Off` **Note** The original scaling is vis-à-vis a 1920x1080 grid.
`positioning`	BottomRight	Specifies the position for the logo: • BottomRight • TopRight • BottomLeft • TopLeft • Centered • Absolute: Uses the exact X and Y coordinates. • Relative: Uses the X, Y coordinates in relation to a 1920x1080 display area.

Parameter	Default	Description/Values
`x`	0	Horizontal coordinate used to position the top left point of origin in Absolute or Relative positioning modes. When using Absolute positioning, this is the exact horizontal position of the logo's top left point of origin.
`y`	0	Vertical coordinate used to position the top left point of origin in Absolute or Relative positioning modes. When using Absolute positioning, this is the exact vertical position of the logo's top left point of origin.

Example

```
# logo set filename=HaivisionLogoTransparent.oly opacity=65 positioning=bottomright display=on
```

Configures the file `HaivisionLogoTransparent.oly` to display as a logo on the system.

Related Topics

- mklogo
- Configuring Logo Overlays

metadata

The `metadata` command is used to manage metadata sources. This command configures the Makito X to capture either KLV (Key Length Value) or CoT (Cursor on Target) metadata and then incorporate data information within the metadata elementary stream of the standard MPEG Transport Stream.

The Makito X supports three metadata input types: either from the COM1 serial port, the HD-SDI interface, or a user-definable UDP network port. The serial port and HD-SDI interface are available on the Makito X-SDI only. UDP is always available.

Multiple metadata sources can be multiplexed into the same Transport Stream. To do so, you must specify the metadata source ES IDs in the **stream** command (`datasrc`), using multiple comma-separated metadata source id/names.

CoT/UDP and CoT/Serial metadata sources can also be retransmitted to other IP destinations for follow-up analysis by third party systems. For more information, see **CoT Retransmission**.

You can define a small set of static KLV objects for KLV and CoT metadata sources. This can be used to modify erroneous or insert missing mission IDs and security classification within outbound TS steams. For more information, see **KLV Metadata Insertion**.

KLV/SDI metadata sources can be frame-decimated to reduce the bandwidth used by the metadata service. You can also create additional HD-SDI sources which can be configured to different decimation settings. For more information, see **Metadata Decimation**.

You can also configure MISB Metadata Filtering on KLV metadata from the HD-SDI interface. For more information, see **UAS KLV Metadata Tag Filtering**.

Synopsis

```
metadata ID start
metadata ID stop
metadata create type=network port=udpport [addr=ipaddr] [name=text]
 -or-
metadata create type=hdsdi [input=bnc1] [decimation=factor] [name=text]
metadata ID delete
metadata ID set parameter=value [parameter=value ...]
metadata ID get
metadata ID clear
enable_metadata_on_serial_port
enable_console_on_serial_port
```

Actions

Action	Description
start	Starts the metadata source.
stop	Stops the metadata source.

Action	Description
create	Creates a new network (UDP) or HD-SDI metadata source. A series or one or more `parameter=value` pairs can be specified at once. See Parameters below.
delete	Deletes a UDP metadata source.
set	Configures metadata source settings. A series of one or more parameter=value pairs can be specified at once. See Parameters below.
get	**Tip** To display a summary of all the encoders in a table format, you can use `metadata all get table`.
clear	Clears the metadata source's statistics.
enable_metadata_on_serial_port	Enables metadata capture from the serial port.
enable_console_on_serial_port	Enables console management from the serial port. (default)

Parameters

Parameter	Default	Description/Values
General parameters		
`type`	network	Specifies the type of metadata source to create, either `network` or `hdsdi`. **Note** Additional HD-SDI sources can be created to stream KLV over SDI at different rates.
`name`		(optional) A name of up to 63 characters.
Network Source-specific parameters		
`port`		Specifies the UDP port for a network metadata source (i.e., the port on which to listen for KLV messages). Range: 1025–65,535
`address`		(optional) Specifies the IP address for a network metadata source. The address is only required to: • receive messages from a source that is multicasting. In this case, you need to provide the multicast IP address to which the data is being sent. OR • accept KLV messages coming from a specific sender.
HD-SDI Source-specific parameters		
`input`	bnc1	(optional, HD-SDI source only) Specifies the Input port for the metadata source: • bnc1 • bnc2

Parameter	Default	Description/Values
`decimation`		(Optional) For KLV over SDI metadata input, the ingested KLV messages can be frame-decimated to reduce the bandwidth used by the metadata service. Either specify the decimation factor. Range: 1–60 **Note** 1 means no decimation, 2 means divide by half, etc. Or you can specify another video encoder that uses the same input and the metadata AU rate will match the other video encoder's framerate. To do so, enter `videncX` where X is the actual encoder ID. See Metadata Decimation.
UAS KLV Tag Filtering parameters (See UAS KLV Metadata Tag Filtering)		
`uastags`	off	A list of comma-separated tag numbers from the UAS Datalink Local Set that are allowed to be streamed. Tags not included in this list will be discarded. • `minimum` : Includes the list of uastags as specified in MISB 0902. • `all` : Includes the list of uastags as specified in MISB 0601. • `none` : filters *out* everything for the given set.
`sectags`	off	A list of comma-separated tag numbers from the Security Local Data set inside the UAS that are allowed to be streamed. Tags not included. • `minimum` : Includes the list of sectags as specified in MISB 0102. • `all` : Includes the list of sectags as specified in MISB 0102. • `none` : filters *out* everything for the given set. **Note** `sectags` filtering requires `uastags tag #48` to be included as part of the list.
Static KLV Insertion parameters (See KLV Metadata Insertion)		
`missionid`		A string of up to 127 characters.
`reclassify`	off	(KLV input only) When set to on, enables reclassification of received UAS KLV messages.
`classification`	unclassified	Specifies the classification of the security data set: • `unclassified, restricted, confidential, secret, topsecret`
`classcountry`		The ISO 3166-1 3-letter code for the classifying country.
`objcountry`		The ISO 3166-1 3-letter code(s) for up to six object countries separated by semicolons.

Parameter	Default	Description/Values
CoT Retransmission parameters (See CoT Retransmission)		
`retransmit`	off	When set to on, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP.
`relays`		(Mandatory) Specifies the IP address and UDP port of the relayed packets. You can optionally specify the TTL and ToS. `ipaddr1:port1[:ttl1[:tos1]],ipaddr2:port2[:ttl2[:tos2]]..`
`ttl`	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `1..255`
`tos`	0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = `0..255` (decimal) or `0x00..0xFF` (hex) **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.
Serial and UDP Source-specific parameters		
`format`	KLV	Selects the data format for the metadata. • KLV • CoT **Note** CoT is only available from the serial port. For details on setting up CoT, refer to *Cursor-on-Target Capture from the Makito X*.
`spiuid`		(CoT input only) Specifies the UID of SPI (Sensor Point of Interest) messages to ingest.
`discovery`	Off	(CoT input only) When set to On, enables the discovery of SPI UIDs (User Identifiers) that will be shown in the stats output and can then be potentially used as the spiuid for SPI message filtering.

Parameter	Default	Description/Values
`delta`	0	(CoT input only) Specifies the maximum delta between SPI and Air Craft message timestamps for them to be considered a valid pair that can be converted to KLV.
Serial Source-specific parameters		
`standard`	RS232	Specifies the transceiver mode for the metadata capture: • RS232 • RS422 **Note** Only valid for the serial port.
`baudrate`	115200	Specifies the baud rate for the serial port: • 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200

Note

When a KLV over SDI metadata source is started but the input signal is not in a format supported for KLV extraction, its state in the statistics display will show up as “DISABLED”. The moment a supported signal (1080p or 720p) is present, KLV extraction will resume and the status will be updated to “WORKING”.

Related Topics

- metadata Command Examples
- Configuring Metadata Capture
- CoT Retransmission
- KLV Metadata Insertion
- Metadata Decimation
- UAS KLV Metadata Tag Filtering

metadata Command Examples

Example #1: Creating a Stream with Serial Metadata

[Source ID=0]

1. Set the baud rate for the serial port to 115,200 using the following command:

```
#metadata 0 set baudrate=115200
```

2. Start the serial metadata encoder instance:

```
#metadata 0 start
```

3. Create a stream with video, audio and metadata using the following syntax:

```
#stream create addr=<IPaddr> port=<UDPport> vid=0 aud=0 data=0
```

4. Verify the metadata encoder stats:

```
# metadata 0 get all
```

The system will return the metadata information:

```
Metadata ID : 0
Name : (None)
Configuration:
  Type : serial
    Format : KLV
    Device : "/dev/tts/0"
    Standard : RS-232
    Baud Rate : 115200
Statistics:
  State : STOPPED
    Rx Bytes : 0
    Rx OK Messages : 0
    Rx Corrupt Messages : 0
```

Example #2: Creating a Stream with SDI Metadata

[Source ID=1]

1. Start the SDI metadata encoder instance using the following command:

```
#metadata 1 start
```

2. Create a stream with video, audio and metadata using the following syntax:

```
#stream create addr=<IPaddr> port=<UDPport> vid=0 aud=0 data=1
```

3. Verify the metadata encoder stats:

```
# metadata 1 get all
```

The system will return the metadata information:

```
Metadata ID             : 1
Name                    : (None)
Configuration:
  Type                  : HD-SDI
    Format              : KLV
Statistics:
  State                 : STOPPED
    Rx Bytes            : 0
    Rx OK Messages      : 0
    Rx Corrupt Messages : 0
```

Example #3: Streaming with UDP Metadata

[Source ID=2]

1. Create a UDP metadata encoder instance using the following syntax:

```
metadata create [addr=<IP source>] port=<dest port>
```

Ex:

```
# metadata creat port=8500
```

The system will return the following message, including the UDP metadata ID:

```
Metadata source created successfully - ID: 2
```

2. Start the metadata UDP metadata encoder using the following syntax:

```
# metadata <ID> start
```

Ex:

```
# metadata 2 start
```

3. Create a stream with video, audio and metadata using the following syntax:

```
stream create [addr=<dest IP>] port=<dest port> vid=<id>
  aud=<id> data=<id>
```

Ex (showing multiple metadata stream):

```
# stream create addr=10.64.1.124 port=1234
 encap=ts-udp videosrc=1 audiosrc=1 datasrc=1,3
```

4. Verify the metadata encoder stats using the following syntax:

```
# metadata <ID> get all
```

Ex:

```
# metadata 2 get all
```

The system will return the metadata information:

```
Metadata ID             : 2
Name                    : (None)
Configuration:
  Type                  : Network
    Format              : KLV
    Address             : 0.0.0.0 (Any)|
    UDP Port            : 8500
Statistics:
  State                 : WORKING
    Rx Bytes            : 0
    Rx OK Messages      : 0
    Rx Corrupt Messages : 0
    Source Address      : 0.0.0.0
```

Example #4: Configuration Information for Multiple Metadata Sources

1. Get the metadata configuration information for the encoder using the following command:

```
# metadata get all
```

Returns configuration information for three metadata sources: (1) serial port source configured for CoT, (2) HD-SDI source configured for KLV, and (3) network source configured for KLV:

```
Metadata ID              : 0
Name                     : (None)
Configuration:
  Type                    : Serial
    Format                : CoT
    Status                : STOPPED
    Device                : "/dev/ttyO0"
    Standard              : RS-232
    Baud Rate             : 115200
SPI Sensor Discovery      : Off
  SPI UID                 : (Any)
  Max AirCraft-SPI Delta  : 0 ms
  CoT Relaying            : Off
  Number Of Relays        : 0
  Reclassification        : Off
    Classification        : UNCLASSIFIED
    Classifying Country   : (None)
    Object Country        : (None)
Metadata ID               : 1
Name                      : "HD-SDI-BNC-1"
Configuration:
  Type                    : HD-SDI
    Format                : KLV
    Status                : STARTED
    Reclassification      : Off
      Classification      : UNCLASSIFIED
      Classifying Country : (None)
      Object Country      : (None)
Metadata ID               : 2
Name                      : "KLV/UDP"
Configuration:
  Type                    : Network
    Format                : KLV
    Status                : STARTED
    Address               : 10.65.11.169
    UDP Port              : 20000
    Reclassification      : Off
      Classification      : UNCLASSIFIED
      Classifying Country : (None)
      Object Country      : (None)
```

Example #5: Creating Additional HD-SDI Metadata Sources

To create an additional HD-SDI metadata source and use it in a stream:

```
# metadata create name="Half the KLV of first input" type=hdsdi
    input=bnc1 decimation=2
Metadata source created successfully - ID: 3

# stream create addr=10.65.11.166 port=5678 vid=1 data=3
Stream created successfully - ID: 3

# stream 1 get
Stream ID : 1
Name : (None)
Configuration:
  Address : 10.65.11.166
  UDP Port : 5678
  Encapsulation: TS-UDP
  Contents : Video ("H.264 Video Encoder 1":1),
               MetaData ("Half the KLV of first input":3)
…
```

CoT Retransmission

You can configure retransmission of COT metadata received over the Serial or UDP interface. The metadata will be retransmitted as a CoT/UDP unicast or multicast stream so that multiple CoT listeners can access the source CoT data. You can retransmit up to eight (8) CoT/UDP messages. To do so, you specify the Destination Address (which can be a FQDN), UDP Port, TTL, and ToS.

Example

To define CoT Retransmission:

```
# metadata 3 set retransmit=on relays=10.65.129.65:2000:1:2,
    10.65.129.63:3000:3:4
```

The above example uses TTL and TOS values of 1 and 2, and 3 and 4, respectively. And ports 2000 and 3000, respectively.

Related Topics

- Configuring CoT Retransmission

KLV Metadata Insertion

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

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

or Top Secret), the classifying country, and the object country/ies (up to 6) (using the proper ISO 3-letter country code).

In both cases, the mission ID or security data will get replaced or inserted with the ones created by the Makito X based on the configuration.

Example

To define a mission ID (up to 127 characters long):

```
# metadata 1 set missionid="XYZ"
```

To unconfigure the insertion/modification of the mission ID element:

```
# metadata 1 set missionid=none
```

To enable security modification/insertion:

```
# metadata 1 set reclassify=on classification=confidential objcountry=afg
    classcountry=usa
```

To disable the insertion and modification of the security data set:

```
# metadata 1 set reclassify=off
```

Related Topics

- Configuring KLV Metadata Insertion

Metadata Decimation

KLV/SDI metadata sources can be frame-decimated to reduce the bandwidth used by the metadata service. You can also create additional HD-SDI sources linked to the same video input which can be configured to different decimation settings (as well as security reclassification and mission ID override) as needed. For example, you can have one high bitrate stream sending out all the KLV as well as a lower bitrate stream that uses KLV decimation. You can either specify a decimation factor for a metadata source or set the decimation rate to match a reference video encoder frame-rate. See **decimation** in the `metadata` parameters table.

Example #1: Metadata Decimation

To reduce the KLV bitrate on BNC-1 by half (i.e., divided by 2):

```
# metadata 1 set decimation=2
Metadata source configured successfully.
```

Example #2: Decimating at the Same Rate as a Video Encoder

To configure a metadata source to decimate at the same rate as a reference video encoder configured to use the same SDI input:

```
# metadata 1 set decimation=videnc0
Metadata source configured successfully.
```

Related Topics

- Configuring HD-SDI Metadata Sources

UAS KLV Metadata Tag Filtering

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

When filtering MISB 0601 metadata tag 48 (security metadata), you can also filter the security metadata tags defined in MISB 0102. See **uastags** and **sectags** in the `metadata` parameters table.

Example

To enable UAS tag filtering and list the items that will be included in the stream:

```
# metadata 1 set uastags=2,3,13,14,48 sectags=1,2,3
Metadata source configured successfully.

# metadata 1 get
Metadata ID             : 1
Name                    : "HD-SDI-BNC-1"
Configuration:
  Type                  : HD-SDI
  Input                 : BNC-1
  Format                : KLV
  Status                : STARTED
  Decimation            : (None)
  Reclassification      : Off
    Classification      : UNCLASSIFIED
    Classifying Country : (None)
    Object Country      : (None)

UAS Tag Filtering       : On
  Included Items:
    Tag 2 (UNIX Time Stamp)
    Tag 3 (Mission ID)
    Tag 13 (Sensor Latitude)
    Tag 14 (Sensor Longitude)
    Tag 48 (Security Local Metadata Set)
Security Filtering      : On
 Included Items:
   Tag 1 (Security Classification)
   Tag 2 (Classifying Country and Releasing Instructions Country Coding Method)
   Tag 3 (Classifying Country)
```

In order to show how the sectags option works, the main `uastags` filter includes the security local metadata set (tag #48) but only specifies the security classification, the country coding method and classifying country information. Note that you can set the MISB ST 0902 recommended minimum metadata set by specifying “minimum” for the `uastags` parameter.

To disable KLV tag filtering and receive the full KLV metadata:

```
# metadata 1 set uastags=all sectags=all
Metadata source configured successfully.
```

You can filter out the entire UAS or security data set by using "none" for `uastags` or `sectags` instead.

When security re-classification is enabled on a metadata source, the security tag filtering settings (if configured) will not be used.

Related Topics

- Filtering UAS KLV Metadata Tags

mklogo

In order to display an image as a logo overlay on the Makito X, you need to copy a still image file to the Makito X file system and then convert the file to Haivision's overlay image format (.oly). The image file can be in either BMP, JPEG, PNG, or GIF format. The `mklogo` command is used to convert the graphic file to .oly format.

The Makito X supports logos up to a maximum of 256 x 256 pixels. If you supply a larger image file, the converter scales it down, while keeping the aspect ratio. Logo files are stored on the Makito X file system under `/usr/share/haivision/logos`.

The .oly file can then be configured to display as a logo overlay in the encoded video. There can be one logo per Makito X.

Synopsis

```
mklogo <infile>
```

where:
`infile` is the name of the image file to convert into a logo.

Actions

N/A

Parameters

N/A

Example

```
# mklogo mylogo.jpg
```

Converts the file `mylogo.jpg` to `mylogo.oly`.

Related Topics

- logo
- Configuring Logo Overlays

mkstill

The `mkstill` command is used to convert a static picture into a file containing an encoded single H.264 GOP sequence. This is required in order to configure a Makito X stream with a static image that will replace the “real” video stream when streaming is paused.

> **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`.

Synopsis

```
mkstill <infile> resolution
```

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

Actions

N/A

Parameters

Parameter	Default	Description/Values
`resolution`		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 • WXGA3 for 1360x768 • WXGA4 for 1366x768 • WXGA+ for 1440x900 • SXGA+ for 1400x1050 • HD+ for 1600x900 • UXGA for 1600x1200 • WSXGA+ for 1680x1050 • WUXGA for 1920x1200

Example

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

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

Related Topics

- still
- Configuring Still Image Streaming

passthrough

On the Makito X with SDI, you can enable bi-directional serial passthrough for controlling serially attached devices such as PTZ controlled cameras. Both RS-232 and RS-422 are supported. The `passthrough` command is used to manage passthrough settings.

Synopsis

```
passthrough start
passthrough stop
passthrough set parameter=value [parameter=value...]
passthrough get [config, stats, all]
passthrough clear
enable_passthrough_on_serial_port
```

Actions

Action	Description
start	Starts listening for passthrough clients.
stop	Stops passthrough and disconnects any clients that were connected.
set	Configures passthrough settings. A series of one or more parameter=value pairs can be specified at once. See Parameters below.
get	**Tip** To display a summary of all the encoders in a table format, you can use passthrough all get table.
clear	Clears passthrough statistics.
help	Displays usage information for the passthrough command.
enable_passthrough_on_serial_port	Enables passthrough from the serial port.

Parameters

Parameter	Default	Description/Values
`standard`	RS232	Specifies the transceiver mode for the passthrough: • RS232 • RS422 **Note** Only valid for the serial port.
`baudrate`	9600	Specifies the baud rate for the passthrough: • 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200
`databits`	8	Specifies the number of data bits in each character. • 8, 7
`stopbits`	1	Specifies the number of stop bits sent at the end of every character. • 1, 2
`flowctrl`	none	The flow control for the serial port: • none, xonxoff **Tip** Flow control is useful in atypical cases such as when the remote controlling device's serial port is set to a much higher baud rate than the encoder's serial port.
`port`	7777	The TCP port on which to listen for passthrough clients.
`timeout`	0 (no timeout)	**Tip** You can use 0 for an infinite timeout to keep the connection open until the client closes it.

Example

This example shows how to use TCP port 8888 to listen for passthrough clients. The camera has an RS232 COM port running at 9600 bps:

```
# passthrough set port=8888 baudrate=9600 standard=rs232

Passthrough configured successfully.

# passthrough get
Configuration:
  TCP Port            : 8888
  Standard            : RS-232
  Baud Rate           : 9600
  Flow Control        : None
  Disconnect Timeout  : None
```

If passthrough is not started, you will have to start it:

```
# passthrough get stats
Statistics:
  State           : DISABLED

# passthrough start
Passthrough started successfully.

# passthrough get stats
Statistics:
  State           : LISTENING
  Caller Address  : 0.0.0.0
  Network:
    Rx Bytes      : 0
    Tx Bytes      : 0
  Serial:
    Rx Bytes      : 0
    Tx Bytes      : 0
```

Passthrough Statistics

When a remote client is connected, the state will show up as CONNECTED and the IP address of the client will be displayed.

The statistics are divided in two sections: network and serial.

- The network stats show what is going in terms of the TCP connection with the remote controller, i.e., how many bytes were received from and sent to the remote controller.
- The serial stats show how many bytes were sent to the serial device connected to the encoder and how many were received from it.

In normal operation the number of bytes received on the TCP connection would match the number of bytes sent on the serial port and the number of bytes received on the serial port would match the number sent on TCP. However, if the device connected to the Makito X sends serial data when no client is connected, these numbers won't match.

Additional stats can show up under special conditions, as explained below:

Statistic	Description
Network dropped bytes	This counter shows the number of bytes received on the encoder's serial port that could not be sent over the TCP link. The network connection will always be orders of magnitude faster than the serial port connection so this statistic is seldom seen
Serial Dropped bytes	This counter shows the number of bytes received on the network connection that could not be sent on the serial link. Again if the controlling remote device and the encoder are set to the same baud rate, it is unlikely that the encoder would receive data at a rate that can't be accommodated. If, however, the baud rates don't match and the remote device is set to a higher value, this could occur. In that case, it is a good idea to reconfigure the remote device or use flow control.
Flow Control Stats	When flow control is used, the network section of the stats will display the number of XON and XOFF control bytes sent to the remote device over TCP. This indicates whether or not data from the controlling device was sent too fast to be forwarded to the encoder's serial port. When flow control is used, the Makito X will queue up to 2 seconds of serial data at 115,200 bps locally from the remote device. If the remote device also supports XON XOFF (otherwise, do not use flow control), this ensures that no data is ever lost from it.

Related Topics

- Enabling and Disabling Network Services
- service

record

The `record` command is used to create and manage video recordings. For more information, see Configuring Recording Outputs and Managing Recordings.

Synopsis

```
record create stream=id
record ID start
record ID stop
record ID close
record ID get
record list
record delete [filename, all]
record copy filename usb
record move filename usb
```

Actions

Action	Description
create	Creates a recording for a stream. A series of one or more parameter=value pairs can be specified at once. See Parameters below.
start	Starts recording a stream.
stop	Stops recording a stream.
close	Closes a recording of a stream
get	**Tip** To display a summary of all the streams in a table format, you can use record all get table.
list	Lists the available recordings on the system.
delete	Deletes either the recording specified by `<filename>` or all recordings.
copy	Copies the recording specified by `<filename>` to a USB device
move	Moves the recording specified by `<filename>` to a USB device and deletes the recording from the encoder.

Parameters

Parameter	Default	Description/Values
`name`		The identifying prefix for recorded files. If not specified, the stream name or ID will be used.
`format`	ts	The file format for recordings, either: • mp4 • ts

Parameter	Default	Description/Values
`limit`		The recording duration or size, ex 1h30m, 500M
`segment`		Enables segmented recording by specifying the duration or size of each segment.
`recycle`	off	When segmented recording is enabled and the recording is limited in space or time, this enables the overwriting of older segments when that limit is reached.
`subtitles`	off	When recording in mp4 format, this enables the generation of SubRip files to save any closed caption present in the stream being recorded.
`start`	off	Starts recording directly at recording creation time. The IDs of recordings always match the ID of the stream associated with it.
`export`	off	Exports recordings and segments automatically when they are complete.
`destination`		The destination of recording transfers when export is enabled. • `id` or `name`
`delete`	off	Deletes recordings when they are successfully transferred. The IDs of recordings always match the ID of the associated stream.

Examples

```
# record all get
```

Records information for the recording, for example:

```
Recording ID  : 1
Recording Name : "continuous"
Configuration:
  Format      : TS
  Recording Limit : 5d5h
  Segmented   : On
  Segment Limit : 10m
  Segment Recycling : Off
  Auto-Export : Off
```

```
# record list
```

Lists the available recordings, for example:

```
Recordings (in /mnt/storage1/recordings/):
  Test-2015-04-10-14h11m09s.mp4     (1920x1080, 36s, 25.66MB, root)
  REC-2015-04-12-21h11m06s.mp4      (1920x1080p29, 23s, 16.55MB, root)
  TEST-2015-04-12-23h20m20s.mp4     (1280x720p60, 2h41m12s, 43.50MB, root)
  TEST-2015-04-13-10h10m15s.mp4     (1280x720p60, 27m36s, 35.70MB, root)
  TEST-2015-04-13-10h38m56s.mp4     (1280x720p, 1m, 35.59MB, root)
  TEST-2015-04-14-11h52m05s.mp4     (1280x720p, 1m, 41.51MB, root)
  TEST-2015-04-14-13h50m52s.ts      (1280x720p60, 3h34m49s, 44.77MB, root)
  TEST-2015-04-14-17h26m45s.ts      (1920x1080i29, 1m, 44.24MB, root)
  continuous-2015-05-19-12h16m12s (Segmented, 1920x1080p30, 20h34m49s,
    222.34GB, root)

9 recordings are available.
222.81GB (100%) of 222.81GB recording disk storage space used.
```

Related Topics

- Configuring Recording Outputs
- Managing Recordings

roi

(H.264 only) The `roi` command is used to create a static region of interest (one per video encoder) to enhance the quality of the encoded video within the region. This allows you to choose what portion of the image is important to have maximum quality.

The region position can either be relative (top left, top right, centered, etc.) or absolute (positioned at the exact X and Y coordinates specified). You can also specify the scaling and transparency display settings.

Synopsis

```
roi create
roi ID set [parameter=value]
roi ID delete
roi ID get
roi ID enable
roi ID disable
```

Actions

Action	Description
create	Creates a region of interest on an encoder.
set	Configures ROI parameters. A series of one or more `parameter=value` pairs can be specified at once. See Parameters below.
delete	Removes the region of interest.
get	Displays information on the region of interest.
enable	Enables a created but disabled region of interest
disable	Disables a created region of interest

Parameters

Parameter	Default	Description/Values
`name`	n/a	Optional name for this region of interest.
`encoder`	n/a	Specifies the ID of the video encoder.
`type`	normal	Specifies the effect of the region: • normal: ROI is translucent, therefore enhances the video in the region. • privacy: ROI is opaque to block out the ROI video.
`emphasis`	4	Sets the difference in quality between the background and the ROI. 1 to 8

Parameter	Default	Description/Values
`positioning`	Centered	Specifies where the region should appear: • BottomRight • TopRight • BottomLeft • Centered • Absolute: Uses the exact X and Y coordinates.
`x`	910	Horizontal coordinate of the top left point of the region in Absolute mode.
`y`	490	Vertical coordinate of the top left point of the region in absolute mode.
`width`	100	Width in pixels of the region of interest.
`height`	100	Height in pixels of the region of interest.
`border`	none	Applies a border to the region: • `none, corners, box`
`enable`	on	Enables the region of interest. `on,off`.

Example

```
# roi 0 set type=privacy
```

Sets the region of interest type to privacy, i.e., opaque to block out the ROI video.

Related Topics

- Region of Interest (ROI) (H.264 only) under Video Encoder Settings

session

The `session` command is used to manage Session Announcement Protocol (SAP) multicast advertising sessions on the encoder.

Synopsis

```
session create stream=id/name name=sessname advertise=yes/no
 description=text keywords=text author=text copyright=text
 [id=number] [addr=advipaddr] [port=advudpport]

session id/name delete
session id/name start
session id/name stop
session id/name get
```

Actions

Action	Description
create	Creates an SAP session on the encoder. A series of one or more `parameter=value` pairs can be specified at once.
delete	Deletes the specified SAP session.
start	Starts the specified SAP session.
stop	Stops the specified SAP session.
get	Displays configuration information for the specified SAP session.

Parameters

Parameter	Default	Description/Values
`stream`	n/a	**Tip** Use `"stream get all"` to find the available streams and their IDs.
`name`	n/a	(Optional) Enter a unique name for the session. 1 to 63 characters
`advertise`	no	Enables or disables SAP network announcements.
`description`	n/a	(Optional) Enter an expanded description of the session.
`keywords`	n/a	(Optional) Enter one or more keywords to associate with the session. Keywords can serve as filters.
`author`	n/a	(Optional) Enter the name of the program's author.
`copyright`	n/a	(Optional) Enter the copyright information for the session.

Parameter	Default	Description/Values
[id]	n/a	**Note** When creating an SAP session, you can specify a unique id to assign to it or let the system assign one (a sequential number) for you.
address	Based on the stream's destination IP address	(Optional) Use to overwrite the default to use specific non-standard advertising addresses for SAP messages.
port	9875	Enter the SAP advertising UDP port.

Example

`# session 1 get`	Returns SAP session configuration information for the encoder, such as:
	`Session ID : 1`
	`Name : "InfoDevSAP"`
	`Configuration :`
	` Description : "Test to document session command"`
	` Keywords : "session"`
	` Author : (None)`
	` Copyright : "2018"`
	` Advertise : Yes`
	` Advertisement Address : Auto-Assign (224.2.127.254)`
	` Advertisement Port : 9875`
	` Streams : 8`

Related Topics

- Session Announcement Protocol (SAP)

snapshot

The `snapshot` command is used to take and manage snapshots from the video received on any input port. You can save the snapshots in JPEG or YUV format. Also, when saving in JPEG format, you can specify the compression ratio to determine the image quality. You can also specify the location where the snapshot is stored. Snapshots can be stored on a mounted SSD, SD, USB or NFS media, or within the on-board NAND flash.

When taking a snapshot of the current video input, the filename is optional. If none is specified, a unique name will be generated based on the current time if NTP is enabled, or a simple index such as snap-1.jpg if NTP is not enabled. To overwrite an existing file, use the `overwrite=yes` option and specify the filename when capturing the snapshot. You can specify different formats and quality per snapshot in the `snapshot take` command. You can also set system-wide defaults for the preferred snapshot format and quality via the `snapshot set` command.

Tip

Thumbnail generation can be disabled to speed up snapshot acquisition and storage time.

ID is used to select the video input on dual channel encoders (either 0 for BNC-1 or 1 for BNC-2 on #S/B-292E-HDSDI2). ID is optional on single input encoders such as the #S/B-292E-HDSDI1 and the #S/B292E-DVI. If entered, only 0 will be accepted.

Configuring a limit on the storage space available for snapshots is only valid for flash, SSD, or NFS locations. For USB and SD locations, any available space will be used without constraint.

Synopsis

```
snapshot ID take [format=value] [filename=<filename> [overwrite=yes,no]]
  [quality=value]
snapshot set [format=value] [quality=value] [maxsize=value] [location=value]
  [thumbnail=on,off] [overwrite=yes,no]
snapshot get
snapshot list
snapshot delete [<filename>, all]
```

Actions

Action	Description
take	Takes a snapshot from either: • the current active video (Makito X DVI, S/B-292E-DVI or Makito X SDI single-BNC, S/B-292E-HDSDI1) • the video received on any input port, where ID is the video input (Makito X SDI dual-BNC, S/B-292E-HDSDI2). ID is either 0 for BNC-1 or 1 for BNC-2. You can optionally specify the format and image quality per snapshot, as well as the filename.
set	Sets system-wide defaults for the preferred snapshot format and quality.
get	Displays the current format and quality defaults for the snapshot utility.

Action	Description
list	Displays the available snapshots on the system along with the resolution. Snapshot files are stored under /usr/share/haivision/snapshots.
delete	Deletes either the snapshot specified by `<filename>` or all snapshots stored under `/usr/share/haivision/snapshots`.

Parameters

Parameter	Default	Description/Values
`format`	jpeg	**Note** YUV snapshots always have the best possible quality but take the most amount of space.
`overwrite`	no	(Only applies when a filename is provided) When enabled, any existing snapshot file with the same filename will be overwritten. `yes,no`
`quality`	100	Specifies the desired image quality from 1 (lowest) to 100 (highest). `1..100` **Note** This setting only applies for jpg snapshots
`maxsize`	100 MB	(Users must be assigned Administrator role) Specifies the amount of storage in MB available to snapshots. -1, 0..4096 • `0` disables the snapshot feature. • `-1` is used for unlimited storage and is only available when the location is an NFS-mounted drive.
`location`	Internal Flash	Specifies the storage location, either: • flash - Internal on-board NAND flash • ssd - SATA Solid State Drive • sd - Secure Digital card • usb - Universal Serial Bus Mounted media • nfs - Network file system
`thumbnails`	on	When set to On, enables thumbnail generation for snapshots. `on,off`

Examples

```
# snapshot 0 take format=jpg filename=mysnaphot.jpg quality=80
```

Takes a single image snapshot (immediately) in JPEG format at 80% image quality and stores it under the filename mysnapshot.jpg.

```
# snapshot set format=jpg quality=80
```

Sets the system-wide defaults for the preferred snapshot format to jpg at 80% image quality.

`# snapshot set location=ssd` Sets the snapshot storage location to an SSD.
`# snapshot set thumbnail=off` Disables thumbnail generation for snapshots.

`# snapshot get`
 	
Returns the system-wide settings for the snapshot format, for example:
`Current Defaults:`
`  Format  : JPEG`
`  Quality  : 100`
`  Thumbnails  : On`
`  Storage Device  : Internal Flash`
`  Max Storage  : 100MB`

`# snapshot list`
 	
Lists the contents of the snapshot folder:
`Snapshot Files (in /usr/share/haivision/snapshots/):`
`  snap-2015-05-01-11h58m15s.jpg (BUSY)`
`  snap-2015-05-01-11h58m39s.jpg (BUSY)`
`  snap-2015-05-01-12h00m25s.jpg (BUSY)`
`  snap-2015-05-01-12h03m19s.jpg (BUSY)`
 	
`4 snapshot files are available.`
`5.90MB (5%) of snapshot disk storage space used.`

Related Topics

- Capturing Image Snapshots
- Managing Snapshot Storage Locations

still

The `still` command is used to manage available still image files on the Makito X file system. Static image files must already have been converted into files containing encoded single H.264 GOP sequences and be located the folder `/usr/share/haivision/still_images` on the Makito X file system. 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 `stream set` command with the parameter `[stillimage=fname]`. See **stream** for details.

> **Note**
>
> You can convert the image file either using the **mkstill** command, or from the Web interface Still Images page (see **Configuring Still Image Streaming**).

Synopsis

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

Actions

Action	Description
list	Lists the available still image files in `/usr/share/haivision/still_images`
delete	Deletes a single image file.

Parameters

N/A

Example

```
# still delete myimage.mp4
```

Deletes the image file myimage.mp4

Related Topics

- **mkstill**
- `stillimage` in **stream** Parameters
- **Configuring Still Image Streaming**

stream

The `stream` command is used to manage audio/video streams. The `type` parameter only needs to be specified when creating a stream that will be used solely for recording and not sent on any network. For that specific use, use `type=recorder` and simply specify the content sources.

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

On Makito X HEVC units, to create an HEVC stream, specify 4 or 5 instead of 0 to 3 for the `videosrc` id.

When a stream has started, you may either pause or stop it. The main difference between pausing and stopping a stream is that when a stream is paused, the configured still image will be streamed instead of the configured video source. For more information, see **Configuring Still Image Streaming**.

Synopsis

```
stream create [type=tx] [name=text] [id=number]
 [addr=ipaddr] [port=udpport]
 [encapsulation=ts-rtp | ts-udp | direct-rtp | rtmp | ts-srt]
 [start=yes,no] [ttl=64] [tos=0xB8] [mtu=1496] [videosrc=id/name]
 [audiosrc=id/name[,id/name,id/name]] [datasrc=id/name[,id/name,id/name]]
 [stillimage=fname] [shaping=yes,no [ceiling=percentage] [idlecells=yes,no]
 [delayaudio=yes,no]] [datacarriage=sync | async | async-syncau]
```

Possible encapsulation formats and their specific options:

```
 ts-rtp: MPEG2 transport stream over RTP
   [rtcp=on [rtcpport=udpport]] [fec=yes,no] [rows=10] [columns=10]
   [level=A, B] [alignment =yes, no]
 ts-udp: MPEG2 transport stream over UDP (no RTP header)
   [fec=yes,no]
 direct-rtp: RFC3984
   [rtcp=on [rtcpport=udpport]]
 rtmp: Real-time messaging protocol
   [publish=streampubname] [username=uname] [password=pwd]
 ts-srt: MPEG2 transport stream over SRT
   [mode=caller, listener, rendezvous] [sourceport=udpport]
   [encryption=none, AES128, AES256] [passphrase="My PassPhrase"]
   [latency=250] [overhead=percentage] [adaptive=yes,no]
```

Parameters available for all ts-based streams:

```
 [videopid=pid] [audiopid=pid[,pid,pid]] [datapid=pid]
 [pcrpid=pid] [pmtpid=pid]
 [program=num] [tsid=id]
```

```
stream id/name stop
stream id/name pause
stream id/name resume
stream id/name delete
stream id/name/all get
stream id/name clear
```

Actions

Action	Description
create	Creates a streaming session from the encoder. A series of one or more `parameter=value` pairs can be specified at once.
start	**Note** By default, a stream will start immediately since start=yes by default. To delay the start of a stream, include the parameter start=no.
stop	Stops the specified stream ID or name.
pause	**Note** If configured, a still image will be streamed instead of the configured video source. See “stillimage” in Parameters below.
resume	Resumes the specified stream ID or name.
delete	Deletes the specified stream ID or name.
get	Gets stream status information. See Parameters below. You can specify a stream or all streams. **Tip** To display a summary of all the streams in a table format, you can use stream all get table.
clear	Clears all active sessions on the encoder.
help	Displays usage information for the stream command.

Parameters

Parameter	Default	Description/Values
`type`	tx	**Note** `type` only needs to be specified when creating a stream that is used solely for recording and not sent on any network. For that specific use, use `type=recorder` and simply specify the content sources.
`addr`	n/a	The destination IP address. Enter an IP address in dotted-decimal format. **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`).

`port`	n/a	The destination UDP port. Enter a number in the range `1025..65,535`. Note that RTP streams use even numbers only within this range.
Optional		
`id`	n/a	**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 select the proper stream to manage.
`name`	n/a	(Optional) When creating a stream, you can also specify a name for the stream. `1` to `32` characters

`rtcp`	on	(Optional) When `rtcp` is On, the stream is activated in RTCP mode. This causes the system to establish one RTP stream and one RTCP session for monitoring purposes. RTP/RTCP is useful to collect network metrics such as network jitter, packet loss, etc. Note that this requires a remote decoder capable of supporting this feature as well.
`rtcpport`	n/a	(Optional, `rtcp` must be On) The destination UDP port for the RTCP session.
`ttl`	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = `1..255`
`tos`	0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = `0..255` (decimal) or `0x00..0xFF` (hex) **Important** A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474. **Note** The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.
`mtu`	1496	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing RTP data stream. `228..1500`
`encapsulation`	ts-udp	(Optional) The Encapsulation Type for the encoded stream. • `ts-rtp:` MPEG2 transport stream over RTP • `ts-udp:` MPEG2 transport stream over UDP (no RTP header) • `ts-srt:` MPEG2 transport stream over SRT (see Configuring Secure Reliable Transport (SRT)) • `direct-rtp:` (H.264 only) RFC3984 • `rtmp` : (H.264 only) Streams to a Flash Media Server or Content Delivery Network (see CDN Interoperability (RTMP)).
`start`	yes	(Optional) By default, the stream will start immediately. To delay the start of a stream, specify `start=no`. You can enter a `stream start` command later.

`videosrc`	0	(Optional) The video source (ID/Name). For H.264, the `id` is either `0`, `1`, `2`, or `3` (corresponding to the encoder instance number in the Web interface). For HEVC encoders, two additional `ids` of `4` and `5` are available and should be used to stream HEVC-encoded video. **Note** By default, if you don't specify the source, the stream uses video encoder `0` and audio encoder `0` for a TS stream (UDP or RTP), and video encoder `0` for DirectRTP and other encapsulations. Once you specify an audio or video source, you have to enter all of them explicitly. For example, even though a TS stream with no sources specified automatically uses video `0` and audio `0`, if you specify that video `0` is your source, then you must enter the audio source or else the stream will not have any audio in it. **Tip** Combined videosrc/audiosrc/datasrc status shown under Contents in return output.
`audiosrc`	0	(Optional) The audio source (ID/Name). The `id` is either `0`, `1`, `2`, `3`, `4`, `5`, `6`, or `7`. See Note and Tip above in the videosrc description. **Note** To configure multi-track audio TS streams (TS over UDP or RTP), you can put more than one `audiosrc` (audio encoder) in the stream. See "Examples" below. **Important** Audio sources should always be associated with the same video interface for the dual channel SDI encoder. (See Setting Up Streaming.)
`datasrc`	n/a	(Optional) The metadata source. `id/name` (`0=serial, 1 or 2=SDI;` all others are `UDP`) See metadata to determine the ID mappings. **Note** To stream metadata from multiple sources into the same KLV Elementary Stream, use multiple comma separated metadata source id/names to indicate the metadata source ES IDs to be multiplexed in the stream. e.g.: `stream create ….. data=1,2`
`videopid`	33	(Optional) Video Packet Identifier. 16-8190

`audiopid`	36	(Optional) Audio Packet Identifier. 16-8190. For MPEG-2 TS streams, the audio PIDs for each audio source can be assigned explicitly. The order of PID assignment is the same as the audiosrc parameters. e.g.: `audiosrc=0,1,3 audiopid=64,65,66` will result in the audio elementary stream from audio source `0` being assigned an elementary PID of `64`, etc.
`datapid`	40	(Optional) Data (metadata) Packet Identifier. 16-8190
`prcpid`	34	(Optional) (Program Clock Reference) Packet Identifier. Timestamp in the TS from which the decoder timing is derived. `16..8190`
`pmtpid`	32	(Optional) (Program Map Table) Packet Identifier. 16-8190
`program`	1	(Optional) Program Identifier used in the Program Map Table (PMT) of the TS stream. 0-65535
`tsid`	0	(Optional) Transport Stream ID. Identifies the transport stream in the Program Association table (PAT) of the TS stream. 0-65535
`stillimage`	n/a	**Note** The static image file must already have been converted into a file containing an encoded single H.264 GOP sequence. You can either use the mkstill command, or the Web interface's Still Imagespage (see **Configuring Still Image Streaming**). Still Image insertion when pausing a stream is not supported when a HEVC/H.265 video encoder is selected as a content source.
`shaping`	no	(Optional) To enable Traffic Shaping for the stream, specify `shaping=yes`. For some limited networks such as satellites or some dedicated network pipes, it may be necessary to enable Traffic Shaping to smooth the traffic and respect the absolute upper limit configured. **Note** Using Traffic Shaping on streams above 7Mbps will create audio/video artifacts.
`ceiling`	n/a	(Optional, shaping must be `yes`) The percentage of network bandwidth beyond the average rate that the encoder is allowed to use if needed. This is used to set the ceiling bandwidth range. `5..100%`, default = `15` **Note** To configure the ceiling percentage for CBR streams with metadata, see **Bandwidth Overhead for CBR Streams with Metadata**.

`idlecells`	no	(Optional, shaping must be `yes`) When enabled, Idle TS cells will be inserted into a TS stream when necessary. `yes,no`
`delayaudio`	no	(shaping and idlecells must be `yes`) When enabled, delays the transmission of audio information to prevent MPEG-2 TS HRD main buffer overflows. Per reference decoder main audio buffer defined in IEC/ISO 13818- 1/H.222.0. `yes,no`
`datacarriage`	sync	Specifies the method of KLV data carriage: • `sync`: synchronous metadata AU (ISO/IEC 13818-1) • `async`: asynchronous private data (SMPTE RP 217) • `async-syncau`: asynchronous private data carrying sync metadata AU
`publish`	n/a	**Note** A single Publish Name may be assigned to multiple streams, configured on separate servers or content distribution services, to provide redundancy and fail-over capability. The encoder will send multiple RTMP streams to different FMS servers using the same published name. If an FMS fails, the players will have the option of fail-over to the redundant FMS server. **Important** When interoperating with Kaltura using RTMP, add a slash "/" at the end of the URL provided by Kaltura. See CDN Interoperability (RTMP).
`username`	n/a	(Required when streaming to a CDN using RTMP) Enter the CDN login username.
`password`	n/a	(Required when streaming to a CDN using RTMP) Enter the CDN login password.
`fec`	no	Enables Forward Error Correction (FEC). `yes,no` • Pro-MPEG FEC if encapsulation is `ts-rtp` • VF FEC if encapsulation is `ts-udp` **Note** VF FEC is a proprietary FEC and is not interoperable with devices outside of the Haivision family.
SRT (see Configuring Secure Reliable Transport (SRT))		
`mode`	caller	Specifies the SRT Connection Mode: • caller • listener • rendezvous
`sourceport`	auto	(SRT connection mode must be caller) Specifies the UDP source port for the SRT stream.
`encryption`	none	(encapsulation must be `ts-srt`) Enables AES encryption and specifies the key length, either: none, AES-128, or AES-256

`passphrase`	n/a	(Only required and accepted if `encryption` is enabled, encapsulation must be `ts-srt`) Specifies a string used to generate the encryption keys to protect the stream. Range = 10-79 UTF8 characters
`latency`	250	(encapsulation must be `ts-srt`) Specifies the SRT receiver buffer that permits lost packet recovery. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). **Note** Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the endpoint devices.
`overhead`	25%	(encapsulation must be `ts-srt`) Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-50%
`adaptive`	no	(encapsulation must be `ts-srt`) When set to `yes` enables Network Adaptive Encoding. NAE directs the video encoder to adapt to changing network throughput used by the SRT stream during operational use with the goal of maximizing video quality for a given network. NAE may adjust video bitrate depending on measured link throughput without stream tear-down and re-build.

Examples

```
# stream create addr=192.0.2.106 port=2000 start=yes
```

Creates a streaming session to IP Address 192.0.2.106 at port 2000; starts streaming immediately. Returns the following confirmation and stream ID:

```
Stream created successfully - ID : 3
```

```
# stream create addr=192.0.2.235 port=1234 stillimage=haivision.mp4
```

Creates and starts a streaming session. Specifies a static image to replace the "real" video stream when streaming is paused.

```
# stream create addr=10.64.1.124 port=1234 encap=ts-udp videosrc=1 audiosrc=1
datasrc=1,3
```

Creates and starts a multiple metadata streaming session.

```
# stream create addr=10.64.1.124 port=1234 encap=ts-udp videosrc=1
audiosrc=0,2,4 audiopid=36,37,38
```

Creates a TS stream with multi-track audio using audio encoders 0, 2 and 4. The corresponding audio PIDs are 36, 37 and 38.

```
# stream 3 pause
```

Pauses the stream created above (stream ID 3), which activates the still image.

```
# stream 3 resume
```

Resumes the stream created above.

```
# stream create addr=192.0.2.235 port=1234 vid=0 aud=0
# videnc 1 start
# audenc 1 start
# stream create addr=198.51.100.106 port=1234 vid=1 aud=1
```

Creates two streams, the first using Video and Audio encoder 0, and the 2nd using Video and Audio encoder 1.

```
# stream create addr=192.0.2.235 port=1234 videosrc=4 audiosrc=0
```

Creates an HEVC stream using video encoder 4.

```
# stream 1 get all
```

Returns configuration information and statistics for all encoder streams, for example:

```
Stream        : 1
Name          : "web1"
Configuration :
  Address     : 192.0.2.235
    UDP Port  : 1234
    Encapsulation           : TS-RTP
    Contents                : Video ("HD Video Encoder 0":0),
                              Audio ("Audio Encoder 0":0)
    Still Image File        : (None)
    Video PID               : 33
    Audio PID               : 36
    PCR PID                 : 34
    PMT PID                 : 32

    Transport Stream ID     : 0
    Program Number          : 1
    MTU                     : 1500
    TOS                     : 0xB8
    TTL                     : 18
    Bandwidth               : 6,510 kbps
    Traffic Shaping         : Off
    AES Encryption          : On
    FEC                     : On
Persistent : No
Statistics :
  State                     : STREAMING
  Up Time                   : 1h16m8s
  Sent Packets              : 1,040,512
  Sent Bytes                : 1,252,450,560
Bitrate                     : 198 kbps
```

```
# stream 2 show stats
```

Returns status information for Stream #2, such as:

```
Session ID : 2
  Name              : "web1"
Statistics :
  State             : STREAMING
  Up Time           : 10m50s
  SSRC              : 0x94328a6a (2486340202)
  Sent Packets      : 413,274
  Sent Bytes        : 417,249,304
  Unsent Packets    : 1,214
  Unsent Bytes      : 1,272,100
  Last Error        : 11, Resource temporarily unavailable
Ocurred             : 6hr44m4s ago
RTCP                : Off
```

```
# stream 1 del
```

Deletes Stream #1.

Related Topics

- Configuring Streaming Outputs
- Setting Up Streaming

talkback

The `talkback` command is used to manage audio talkback settings. 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. See Audio Talkback.

The talkback is sent by a software player application (such as Haivision's InStream or the Makito X decoder) to the Makito X, where it is played out of the encoder's 8-pin Mini-DIN connector. To develop custom applications to send talkback audio to Haivision encoders, see Talkback Audio Format Specifications.

> **Note**
>
> The source UDP port of sender does not matter; however, the destination has to match what is configured on the encoder (`9177` by default).

There is no audio mixer on the Makito X, so the encoder handles the talkback sessions on a first-come first-serve basis. To prevent a single user from monopolizing the talkback, the InStream software player provides "push-to-talk" functionality, which requires that the talkback user physically push and hold a button to transmit audio. When the button is released, the talkback application stops sending audio. The Makito X considers the session terminated if it does not receive a packet for a duration of one second (i.e., after at least one second of inactivity). The Makito X is then ready to accept the session (talkback packets) from another device.

The Talkback network service may be stopped or started from the Web interface (Services page) or using the service command.

> **Tip**
>
> It's a good idea to save your configuration if you are running Talkback in order to avoid having to restart Talkback after a reboot.

Synopsis

```
talkback start
talkback stop
talkback set
talkback get
talkback clear
```

Actions

Action	Description
start	Starts reception of talkback audio.
stop	Stops reception of talkback audio.
set	Configures talkback settings.

Action	Description
get	Displays talkback information (i.e., volume and UDP port). You can specify configuration, stats, or all talkback information.
clear	Clears talkback statistics.

Parameters

Parameter	Default	Description/Values
`volume`	10	Controls the volume on the Encoder's audio output port. Range: 0-10

Example

```
# talkback start
```

Starts reception of audio talkback on the Makito X.

```
# talkback set volume=6
```

Sets the volume of the audio talkback to 6.

```
# talkback get all
```

Returns talkback configuration and statistics, such as:

```
Configuration:
  Volume           : 10
  UDP Port         : 9177
Statistics:
  State            : LISTENING
  Source Address   : 10.65.134.102
  Received Packets : 1,087
  Received Bytes   : 960,908
  Last Received    : 2s ago
```

Related Topics

- Audio Talkback
- Talkback Audio Format Specifications

Talkback Audio Format Specifications

Haivision's InStream software player provides a talkback audio stream to the encoder. The InStream player is available either with the Furnace IP Video System v6.x or as a mobile application. For more information, see the *InStream User's Guide* or the *InStream Mobile (iOS or Android) Quick Start Guide* available through Haivision's Download Center.

The following specifications are provided for customers or system integrators who choose to develop their own applications to send talkback audio to Haivision encoders:

1. Audio data in each payload is uncompressed PCM digitized audio. There is no encoding/decoding involved.
2. Transmitted over unicast UDP (only port 9177) to the Makito X.
3. Audio sampling rate = 22.05 kHz (44.1 divided by 2).
4. Each audio sample is a raw 16-bit PCM (LSB First).
5. Mono audio only.
6. Each UDP packet contains 440 samples.
7. UDP payload is 880 bytes minimum. (Anything beyond the 880th byte is discarded.)
8. There is no audio mixing; one audio channel at a time: first in / first served. The talkback application software should be equipped with "push-to-talk" type of feature.
9. The talkback service locks out all other talkback sources for 500-ms period during which time only a single identified source may be played.
10. Once an end-point has acquired the talkback interface, it maintains control of the talkback interface until audio is no longer streamed to the Makito X for 500 ms.
11. If the audio input is disconnected, the application does not need to send filler zero (silence) bytes, because talkback on the Makito X inserts zeros (silence) to maintain the output audio clock.
12. Talkback audio is output over the mono analog "Audio Out" connector on the Makito X encoder.

temperature

The `temperature` command is used to display the current temperature of the unit. If the internal temperature of the unit is rising, that is an indication that the fan may not be operating properly.

Synopsis

```
temperature get
```

Actions

Action	Description
get	Displays the current temperature status of the unit.

Parameters

N/A

Example

```
# temperature get
```

Displays the current temperature for the unit, see example below:

```
Temperature Status :
  Current Temperature   : 47 Celsius measured 0s ago
  Maximum Temperature   : 48 Celsius measured 1d5h8m48s ago
  Minimum Temperature   : 45 Celsius measured 1d5h37m7s ago
```

videnc

The `videnc` command is used to manage video encoding parameters. The `videnc start` and videnc `stop` commands can be used to start and stop encoding of the video input. ID is either the encoder ID (0, 1, 2, or 3) or all. On Makito X HEVC units, the HEVC encoder uses ID 4 and 5.

Synopsis

```
videnc ID start
videnc ID stop
videnc ID set parameter=value [parameter=value...]
videnc ID get [config, stats, all]
videnc ID clear
videnc ID reset
```

Actions

Action	Description
start	Activates encoding of the video input.
stop	Stops (mutes) encoding of the video input.
set	Configures encoder video parameters. A series of one or more `parameter=value` pairs can be specified at once. See Parameters below.
get	**Tip** To display a summary of all the encoders in a table format, you can use `videnc all get table`.
clear	Clears the encoder's statistics.
reset	Resets the encoder.
help	Displays usage information for the `videnc` command.

Parameters

Parameter	Default	Description/Values
`input`		(SDI Dual-BNC only) The Video Input port for the encoder: • BNC1 • BNC2

Parameter	Default	Description/Values
`timecode`	None	Timecodes are used to mark video frames, mainly for editing purposes. This field either disables timecoding, or selects the source to "timecode" the encoded video frame. The following selections are available: • `None`: No time code will be inserted in the video stream (saves bandwidth if not required). • `Video`: (SDI only) The timecode will be extracted from the incoming video signal. • `System`: If no timecode is included in the video feed, the encoded timecode is based on the encoder's system clock. In this case, it is a good idea to enable NTP (see Configuring Network Settings). **Note** See TimeCode Source for currently supported TimeCode features.
aspectratio	Auto	Specifies the aspect ratio of the video source and signals it into the MPEG stream: • `Auto`: Aspect ratio is derived from the incoming video source resolution. • `3:2`, `4:3`, `5:3`, `5:4`, `16:9`, `16:10`, `17:9`: Forces aspect ratio to specified value. • `WSS/AFD`: Extracts aspect ratio from incoming video source based on WSS (Wide Screen Signaling) or AFD (Active Format Description) if detected. **Note** WSS is only supported with analog PAL video; AFD is only supported with SDSDI video.
`bitrate`	6000 kbps	The Video Raw Elementary Stream bitrate (kbps): Range: 32-25000
`resizemode`	Scale	By default, input is scaled to the output resolution. • Scale: Input is scaled to output resolution. • Crop: This setting crops the input and encodes to a rectangle within the input image (at the center of the image) while discarding the rest of the input image. The output resolution is the portion of the input that is encoded from the center. This may be done instead of downscaling. **Note** Cropping is disabled if resolution is set to Auto, 960, or 1440, or if (output) resolution is set to equal or larger than the input resolution.
`gopsize`	120	**Note** For intra-refresh mode, the GOP size is the number of frames between the sequence and picture parameter set NAL transmission.

Parameter	Default	Description/Values
`gopstructure`	IP	The GOP structure for the encoded video: (See "Framing" in Video Encoder Settings) • `I` : I frames only (lowest delay; lowest quality) • `IP` : I and P frames only • `IBP` : I, B and P frames (H.264 only) • `IBBP` : I, BB (two B frames in sequence) and P frames (highest delay; highest quality) (H.264 only) **Note** B frames require a Main Profile decoder. B frames provide more quality as the encoding is more efficient; thus more details can be rendered in the same bandwidth/ bitrate. **Tip** When B frames are used, the GOP may be rounded up to make the sequence end with a P frame.
`entropycoding`	CAVLC	Select the compression scheme: • `CAVLC` : Context-adaptive Variable-length Coding is a lower-complexity alternative to CABAC. CAVLC produces lower quality, but is easier to decode. • `CABAC` : Context-adaptive Binary Arithmetic Coding is an algorithm to losslessly compress syntax elements in the video stream. CABAC compresses data more efficiently than CAVLC and should produce better quality, but requires considerably more processing to decode. **Note** The H.264 decoder must be Main Profile compliant or higher to decode a CABAC video stream. **Tip** Generally, you get better visual quality if you are using CABAC because it is more efficient.
`partitioning`	Off	**Note** Intra-Partitioning requires that the H.264 decoder be High Profile compliant. Generally, you get better visual quality if you enable Intra-Partitioning because it gives the video encoder better coding tools. **Tip** Noisy Matrix completion is enabled automatically when Partitioning is enabled and video bitrate is under 800 Kbps. Noisy Matrix completion enhances video image "noise" reduction to improve video quality at lower bitrates and make blocky artifacts less visible.

Parameter	Default	Description/Values
`intrarefresh`	Off	Enables (on) or disables (off) Intra-refresh video encoding support. Intra-refresh is a video encoding mode of operation in which no distinct IDR frame is sent in the video elementary stream. Instead, the macro-blocks that make up the IDR frame are sent gradually within a certain time so that the entire video reference frame is re-built (at the decoder) within the number of frames specified by the refreshrate parameter. Intrarefresh minimizes latency, smooths the video bitrate, and minimizes GOP pulsing artifacts. **Tip** Intra-refresh requires that the decoder and streams be started first.

Parameter	Default	Description/Values
`refreshrate`	60	**Note** If the refresh rate is set too low, a left-to-right wave-like artifact may result.
`skipframes`	Off	This parameter permits the dropping of frames to improve video quality at lower bitrates. `Off, On` For more information, see Partial Image Skip under Video Encoder Settings.
`picrate`	Auto	The video frame rate per second: • `Auto`: Encodes at the same frame rate as the input • Range: 1-60
`closedcaption`	Off	This parameter enables Closed Captioning on the encoder stream. `Off, On` **Note** For more information, see Closed Captioning.
`ptsoffset`	50 ms.	Offset video timestamps by this value in ms. Range: -1000–1000
`resolution`	Auto	The stream output resolution. Specifies the number of lines per frame and pixels per line to be encoded. Options depend on the Input Format detected. • Auto (output resolution is the same as the input) • 1080p, 1920x1080p • 1080i, 1920x1080i • 1440x1080p • 1440x1080i • 960x1080p • 960x1080i • 720p, 1280x720 • 960x720 • 640x720 • 480p, 720x480p • 480i, 720x480i • 576p, 720x576p • 576i, 720x576i • 540x480p • 540x480 • 704x576p • 704x576i • 540x576p • 540x576i • 352x480p • 352x480i • 352x576p • 352x576i • 352x288p • 352x288i

Parameter	Default	Description/Values
`RGB`		• WUXGA, 1900x1200 • UXGA, 1600x1200 • WSXGA, 1680x1050 • HD+, 1600x900 • SXGA+, 1400x1050 • WXGA+, 1440x900 1360x768 • SXGA, 1280x1024 • WXGA, 1280x768 • XGA, 1024x768 • SVGA, 800x600 • VGA, 640x480 **Note** See Video Encoding.

Examples

```
# videnc 0 set gopsize=120
```

Sets the video GOP to 120. You will receive the following confirmation:
Encoder configured successfully.

```
# videnc 0 set bitrate=6000
```

Sets the video bitrate to 6000.

```
# videnc 0 set bitrate=6000 gopsize=120 resolution=1280x720 Input=BNC-1
```

Combines multiple video parameters in a single line.

```
# videnc 0 get
```

Returns video configuration information for the encoder:

```
Encoder ID                : 0
Name                      : "HD Video Encoder 0"
Configuration :
  Video Input             : BNC-1
  Video Format            : Auto-Detect
  Aspect Ratio            : Auto-Detect
  Time Code               : VIDEO
  Video Bitrate           : 6000 kbps
  Video GOP Size          : 120
  Encoded Picture Rate    : Input/Auto
  Output Resolution       : Input/Auto
  Closed Captioning       : Off
  Video GOP Structure     : IP
  Video Entropy Coding    : CAVLC
  Picture Partitioning    : Off
  Intra Refresh           : On
  Refresh Rate            : 60
```

```
# videnc 0 get stats
```

Returns encoder statistics:

```
Encoder ID                : 0
  Name                    : "HD Video Encoder 0"
  Statistics :
  State                    : WORKING
  Uptime                   : 21h8m28s
  Input Present            : Yes
  Input Type               : SDI
  Input Format             : 1280x720p59
  Output Resolution        : 1280x720p
  Input Aspect Ratio       : 16:9

  Encoded Frames           : 2,148,020
  Encoded Bytes            : 2,326,715,604
  Encoded Frame Rate       : 30
  Dropped Frames           : 2
  Encoded Bitrate          : 5,994 kbps
  Encoder Resets           : 2
  Encoder PTS              : 0x1708c8ce8
  Encoder Load             : 14%

Closed Captioning          : Disabled
  Timecode Source          : SYSTEM
  Timecode                 : 20:18:48:07
  Source Switches          : 5
  UTC                      : 1386188328244254 (2013-Dec-4-
                             20h18m48s244254us)
  H.264 Profile            : Main
  H.264 Level              : 4
```

Related Topics

- Configuring Video Encoders

vidin

The `vidin` command is used to view and manage video input parameters. ID is used to select the video input on dual channel encoders (either 0 for BNC-1 or 1 for BNC-2 on #S/B-292E-HDSDI2). ID is optional on single input encoders such as the #S/B-292E-HDSDI1 and the #S/B292E-DVI. If entered, only 0 will be accepted.

Synopsis

```
vidin ID get
vidin ID set
vidin ID clear
```

Actions

Action	Description
get	Displays information on the video input.
set	Configures video input parameters. See Parameters below.
clear	Clears the video input's statistics.
help	Displays usage information for the vidin command.

Parameters

Parameter	Default	Description/Values
`interface`	Auto	The type of Video Input for the encoder. For Makito DVI device: • Auto • Digital • Component For Makito SDI device: • Auto: auto-detect from the video source • SDI • Composite
`filter`	off	Use this setting to enable Input Image Filtering for the input interface. This parameter filters the video input and removes noise in order to optimize the compression of the image and to enhance the overall quality of the coded video stream.

Examples

```
# vidin 0 get
```

Returns video input information for the encoder:

```
Input ID                  : 0
Name                      : "BNC-1"
  State                   : ACTIVE
  Configured Type         : Auto-Detect
  Input Type              : SDI
  Input Format            : 1280x720p59
  Frame Rate              : 60
  Output Buffers          : 9
  Captured Frames         : 961,721
  Dropped Frames          : 776
  Last Dropped Frame      : 49m51s ago
  Lock Status Changes     : 33
  Last Status Change      : 49m50s ago
```

```
# vidin 0 set interface=SDI
```

Sets the video input to SDI.

Related Topics

- Video Encoder Settings

Administration Commands

account

The `account` command is used to create, delete, and modify user accounts for the encoder.

Note

Only an administrator can use the `account` command.

Important

Makito X Series devices ship from the factory with only the `admin` account enabled. For security reasons, the two default user accounts (`user` and `operator`) are locked at the factory as well as after a factory reset. An administrator must unlock them and change the passwords to use them for the first time.

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
```

Actions

Action	Description
create	Creates a new user account. See 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, including account name, role, state, password expiry status, and public key(s).
list	Lists the account information for the user or the Makito X 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" in Changing Your Password.
pubkey add|remove keyfile	Adds or removes a public key to the user account. See Managing Public Key Authentication for more information.

Action	Description
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.

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.

Examples

```
# account all list
```

Returns the list of all accounts, for example:

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

Related Topics

- Managing User Accounts

audit

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 an administrator.

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 an administrator.

Synopsis

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

Actions

Action	Description
start	Establishes a connection from the Makito X Series device 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 Parameters below.
get	Displays audit configuration and connection status information. You can specify configuration, statistics, or all 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.

Parameters

Parameter	Default	Description/Values
server	n/a	The server IP address. Enter an IP address in one of the following formats: • `fqdn[:port]` • `ipv4_addr[:port]` • `[ipv6_addr][:port]` **Note** When configuring an IPv6 server, the address must be enclosed in square brackets. • `hostname[:port]`
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:`

Example

```
# audit get
```

Returns audit server configuration information, such as:

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

Related Topics

- Managing Audits

banner

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

Note

The `banner` command can only be used by an administrator.
In the current release, only ASCII file format is supported for the banner file; the maximum file size for the banner is 4KB.

Important

IP display is enabled on the serial port login prompt by default and takes precedence over a banner. If both Banner and IP display are enabled, users will see the IP, not the banner on the serial port.
You can disable and re-enable IP display using the CLI commands `disable_ip_display_on_serial_port` and `enable_ip_display_on_serial_port`. If you disable IP display with this CLI command, the banner works.

Synopsis

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

Actions

Action	Description
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	**Important** The text file must be downloaded to the encoder and locally stored in the current (administrative) user's directory before it can be installed from the CLI. The Makito X 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.

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 encoder.

Examples

```
 # banner get
 The Advisory Notice and Consent Banner is disabled.
Unable to display banner: No banner file.
```

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 SDI #4 *
**************************************************
```

Related Topics

- Managing Banners

bist

The `bist` command provides information about the current status of the device and the results of any BIST (built-in self-test) or POST (power-on self-test) operations executed by the device or the administrator. The purpose is to provide confidence that the Makito X hardware and software are operating reliably and correctly. Some tests are performed immediately, while others are the most recently recorded results of POST operations

> **Note**
>
> The `bist` command can only be used by an administrator.

Synopsis

```
bist
```

Actions

N/A

Parameters

N/A

Example

```
# bist
```

bist displays the list of built-in self-tests for you to select.

```
Built-in Self-tests:
1) Show Ethernet status
2) Show video inputs status
3) Show video encoders status
4) Show CPU usage
5) Show memory usage
6) Show temperature
7) Show FIPS POST results
Q) Quit
Enter test number or q to exit:
```

certificate

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 to secure HTTPS sessions.

> **Note**
>
> The `certificate` command can only be used by an 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.

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= [type=id] [fmt=auto]
certificate name select
certificate name verify
```

Actions

Action	Description
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 encoder, 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 Parameters below.
delete	Deletes the selected certificate. The `type` can be specified. See 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 Parameters below.
select	Selects the certificate used when establishing a TLS connection with the audit server or starting an HTTPS session.

Action	Description
verify	Verifies the validity of the specified 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
`type`	id	**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	**Note** The administrator has previously downloaded/uploaded the certificate file to import in its home directory (using SCP, for example).

Related Topics

- Managing Certificates

config

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

> **Note**
>
> This is equivalent to saving and loading Presets in the Web interface. See Saving and Loading Presets.

Synopsis

```
config save [cfgname] [startup=yes,no]
config load [cfgname]
config delete [cfgname, all]
config list
```

Actions

Action	Description
save	Saves the current configuration. Saves every parameter in the system, including encoder settings and stream destination and status (excluding the system IP address). All configuration files are stored in `/usr/share/haivision/config`. See the note below in `cfgname` description.
load	Loads a previously saved configuration identified by `<cfgname>`. Reassigns every parameter in the system, including encoder 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.

Parameters

Parameter	Default	Description/Values
`cfgname`	n/a	**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 (or) • Semicolon ; • Apostrophe ’ • Double Quote ” • Left and Right Angle Brackets < or >
`startup`	no	Sets saved configuration as the startup configuration. `yes,no`

Examples

`# config save Class430 startup=yes` Saves the current configuration under the name "Class430" and sets it to be the startup configuration.
`# config load Class430` Loads a previously saved configuration identified by the name "Class430" (located in the active (local) directory).

Related Topics

- Saving and Loading Presets

date

The `date` command is used to display the current date and time.

Synopsis

```
date
```

Actions

N/A

Parameters

N/A

Example

```
# date
```

Displays the current date, e.g.:

```
Tue Jun 9 17:04:18 EDT 2020
```

Related Topics

- dtconfig
- tzconfig
- Configuring Date and Time

dest

Important

The `dest` command is only available on Makito X with Storage dual-height model.

The `dest` command is used to manage recording export destinations (i.e., add destinations, edit settings for destinations, and delete destinations).

Tip

First create the destination, then use the transfer command.

Synopsis

```
dest create host=addr name=destname [type=ftp,ftps] [path=rpath]
  [username=uname] [password=pwd] [port=ftpport] [passive=yes, no]
  [untrust=yes, no] [watchfolder=yes, no]
dest id/name/all delete
dest id/name/all get
dest id set
dest id/name test
```

Actions

Action	Description
create	Creates an export destination to be available to transfer video and metadata. A series of one or more parameter=value pairs can be specified. See Parameters below.
delete	Removes the destination.
get	Displays information about the destination. See dest below. You can specify a destination or all destinations. **Tip** To display a summary of all the destinations in a table format, you can use `dest all get table`.
set	Changes the information on the destination if it is not used by any transfer.
test	Tests the FTP connection of this destination.

Parameters

Parameter	Default	Description/Values
`name`	n/a	Specify a name for the destination, 1 to 32 characters.

Parameter	Default	Description/Values
`type`	ftp	Select the protocol type, either: • ftp: File Transfer Protocol • ftps: FTP with explicit Transport Layer Security (TLS)
`host`	n/a	The server's DNS host name or IP address for the destination.
`path`	n/a	The directory on the host.
`username`	n/a	A valid username to access the ftp server.
`password`	n/a	The password to access that ftp server with the provided username.
`port`	21	The port number for the destination server.
`passive`	yes	The FTP data connection mode for the transfer, either yes for passive mode, or no for active mode: • no: Active—The client tells the server what port it is listening on, and the data connection is established by the server with the client via the specified port. For this to work, there either needs to be no firewalls or the firewalls defined must understand the FTP protocol. • yes: Passive—The client opens two random ports. One port issues a PASV command to inform the server that it is in Passive mode. The server opens a random port and responds to the client. The client uses the second port to establish the data connection with the server via the port specified by the server.
`untrust`	no	**Note** Type yes to accept untrusted certificates if type is ftps.
`watchfolder`	no	**Note** This file contains information about recording used by platforms to process files. When files show up here, HVC starts processing.

Example

```
# dest all get
```

Displays information about the export destinations, such as:

```
Destination ID     : 1
Name               : "Dest1"
Configuration:
  Type             : FTP
  FTP Server       : 10.65.10.57
  Path             :
  FTP Port         : 21
  Passive Mode     : Off
  HVC Watch Folder : Off


Destination ID     : 2
Name               : "Active_dest"
Configuration:
  Type             : FTP
  FTP Server       : dfs.haivision.com-1
  Path             : /
  FTP Port         : 21
  Passive Mode     : Off
  HVC Watch Folder : Off


Destination ID     : 3
Name               : "s1_HVC"
Configuration:
  Type             : FTP
  FTP Server       : 240844.upload.akamai.com
  Path             : /240844/HAIVISION-RD/watch
  FTP Port         : 21
  Passive Mode     : On
  HVC Watch Folder : On

3 dests displayed.
```

Related Topics

- Configuring Export Destinations

dtconfig

The `dtconfig` command is used to set the date and time on the encoder.

> **Note**
>
> Setting the encoder to a date in the past (compared to the current date) may cause the encoder to reboot.

Synopsis

```
dtconfig YYYYMMDDhhmm[.ss]
```

Actions

N/A

Parameters

N/A

Example

```
# dtconfig 201310211100
```

Sets the encoder clock to Monday Octoder 21 11:00:00 EDT 2013

Related Topics

- date
- tzconfig
- Configuring Date and Time

edid

The `edid` command is used on the Makito X DVI to set the DVI-D preferred resolution advertised as part of the HDMI EDID (Extended Display Identification Data), so that connected devices do not scale their output resolutions to match the current Makito X DVI default (1080p). The current default may cause image distortion issues when computer graphics resolutions are encoded for some third party equipment.

Tip

This is useful because some computer video cards do not allow users to specify a resolution other than the advertised preferred one. If you have trouble getting your computer to send the proper graphic resolution to the Makito X, forcing the EDID to advertise that resolution as its preferred input format is likely to remedy that situation.

Note

EDID (Extended Display Identification Data) is a data structure provided by a digital display to communicate its capabilities to a video source device.

Synopsis

```
edid set preferred=res
edid get
edid reset
```

Actions

Action	Description
set	Selects the DVI-D preferred resolution.
get	Displays the current EDID settings.
reset	Resets the preferred resolution to the driver internal default EDID.

Parameters

Parameter	Default	Description/Values
`preferred`	1920x1200p60	Following are the available values for the DVI-D preferred resolution: • 1920x1200p60 (default) • 1920x1080p60 • 1680x1050p60 • 1600x1200p60 • 1600x900p60 • 1440x900p60, 1440x900p75 • 1400x1050p60, 1400x1050p75 • 1360x768p60 • 1280x1024p60, 1280x1024p75 • 1280x800p60, 1280x800p75, 1280x800p85 • 1280x768p60, 1280x768p75, 1280x768p85 • 1152x864p75 • 1024x768p60, 1024x768p75, 1024x768p85 • 800x600p60, 800x600p75, 800x600p85 • 640x480p60, 640x480p75, 640x480p85

Examples

```
# edid get
```

Returns EDID configuration information for the encoder, such as:

```
Configuration:
  EDID File               : (Using driver internal data)
  Preferred Resolution    : 1920x1200p60
```

```
# edid set preferred=1280x1024p60
```

Sets the DVI-D preferred resolution to 1280x1024p60

Related Topics

- Video Encoder Settings

ethercfg

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

When the Makito X 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 disable autonegotiation.

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

```
ethercfg
  Speed               : 1000mbps
  Duplex              : Full
  Auto-Negotiation    : On
  Advertised Mode     : All
  Link Detected       : Yes
  Ceiling             : 100000kbps
```

Synopsis

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

Options

Option		Description/Values
`-a`	`--autoneg`	Enables (on) or disables (off) autonegotiation.
`-s`	`--speed`	If autonegotiation is disabled, sets the speed: 10, 100, 1000. If autonegotiation is enabled, this is the advertised supported speed which will be available for the peer Ethernet switch to use.
`-d`	`--duplex`	If autonegotiation is disabled, sets the duplex mode: half, full. 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`	If yes, 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).

Parameter

N/A

Actions

N/A

Example

```
# ethercfg -s 100
```

Sets the line speed to 100 Mbps (which also modifies the advertised mode, see example below).

```
# ethercfg -s 100
  Speed             : 100mbps
  Duplex            : Full
  Auto-Negotiation  : 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

haiversion

The `haiversion` command is used to display status information about the Makito X. Status information can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

Synopsis

```
haiversion
```

Actions

N/A

Parameters

N/A

Example

```
# haiversion
```

Displays information about the hardware and software components.

```
Card Type                  : "Makito2 DVI Encoder"
Part Number                : B-292E-DVI
Serial Number              : HAI-031339010049
MAC Address                : 5c:77:57:00:48:71
Firmware Version           : 1.1.0-42
Firmware Date              : "Dec 2 2013"
Firmware Options           : "KLV"
Hardware Version           : --
Hardware Compatibility     : -001G
CPLD Version               : 2 (Official, Internal flash)
Boot Version               : "U-Boot 2010.06 (Mar 14 2013 - 13:04:35)-
                           MakitoX 0.9.10
```

Related Topics

- Viewing System Status Information

hdcp

The `hdcp` command is used to manage HDCP (High-bandwidth Digital Content Protection) settings on Makito X DVI systems.

Synopsis

```
hdcp enable
hdcp disable
hdcp get
```

Actions

Actions	Description
enable	Enables HDCP support on the DVI input interface.
disable	Disables HDCP support on the DVI input interface.
get	Displays the current status of HDCP support.

Parameters

N/A

Examples

```
# hdcp get
```

Returns hdcp status for the encoder:

```
Configuration:
  HDCP Enabled   : On
```

Related Topics

- Video Encoder Settings

ipconfig

The `ipconfig` command is used to view and set the parameters that specify the IP (IPv4) networking context for the Makito X, including the IP settings, hostname, and DNS. It may also be used to set the Network Time Protocol (NTP) server address and Time Zone.

As shown in the examples that follow, 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.

Note

Enabling the Multicast DNS (mDNS) protocol allows the Safari Web browser (or other mDNS application) to automatically find the encoder. In Safari, navigate to Bookmarks and then select Bonjour to see the Makito X listed.

Warning

If you are connecting to the Makito X through an IPv4 connection, disabling the IPv4 interface will drop your connection. You will need to reconnect using IPv6 or the serial interface (if available).

You must reboot for any changes to take effect.

Synopsis

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

Actions

Action	Description
display	Displays the current IP configuration.
configure	Configures IP settings.
renew	Renews DHCP address lease.
release	Releases current DHCP address lease.
disable	**Note** You cannot disable IPv4 if IPv6 is already disabled.

Parameters

N/A

Examples

```
# ipconfig display
```

Returns current IP settings for encoder configured to use DHCP:

```
Current IP Settings (Obtained via DHCP):
  IP Address                : 10.65.11.188
  Network Mask              : 255.255.254.0
  Gateway                   : 10.65.10.1
  Link-Local Address        : (Disabled)
  Hostname                  : STORAGE-2
  DHCP Vendor Class ID      : "Haivision Makito X Encoder"
Current DNS Settings (Obtained via DHCP):
  Domain                    : haivision.com
  Primary Server            : 10.65.0.10
  Alternate Server          : 10.65.0.11
Current Multicast DNS (mDNS) Settings:
  Responder                 : Enabled
  Identifier                : "MakitoX STORAGE-2"
Current NTP Settings:
  Server                    : pool.ntp.org
  Timezone                  : "America/Montreal"
```

```
# ipconfig display
```

Returns current IP settings for encoder that does *not* use DHCP:

```
Current IP Settings:
  IP Address                : 10.65.129.67
  Network Mask              : 255.255.255.0
  Gateway                   : 10.65.129.1
  Hostname                  : MXE-129-69
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                     : 0.ca.pool.ntp.org
 Timezone                   : "America/Montreal"
```

```
# ipconfig configure
```

Prompts you as follows to modify current settings (using DHCP):

```
Current IP Settings (Obtained via DHCP):
  IP Address                : 10.65.11.188
  Network Mask              : 255.255.254.0
  Gateway                   : 10.65.10.1
  Link-Local Address        : (Disabled)
  DHCP Vendor Class ID      : "Haivision Makito X Encoder"

Change IP settings? (y,N): y
Use DHCP to obtain IP address automatically? (Y,n): y
Auto-assign link-local address when DHCP is unavailable? (y,N)
Enter DHCP Vendor Class Identifier ("Haivision Makito X Encoder"):

Current Hostname            : STORAGE-2
Change hostname? (y,N):

Current DNS Settings (Obtained via DHCP):
  Domain                    : haivision.com
  Primary Server            : 10.65.0.10
  Alternate Server          : 10.65.0.11
Change DNS settings? (y,N):

Current Multicast DNS (mDNS) Settings:
  Responder                 : Enabled
  Identifier                : "MakitoX STORAGE-2"
Change Multicast DNS Settings? (y,N):

Current NTP Settings:
  Server                    : pool.ntp.org
  Timezone                  : "America/Montreal"
Change NTP Settings:
  Server                    : pool.ntp.org
  Timezone                  : "America/Montreal"
Change NTP server? (y,N): n
Change Timezone? (y,N): n

Network settings updated successfully.
You must REBOOT for any changes to take effect!
```

```
# ipconfig configure
```

Prompts you as follows to modify current settings (does *not* use DHCP):

```
Current IP Settings:
  IP Address                : 10.5.1.2
  Network Mask              : 255.255.0.0
  Gateway                   : 10.5.0.1
  Hostname                  : Makito2

Change IP settings: (Y,N): y
Use DHCP to obtain IP address automatically: (Y,N): n
Enter ip address            : 192.0.2.42
Enter netmask               : 255.255.255.0
Enter default gateway       : 192.0.2.24

Current hostname            : Makito2
Change hostname? (Y,N): y

Current DNS settings:
  Domain                    : haivision.com
  Primary Server            : 10.65.0.10
  Alternate Server          : (None)
Change DNS settings? (Y,N): n

Current Multicast DNS (mDNS) Settings:
  Responder                 : Enabled
  Identifier                : "MakitoX (MXE-DVI John)"
Change Multicast DNS Settings? (y,N): n

Current NTP settings:
  server                    : 10.5.0.1
  timezone                  : "America/Chicago"
Change NTP settings? (Y,N): n

Current Time Zone settings:
  America/Chicago
Change system Time Zone? (Y,N): n

Network settings updated successfully.
You must REBOOT for any changes to take effect!
```

Related Topics

- Configuring Network Settings
- Network Settings

ipv6config

The `ipv6config` command is used to view and set the parameters that specify the IPv6 network configuration of Makito X Series devices.

As shown in the examples that follow, when you enter the `ipv6config configure` command, the system displays the current IPv6 settings and takes you through a series of prompts enabling you to change these settings. You can either assign a static IPv6 address or use DHCPv6 (Dynamic Host Configuration Protocol for IPv6).

You must reboot for any changes to take effect.

Synopsis

```
ipv6config display
ipv6config configure
ipv6config disable
```

Actions

Action	Description
display	Displays the current IPv6 configuration.
configure	Configures IPv6 settings.
disable	Disables IPv6 functionality. **Note** You cannot disable IPv6 if IPv4 is already disabled.

Parameters

N/A

Examples

```
# ipv6config display
```

Returns current IPv6 settings for an encoder configured to use IPv6:

```
Current IPv6 Settings:
Current configured IPv6 Settings:
 IPv6 Global Address : fd00:10:65:10::9fdf/128
 IPv6 Global Address : fd00:10:65:10:5e77:57ff:fe00:6be7/64
 IPv6 Link-Local Address : fe80::5e77:57ff:fe00:6be7/64
 Gateway Address : fe80::2efa:a2ff:fed2:7e25
 Hostname : MXE-hevc-steph

Current DNS Settings:
 Domain : haivision.com.
 Primary Server : fd00:10:65::12
 Alternate Server : (None)

Or indicates that IPv6 is disabled:

IPv6 is disabled on this device.
```

```
# ipv6config disable
```

Prompts you to confirm and then disables IPv6.

```
Do you want to disable IPv6 functionality? (Y,n): y
IPv6 has been successfully disabled.
You must REBOOT for any changes to take effect!

admin@x-enc-storage-fixed:~$ reboot
```

```
# ipv6config configure
```

Prompts you to configure IPv6 settings (on system where IPv6 has been disabled, re-configuring IPv6 to the last configured settings):

```
IPv6 is currently disabled on this device.
Do you want to enable IPv6 functionality? (Y,n): y
Last Configured IPv6 Settings:
 IPv6 Global Address : fc00::2/24
 Gateway : fc00::1
Change IPv6 settings? (y,N): n
IPv6 has been successfully configured.
You must REBOOT for any changes to take effect!
```

```
# ipv6config configure
```

Prompts you to modify current IPv6 settings (without using auto-config):

```
Current IPv6 Settings:
 IPv6 Global Address : fd00:10:65:10:5e77:57ff:fe00:3296/64
 IPv6 Link Local Address : fe80::5e77:57ff:fe00:3296/64
 Gateway Address : fe80::2efa:a2ff:fed2:7e25
Change IPv6 settings? (y,N): y
Configure IPv6 automatically (Y,n): n
Enter IP address:
Enter network prefix length:
Enter default gateway:
IPv6 has been successfully configured.
You must REBOOT for any changes to take effect!
```

Related Topics

- Configuring Network Settings
- Network Settings

license

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. For more information, see Managing Licenses.

Note

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

Synopsis

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

Actions

Action	Description
list	Displays a list of installed licenses. Licenses are stored on the Makito X file system in the folder `/usr/share/haivision/licenses`.
view	Displays the content of the specified license file.
install	**Important** The license file must be uploaded to the encoder and locally stored in the current (administrative) user's folder before it can be installed. The Makito X 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.

Parameters

N/A

Examples

```
# license list
```

Displays a list of licenses currently installed on the system:

```
License Files (in /usr/share/haivision/licenses):
  metadata-PO123456.lic
```

```
# license view metadata-PO123456.lic
```

Displays the contents of the specified license:

```
#----------BEGIN LICENSED FEATURE---------- metadata.lcf ----------
[INFO]
Feature=Metadata
Description=Metadata KLV CoT

[KLV]
Enabled=On

[CoT]
Enabled=On

#----------END LICENSED FEATURE---------- metadata.lcf ----------

#----------BEGIN LICENSING DATA----------------------------------
[LIC-SIGNATURE]
CreatedOn=2013-06-13 09:27:06
CreatedBy=support@haivision.com
Sequence=fw100001_metadata.lic

[LIC-DEVICES]
HAI-031233010018=Yes
HAI-090022300016=Yes
HAI-100022230061=Yes
HAI-100009820054=Yes

#----------END LICENSING DATA------------------------------------
```

```
# license verify metadata-PO123456.lic
```

Verifies the specified license:

```
Verifying license /usr/share/haivision/licenses/metadata-PO123456.lic...
License verification successful.
```

Note

This command first checks to see if the specified license is in the current working directory.

If Yes, it will verify that one.
If No, it will look for it in the installed licenses directory (`/usr/share/...`)
This allows the verification of licenses before they are installed.

Related Topics

- Managing Licenses

messages

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.

Note

The `messages` command can only be used by an administrator.
Messages starting with "POST" are Power-On Self Test events. If you repeatedly get POST errors, the cryptographic module of the encoder may be compromised, and it is recommended to re-installed the firmware.

Synopsis

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

Actions

Action	Description
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.

Parameters

N/A

Example

```
# messages get

Wed Dec 6 13:48:17 EST 2017: There were 2 failed login attempts on the admin
  account since the last successful login.
Fri Jan 12 22:41:11 EST 2018: There were 2 failed login attempts on the admin
  account since the last successful login.
Thu Jan 18 21:07:12 EST 2018: There was 1 failed login attempt on the admin
  account since the last successful login.
Thu Feb 8 09:41:27 EST 2018: There were 5 failed login attempts on the admin
  account since the last successful login..
```

Related Topics

- Managing Messages

nas

The `nas` command is used to manage Network Assisted Storage settings. This is useful to set an NFS mount point on the Makito X for storing snapshots or (with the Makito X with Storage) for copying recordings after they are completed.

Synopsis

```
nas enable location=remotehost:remotedir
nas get
nas disable
```

Actions

Action	Description
enable	Configures and enables NAS. A series of one or more `parameter=value` pairs can be specified as once. See Parameters below.
get	Displays NAS configuration and status information.
disable	Disables NAS.

Parameters

Parameter	Default	Description/Values
`location`	n/a	Specifies remote host IP address and path, using the format: `remotehost:remotedir`

Example

```
# nas enable location=indigo:/home/flemieux/shared
```

Activates Network Assisted Storage and specifies the remote host IP address and path.

```
# nas get
```

Returns NAS configuration information for the encoder, such as:

```
Configuration:
  Status            : Enabled
  Remote Host       : "tserver.haivision.com"
  Remote Dir        : "/NFS"
```

```
# nas get all
```

Returns NAS configuration information and statistics for the encoder, such as:

```
Configuration:
  Status           : Enabled
  Remote Host      : "tserver.haivision.com"
  Remote Dir       : "/NFS"
Statistics:
  Capacity         : 49.08GB
  Used             : 79.96MB (0%)
  Available        : 40.94GB (83%)
```

Related Topics

- Managing Network Storage

nmcfg

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. 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 user groups (administrator, operator, and guest).

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 SNMP Agent Components.

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>
```

Options

Name	Description
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
system	Defines contact and location system parameters.
user	Defines user-based (v3) security configuration for the Makito X.

Name	Description

Actions

Action	Description
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	**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 settings which are lost when the unit is rebooted unless saved as a configuration.

Parameters

N/A

Example #1: Initializing 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/group      community             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: Creating 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 permit johnsmith operator
```

Example #3: Initializing 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/group         community             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 administrator priv
# nmcfg access usm permit johnsmith operator priv
# nmcfg access usm permit guest guest
# nmcfg agent start
# nmcfg

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

model            perm/group    level    user/community         source
---------------- ------------- -------- ---------------------- ---------
usm              guest         auth     guest                  -
usm              administrator priv     joenet                 -
usm              operator      priv     johnsmit               -

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

Related Topics

- SNMP Agent Components

package

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

> **Note**
>
> The package command can only be used by an 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 administrators (see **messages** CLI command). A successful package installation notice is added to the messages upon successful installation.

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
```

Actions

Action	Description
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.
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.

Parameters

N/A

Example #1: Package Download and Installation

```
# package download makitox_enc_v2.2.0-59.hai mytftp.example.com
1/5) Temporarily pausing encoder(s)...
2/5) Downloading package makitox_enc_v2.2.0-59.hai from mytftp.example.com...
3/5) Verifying integrity of downloaded package...Package verified successfully.
4/5) Synching file system...
5/5) Resuming encoder(s)...
Package downloaded successfully.

# package install makitox_enc_v2.2.0-59.hai
Package makitox_enc_v2.2.0-59.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_enc_v2.2.0-59.hai mytftp.example.com
1/5) Temporarily pausing encoder(s)...
2/5) Downloading package makitox_enc_v2.2.0-59.hai from mytftp.example.com...
3/5) Verifying integrity of downloaded package...Package verification failed!
Try downloading the package again.
```

Examples (General)

```
# package list
```

Displays the list of downloaded packages:

```
Package Files (in /usr/share/haivision/packages/):
  makitox_enc_v2.2.0-59.hai
  makitox_enc_v2.2.0-58.hai
```

```
# package info makitox_enc_v2_2_0.hai
```

Displays information about the package.

```
# package install makitox_enc_v2_2_0.hai
```

Installs the package.

passwd

The `passwd` command is used to change your own password.

> **Note**
>
> To modify the password for other users' accounts, see the **account** CLI command.

Synopsis

```
passwd
```

Actions

N/A

Parameters

N/A

Examples

```
# passwd
```

> **Note**
>
> Passwords can be up to 80 characters long. See "Password Requirements" in **Changing Your Password** for the supported character set. Password policies set by the administrator may enforce the selection of strong passwords.

Related Topics

- **Role-based Authorization**
- **Managing User Accounts**

personality

The `personality` command is used to manage the Makito XR (Ruggedized) encoder "personality" by providing a means to set the XR personality to either the two-port variant (#S-292E-X2R) or the four-port variant (#S-292E-X4R).

For details on the Makito XR encoder, please refer to the *Makito XR (Ruggedized) Installation Guide* (available from the **Download Center** on the Haivision Support Portal). The change of personality takes effect after the next reboot of the unit.

> **Note**
>
> This command may only be used on a Makito XR encoder by an administrator. XR personalities do not change due to a factory reset.

Synopsis

```
personality set <TYPE>
personality get
```

Actions

Action	Description
set	Sets the Makito XR (Ruggedized) encoder personality.
get	Displays the current Makito XR encoder personality.

Parameters

Parameter	Default	Description/Values
`TYPE`	n/a	Sets the personality that will take effect on the next bott, either X2R or X4R.

Examples

```
# personality get

Current Personality : X4R
```

```
# personality set X4R
```

Sets the personality to X4R.

policy

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.

Note

The policy command can only be used by an administrator.

Synopsis

```
policy password set [quality=basic] [minlen=6] [minuppers=0] [mindigits=0]
  [minsymbols=0] [expiry=yes] [lifetime=90] [remember=5]
policy session set [autologout=yes] [idletimeout=15]
policy crypto set [compliance=None] [tlsv1.{0|1|2}=yes] [sslv3=no]
policy crypto set [compliance=None]
policy pname/all get
```

Actions

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

Parameters

Parameter	Default	Description/Values
crypto		

Parameter	Default	Description/Values
`compliance`	None	Specifies the required cryptographic compliance, either: • None • NDPP11: Activates cryptographic security to a level compliant with the Network Device Protection Profile v1.1. • FIPS140: All management cryptography is operated in the FIPS 140-2 mode. • Sp800-52r1: All management cryptography follows the guidelines of NIST Special Publication 800-52 Rev 1. **Note** Either selection reinforces security for all management functions of the encoder in terms of cryptography. This setting takes effect upon the next reboot.
`sslv3`	See Note	**Note** SSLv3 is disabled on factory new systems. On upgraded systems, SSLv3 is enabled only if upgrading a system where no (None) cryptographic compliance is configured. SSLv3 can be enabled only if compliance is set to None.
Specifies which TLS (Transport Layer Security) versions are accepted from the HTTPS client. At least one TLS version must be enabled.		
`tlsv1.0`	Yes	Enables or disables TLSv1.0 as a supported TLS version: Yes, No
`tlsv1.1`	Yes	Enables or disables TLSv1.1 as a supported TLS version: Yes, No
`tlsv1.2`	Yes	Enables or disables TLSv1.2 as a supported TLS version: Yes, No
password		
`quality`	Basic	Specifies the required password strength, either: • Basic • Strong
minlen	6	Specifies the minimum password length. Range: 6–40
`minuppers`	See Note	(quality must be Strong) Specifies the minimum number of uppercase letters. Range: 0 –40 **Note** Default is N/A if quality=Basic, 0 if quality=Strong.
`mindigits`	See Note	(quality must be Strong) Specifies the minimum number of digits. Range: 0 –40 **Note** Default is N/A if quality=Basic, 0 if quality=Strong.

Parameter	Default	Description/Values
`minsymbols`	See Note	(quality must be Strong) Specifies the minimum number of symbols. Range: 0 –40 **Note** Default is N/A if quality=Basic, 0 if quality=Strong.
`expiry`	No	Enables or disables password expiration: • Yes, No
`lifetime`	90 days	(expiry must be Yes) Specifies the number of days after which users must change their passwords. Range: 1 –180 days
`remember`		(quality must be Strong) Saves the specified last number of passwords used for the encoder, and prevents users from changing their password to any password used within the specified history count. Range: 5 –400
session		
`autologout`	No	Enables (Yes) or disables (No) auto-logout.
`idletimeout`	15 minutes	(autologout must be Yes) Specifies the maximum length of time the system may be idle before the user will be logged out. Range: 1 –1440 minutes

Examples

```
# policy crypto set compliance=NDPP11
```

Sets the required cryptographic compliance to Network Device Protection Profile v1.1.

```
# policy password set quality=strong minlen=10 minuppers=1 minsymbols=1
   expiry=yes lifetime=30
```

Sets the password policy for the encoder 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.

```
# policy all get
```

Returns policy information for the encoder such as:

```
Crypto:
  Compliance          : (None)
  SSLv3               : Yes
  TLSv1.0             : Yes
  TLSv1.1             : Yes
  TLSv1.2             : Yes
Password:
  Quality             : Basic
  MinLen              : 6
  Expiry              : No
Session:
  Autologout          : No
```

Related Topics

- Managing Security Policies

pubkey

Note

The pubkey command can only be used by an administrator.

Synopsis

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

Actions

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

Examples

```
# pubkey add makito.pub
```

Uploads the public key file makito.pub to the encoder.

```
# pubkey list
```

Lists all public key files currently loaded on the encoder 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

reboot

Note

The reboot command can only be used by an administrator.

Synopsis

```
reboot
```

Example

```
# reboot
```

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 sign in again.

Related Topics

- Rebooting the Encoder under Status Settings

service

Important

If the COM1 port is not configured for CLI Management, and all remote management interfaces (HTTP, telnet, SSH, and SNMP) are disabled, the only way to re-enable these services is by a Factory Reset. (For details, see Resetting the Encoder.) Once the serial port is configured for metadata or passthrough use, it is no longer usable for CLI management.

Synopsis

```
service name action
```

where:
`name` can be: `all, http, passthrough, snmp, ssh, talkback, telnet, vf`

Actions

Action	Description
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. Also displays the startup status of the service.

Examples

```
# service telnet stop
```

Stops telnet connection to the Makito X.

```
# service all stop
```

Stops all network connections to the Makito X.

Related Topics

- Enabling and Disabling Network Services

storage

The storage command is used to manage storage devices on the Makito X with Storage dual-height model. This includes formatting and ejecting storage drives. To display available storage devices use storage list.

Synopsis

```
storage list
storage [device] [command] [options] [parameters]
```

Actions

Action	Description
list	Displays available storage devices for the encoder.
[device] [command]	Device specifies the type, either: ssd, usb, sd Command, either: format, mount, eject, restart

Options

Option		Description
-f	--force	Never prompt for confirmation.
-v	--verbose	Display output from low level commands.

Parameters

Parameter	Default	Description/Values
`fs`	ntfs	(format command only) File system type, either: ext4, ntfs, fat32, exfat **Note** The SSD drive can only be formatted as ext4.
`label`	n/a	(format command only) String specifying the volume name.

Examples

```
# storage usb eject
```

Ejects the installed USB storage device.

```
# storage usb format
```

Formats the USB drive as NTFS by default.

```
# storage list
```

Displays a list of available storage devices, for example:

```
Device     Size     Used     Available     Use%     Type     Volume
ssd        229.2G   14.0G    203.5G        6%       ext4
usb        --       --       --            --
sd         59.9G    104.1M   59.8G         0%       exfat
```

Related Topics

- Managing External Storage
- Managing Storage Drives

system_snapshot.sh

The `system_snapshot.sh` command is used take a system snapshot for the purpose of troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

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

Synopsis

```
system_snapshot.sh > filename
```

where:
`filename` is the name of the file to store the system snapshot.

Related Topics

- Taking a System Snapshot

transfer

The `transfer` command is used to manage exporting of files to an external storage location.

Synopsis

```
transfer create [source=ssd] [dest=text] [file=txt][remove=yes,no]
transfer id/name/all start
transfer id/name/all delete
transfer id/name/all stop
transfer id/name/all get [config/stats/all]
```

Actions

Action	Description
create	Creates a file transfer from the encoder. A series of one or more `parameter=value` pairs can be specified at once.
start	Starts the transfer.
delete	Removes the transfer.
stop	Stops the transfer.
get	Displays information about the transfer. See Parameters below. You can specify the `config`, `status`, or `all`.

Parameters

Parameter	Default	Description/Values
`source`	ssd	The source device: `ssd` only in the current release.
`dest`	n/a	The destination ID or name from the preconfigured destination list, or `usb`, `sd`, or `nfs`
`file`	n/a	The name of the file to transfer.
`remove`	no	If yes, removes the source file if the transfer is successful.

Example

```
# transfer create dest=usb file=NewOne-2015-06-23-18
```

Transfer to copy small recording to USB (completed right away). Returns information such as:

```
Transfer created successfully - ID: 1.
# transfer 1 get all
Transfer ID          : 1
Name                 : (None)
Configuration :
  Source             : SSD
  Destination Device : USB
  File               : NewOne-2015-06-23-18h18m00s.mp4
  Remove Source File : No
Status :
  Status             : SUCCESS
  Transfer Type      : COPY
  Transferred        : 100%
  Start Time         : 2015-6-23 18:29:37
  End Time           : 2015-6-23 18:29:39
```

```
# transfer create dest=1 file=Stream#1-2015-06-22-18h02m56s.mp4
```

Transfer using a preconfigured FTP destination (ID=1) to export a larger file. Returns information such as:

```
Transfer created successfully - ID: 2.
# transfer 2 get all
Transfer ID          : 2
Name                 : (None)
Configuration:
  Source             : SSD
  Destination ID     : 1
  File               : Stream#1-2015-06-22-18h02m56s.mp4
  Remove Source File : No
Status:
  Status             : IN PROGRESS
  Transfer Type      : FTP
  Transferring File  : /mnt/storage1/recordings/
                         Stream#1-2015-06-22-18h02m56s.mp4
  Start Time         : 2015-6-23 18:31:7
```

Related Topics

- Managing File Transfer History

tzconfig

The `tzconfig` command is used to configure the timezone on the encoder. tzconfig displays the current timezone and prompts you to change the timezone (Y,N). To change the timezone, type Y and follow the prompts for information about the current location. When you have completed your selections, the encoder saves the newly configured time zone information.

Synopsis

```
tzconfig
```

Example

```
# tzconfig

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.

1) Africa
2) Americas
3) Antarctica
...
$? 2

Please select a country.

1) Antigua & Barbuda 2) Anguilla 3) Netherlands Antilles 4) Argentina 5)
 Aruba 6) Barbados
7) Bolivia 8) Brazil 9) Bahamas
10) Belize 11) Canada 12) Chile
...
$? 11

Please select one of the following timezone regions.

1) St_Johns 2) Halifax 3) Glace_Bay
4) Goose_Bay 5) Montreal 6) Toronto
...
$? 5
```

Related Topics

- date
- dtconfig

Technical Specifications

This appendix lists the technical specifications for the Makito X encoder.

Topics in This Chapter

- Audio/Video Interface Specifications
- Video Encoding
- Audio Encoding
- Advanced Features
- Metadata (Optional)
- KLV Data Specifications
- Network and Management Interfaces
- Chassis Options
- Supported Storage Devices
- Regulatory/Compliance
- Closed Captioning

Audio/Video Interface Specifications

Video Inputs | Audio Inputs

Makito X DVI (#S/B-292E-DVI)		
Y,Pb,Pr / RGBHV		Component Analog video. Also supporting: • RGB with external SYNC (HSYNC & VSYNC) • RGB with SYNC on Green (RsGB)
Y,Cb,Cr / DVI		Component Digital video
Makito X SDI (#S/B-292E-HDSDI2 or #S/B-292E-HDSDI1) **Makito X HEVC (#S/B-292E-SDI2-HEVC or #S/B-292E-SDI1-HEVC)** **Makito X Harsh Environment SDI (#S-292E-X2H or #S-292E-X1H)** **Makito XR (Ruggedized) SDI (#S-292E-X2R or #S-292E-X4R)**		
Composite	NTSC/PAL/PAL-M	RS-170 RS-170A CCIR
SD-SDI	SMPTE-259M-C	270 Mbps interface
HD-SDI	SMPTE-292M	1,485 Gbps interface
	SMPTE-274M	1920 x 1080 video format
	SMPTE-296M	1280 x 720 video format
3G-SDI[1]	SMPTE-424M (Level A only)	3 Gbps interface
	SMPTE-425M	1080p60 video format
Impedance		
DVI-I		100 Ohms
DVI-A		75 Ohms
SDI		75 Ohms

1. 3G-SDI is not supported on the Makito X4R (#S-292E-X4R).

Video Inputs | Audio Inputs

Makito X DVI (#S/B-292E-DVI)
• Two analog audio channels per blade. • The DVI interface supports two channels of embedded audio (channels 1 & 2).
Makito X SDI (#S/B-292E-HDSDI2 or #S/B-292E-HDSDI1) **Makito X HEVC (#S/B-292E-SDI2-HEVC or #S/B-292E-SDI1-HEVC)** **Makito X Harsh Environment SDI (#S-292E-X2H or #S-292E-X1H)[1]**

• Two analog audio channels per blade. • Up to 16 channels of embedded audio per blade, in channel pair groups. The channel pair sources are: sdi1ch1&2, sdi1ch3&4, sdi1ch5&6 ... sdi1ch15&16 sdi2ch1&2, sdi2ch3&4, sdi2ch5&6 ... sdi2ch15&16 **Note** SDI2 audio inputs are only available on dual-BNC systems (#S/B-292E-HDSDI2).
Available through mini-DIN-8 locking connector: • Balanced stereo analog audio • Unbalanced stereo analog audio (Line Level) • Audio Talkback
Digital Embedded Audio • SD-SDI: SMPTE-272M • HD/3G-SDI: SMPTE 299M
Stereo Analog Audio Inputs • Level: Adjustable from 6 to 20dBu • Impedance: 24 KOhms Single Ended (Unbalanced) / 48 KOhms Differential (Balanced)
Analog Audio Output (Talkback) • Level: 2.2 dBu (1Vrms) • Impedance: 100 Ohms

1. Support for analog and embedded audio capture or encoding is not currently provided for the Makito X Ruggedized (#S-292E-X2R or #S-292E-X4R)

Video Encoding

Video Encoding – H.264 AVC/H.265 HEVC (MPEG-4 Part 10)	
DVI Input Resolutions / Scan Rates	1920x1200 60 Hz 1680x1050 60 Hz 1600x1200 60 Hz 1600x900 60 Hz 1440x900 75, 60 Hz 1400x1050 75, 60 Hz 1360x768 60 Hz 1280x1024 75, 60 Hz 1280x800 85, 75, 60 Hz 1280x768 85, 75, 60 Hz 1152x864 75 Hz 1024x768 85, 75, 60 Hz 800x600p 85, 75, 60 Hz 720x576p 50 Hz 720x480p 60/59.94 Hz 640x480p 85, 75, 60 Hz **Note** The DVI interface also supports all the SD/HD/3G-SDI Input Resolutions.

Video Encoding – H.264 AVC/H.265 HEVC (MPEG-4 Part 10)	
SD/HD/3G-SDI Input Resolutions	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 720x480i 60/59.94 Hz 720x576i 50 Hz **Note** For supported video encoding resolutions, see Supported H.264 Video Encoding Input and Downscale Resolutions.
Video Bitrates (H.264)	SD/HD from 32 kbps to 25 Mbps
Video Bitrates (HEVC)	SD/HD from 32 kbps to 15 Mbps
Rate Control	Variable (VBR) Constant bit rate (CBR) **Note** Enabling Partial Image Skip constrains the bitrate generated by the encoder. See “Partial Image Skip” in Video Encoder Settings.
Encoding Latency	Less than 60ms (H.264 encoder at 720p60, 6Mbps) Less than 50ms (HEVC encoder at 720p60, 6 Mbps) **Note** Encoding latency refers to the time delay between capture of a frame and the instant when the frame is encoded and ready for transmission.
Compression Standards (H.264)	• H.264/AVC (MPEG-4 part 10) • ISO/IEC 14496-10 • Baseline, Main, and High Profiles • Up to Level 4.2 and lower Intermediate Levels • I, IP, IBP, and IBBP framing • Configurable Group of Picture (GOP) size • Configurable frame rate • Region of interest coding
Compression Standards (HEVC, with supported hardware)	• H.265/HEVC • ISO/IEC 23008-2 • Up to Level 4.2 and lower Intermediate Levels • IP framing • Configurable Group of Picture (GOP) size • Configurable frame rate • Deblocking filter • Main Profile • Up to Level 4.1 (1080p60 @ 15 Mbps)
Macro-block processing limitation	(H.264 only) The aggregate pixel processing power for all video encoding engines cannot exceed 3 x 1080p60 or 1,468,800 macro-blocks per second.
Video Encoding Limits	• Up to 3x1080p60 H.264 • Up to 1x1080p60 HEVC

Supported H.264 Video Encoding Input and Downscale Resolutions

Encoded Output Resolutions		Input Resolutions and Frame Rates																	
		1080p						1080i		720p						480i	480p*	576i	576p*
Name	Resolution	60/59.94	30/29.97	50	25	24	23.98	30/29.97	25	60/59.94	30/29.97	50	25	24	23.98	30/29.97	60/59.94	25	50
HD 1080p	1920x1080p	2	4	2	4	4	4	4	4	-	-	-	-	-	-	-	-	-	-
HD 1080i	1920x1080i	-	-	-	-	-	-	4	4	-	-	-	-	-	-	-	-	-	-
3/4 HD 1080p	1440x1080p	2	3	2	3	3	3	4	4	-	-	-	-	-	-	-	-	-	-
3/4 HD 1080i	1440x1080i	-	-	-	-	-	-	4	4	-	-	-	-	-	-	-	-	-	-
1/2 HD 1080p	960x1080p	2	4	2	4	4	4	4	4	-	-	-	-	-	-	-	-	-	-
1/2 HD 1080i	960x1080i	-	-	-	-	-	-	4	4	-	-	-	-	-	-	-	-	-	-
HD 720	1280x720p	2	4	2	4	4	4	4	4	4	4	4	4	4	4	-	-	-	-
3/4 HD 720	960x720p	-	-	-	-	-	-	-	-	4	4	4	4	4	4	-	-	-	-
1/2 HD 720	640x720p	-	-	-	-	-	-	-	-	4	4	4	4	4	4	-	-	-	-
SD 480p	720x480p	2	4	-	-	4	4	4	-	4	4	-	-	4	4	4	4	-	-
SD 480i	720x480i	-	-	-	-	-	-	4	-	-	-	-	-	-	-	4	-	-	-
SD 576p	720x576p	-	-	2	4	4	-	-	4	-	-	4	4	4	-	-	-	4	4
SD 576i	720x576i	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-	4	-
4CIFp	704x576p	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	4
4CIFi	704x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-
3/4 D1 NTSCp	540x480p	-	-	-	-	-	-	-	-	4	4	-	-	4	4	4	4	-	-

Encoded Output Resolutions		Input Resolutions and Frame Rates																	
		1080p						1080i		720p						480i	480p *	576i	576p *
Name	Resolution	60/59.94	30/29.97	50	25	24	23.98	30/29.97	25	60/59.94	30/29.97	50	25	24	23.98	30/29.97	60/59.94	25	50
3/4 D1 NTSCi	540x480i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	-	-
3/4 D1 PAL	540x576p	-	-	2	4	4	-	-	-	-	-	4	4	4	-	-	-	4	4
3/4 D1 PAL	540x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-
70% VGA	448x336p	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Half-D1 NTSC	352x480i/p	2	4	-	-	4	4	4	-	4	4	-	-	4	4	4	4	-	-
Half-D1 PAL	352x576i/p	-	-	2	4	4	-	-	4	-	-	4	4	4	4	-	-	4	4
CIF	352x288i/p	2	4	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Legend:

"2", "3" or "4" - Indicates the number of encoding cores that can be supported.

Resolutions marked "-" are not supported.

* DVI-I only.

Supported H.264 Graphic Encoding Input and Downscale Resolutions

Applies to Makito X #S/B-292E-DVI only

Output Resolutions		YPbPr, RGBHV, DVI-A, and DVI-I Computer Graphic Input Resolutions																
		1920 x 1200	1680 x 1050	1600 x 1200	1600x 900	1440x 900	1400 x 1050	1360 x 768	1280 x 1024	1280x 800		1280x 768		1152 x 864	1024 x 768		800x 600		640 x 480
Name	Resolution	60	60	60	60	75/60	75/60	60	75/60	85	75/60	85	75/60	75	85	75/60	85	75/60	85/75/60
HD 1080	1920x1080p	2	-	-		-	-	-	-	-	-	-	-	-	-	-	-	-	-
HD 720	1280x720p	2	2	2	4	4	4	4	4	3	4	3	4	-	-	-	-	-	-
SD 480	720x480p	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	-
SD 576	720x576p	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	-
CIF	352x288p	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	1920x1200	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	1680x1050	2	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	1600x1200	2	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	1600x900	2	2	2	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	1440x900	2	2	2	3	3	-	-	-	-	-	-	-	-	-	-	-	-	-
	1400x1050	-	-	-	-	-	3												
	1360x768	2	2	2	3	3	-	3	-	-	-	-	-	-	-	-	-	-	-
SXGA	1280x1024	2	2	2	-	-	-	-	3	-	-	-	-	-	-	-	-	-	-
WXGA	1280x800	2	2	2	3	3	-	-	3	3	3	-	-	-	-	-	-	-	-

Output Resolutions		YPbPr, RGBHV, DVI-A, and DVI-I Computer Graphic Input Resolutions																	
		1920 x 1200	1680 x 1050	1600 x 1200	1600x 900	1440x 900	1400 x 1050	1360 x 768	1280 x 1024	1280x 800		1280x 768		1152 x 864	1024 x 768		800x 600		640 x 480
Name	Resolution	60	60	60	60	75/60	75/60	60	75/60	85	75/60	85	75/60	75	85	75/60	85	75/60	85/75/60
WXGA	1280 x768	2	2	2	3	3	-	3	3	3	3	3	3	-	-	-	-	-	-
	1152x 864	2	2	2	3	3		-	3	-	-	-	-	3	-	-			
XGA	1024 x768	2	2	2	4	4	-	4	4	3	4	3	4	4	3	4	-	-	-
SVGA	800x 600	2	2	2	4	4	4	4	4	3	4	3	4	4	3	4	3	4	-
VGA	640x 480	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Audio Encoding

Audio Encoding – MPEG AAC [1]	
Audio Channels	Up to 16 audio channels in channel pair groups (in any combination): • 16 embedded audio per blade (SDI) • 2 embedded audio per blade (DVI-D) • 2 analog audio per blade
Audio Bitrates	Mono: 56 to 160 kbps per audio pair Stereo: 80 to 320 kbps per audio pair
Frequency Response	From 20 Hz to 22 kHz
Sampling Rate	48kHz
Audio Modes	• Mono-Right • Mono-Left • Stereo
Maximum Analog Audio Input 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 Impedance	Audio single-ended (unbalanced) → 24 kOhms Audio differential (balanced) → 48 kOhms Audio talkback → 100 Ohms

1. Support for analog and embedded audio capture or encoding is not currently provided for the Makito X Ruggedized (#S-292E-X2R or #S-292E-X4R)

Advanced Features

Advanced Features
Multi-bitrate (MBR) Encoding
HD/SD De-interlacing
Built-in Downscaling
EIA-608-B/NTSC Line 21 Closed Captioning
EIA-708-B/SDI Closed Captioning
Forward Error Correction (FEC) using Furnace format Or PRO-MPEG FEC for TS over RTP streams
AES Encryption 128-bit or 256-bit with Furnace systems or SRT
Aspect ratio configuration
SD AFD and WSS

Metadata (Optional)

Metadata Inputs | Metadata Processing

Metadata Inputs

- KLV over SD-SDI/HD-SDI/3G-SDI
- KLV or CoT over Serial (RS-232 or RS-422)
- KLV or CoT over IP/UDP

Metadata Inputs | Metadata Processing

Metadata Processing

- CoT to KLV Conversion
- CoT relay to another IP device
- Limited KLV Insertion and Editing
- KLV Pass-through
- KLV over SDI Metadata Rate Decimation
- CC 608/708 Pass-through
- SMPTE 336M Compliant
- MISB 0601.11 Compliant
- MISB 0601 UAS metadata tag filtering
- MISB 0604.2 Compliant, supporting:
  - Synchronous and Asynchronous formats
  - High precision timecode insertion
- STANAG 4609 compliant

KLV Data Specifications

KLV Input	The serial KLV data is compliant to SMPTE 336M-2007. A 16-byte Universal Key is used to separate successive KLV packets (messages). The first 5-byte preamble (06 0E 2B 34 02) is used by the Makito X to sync on the beginning of a new KLV packet.
	The incoming serial KLV data is also formatted as per SMPTE 336M-2007 Local Data Set Coding. Examples of KLV group coding are described in MISB 0601.5, Section 5 UAS Datalink Local Data Set. (See Note below for additional implementation considerations).
Stream Insertion	Compressed video frames (and associated KLV data) are time-stamped as per MISB 0604 Section 5.3. It is assumed that users will pre-configure the Makito X Internal System Clock to the desired UTC time.
	The KLV metadata is inserted in the MPEG stream as per MISB 0604, Section 7.2 – Synchronous Carriage of Metadata.
References	SMPTE 336M-2007 Data Encoding Protocol using Key-Length-Value
	MISB 0601.5 UAS Datalink Local Metadata Set
	MISB 0604 Time Stamping Compressed Motion Imagery

Note

In case the KLV serial data is transmitted from the source to the Makito X over a relatively error-prone medium (such as wireless), it is up to the System Integrator to insure the integrity of the KLV packets by using data recovery mechanisms such as Forward Error Correction, etc.
Even with the recovery mechanisms provided by the System Integrator, there will still be some corrupted KLV data messages (e.g., the 5-byte key preamble is corrupted). The Makito X will use serial data inactivity periods of 500ms to re-initialize the internal KLV packet framer. This is in order to minimize error propagation.
Again to minimize the chance for the Makito X to not recover from potentially corrupted KLV data, the length of a KLV packet shall not exceed 500ms. Beyond this time limit, the Makito X will consider that the incoming serial data was probably corrupted (it was not able to find the KLV packet boundaries) and will therefore look for the next 5-byte preamble.

Asynchronous KLV Metadata Support

The Makito X supports Asynchronous Key-Length-Value (KLV) metadata stream signaling and AU (Access Unit) transport support (as per MISB 0604.2).

The Makito X allows users to select the encapsulation type to use for each metadata source. This provides increased flexibility with regard to systems inter-working with the Makito X.

The available encapsulation types are as follows:

- **Synchronous:** The Sync format is implemented in compliance with MISB 0604.2 Section 7.2.1 and ISO 13818-1 Section 2.12. Both content type signaling and data transport use this format.
- **Asynchronous:** The Async format is implemented in compliance with MISB 0604.2 Section 7.2.2. See also SMPTE RP 217. Both content type signaling and data transport use the Async format.
- **Asynchronous With Sync AU:** The AsyncWithSyncAu format uses the Async PMT and PES header signaling format as per MISB 0604.2 Section 7.2.2 and SMPTE RP 217. However, the PES payload / metadata AU is formatted in the same manner as the Sync option in compliance with ISO 13818-1 Section 2.12.

The default value for the metadata encapsulation is Synchronous.

The encapsulation type may be selected from the Web Interface (Output Streams Detail View), the CLI (`stream` command), or via SNMP.

Network and Management Interfaces

IP Network Interfaces | Management Interfaces

IP Network Interfaces

Standard:	• Ethernet 10/100/1000 Base-T, auto-detect, Half/Full-duplex • Static IP/DHCP (Dynamic Host Configuration Protocol) • Unicast streaming • Multicast streaming (IGMPv3, Internet Group Management Protocol) • Multiple Unicast streaming • IPv4 (Internet Protocol version 4) • IGMPv3 (Internet Group Management Protocol) for IP Multicast
Streaming Protocol (H.264):	• MPEG transport stream over UDP/RTP • Secure Reliable Transport (SRT) • RTMP (implemented according to requirements of the FMS/ Wowza/CDN based on Adobe RTMP specification) • Direct-RTP (RFC 3984) • SAP (RFC 2974)
Streaming Protocol (HEVC):	• MPEG transport stream over UDP/RTP • Secure Reliable Transport (SRT) • SAP (RFC 2974)
Connector:	• RJ45 (TIA/EIA-568)

IP Network Interfaces | Management Interfaces

Management Interfaces

Physical Interfaces:	• RS-232 RS-422 (Only available when the serial port is configured for Metadata (KLV or CoT))[1] • RJ45 to RS-232 (DB-9 Serial Management Adapter required, provided with unit) (TIA/EIA-568)[2] • Ethernet
Management Protocols:	• HTTPS (Web browser) • Command line over SSH, Telnet, or RS-232 serial line • SFTP/TFTP/SCP Client/Server • SNMP v3

1. Support for RS-422 is not currently provided for the Makito X Ruggedized SDI (#S-292E-X2R or #S-292E-X4R)
2. Support for RJ45 to RS-232 is not currently provided for the Makito X Ruggedized SDI (#S-292E-X2R or #S-292E-X4R)

Chassis Options

Tip

All blades manufactured by Haivision are hot-swap capable, meaning that they can be installed and removed with the chassis powered.

Single-Height Appliance

Single Height Appliance (#S/B-292E-DVI, #S/B-292E-HDSDI2 or #S/B-292E-HDSDI1)	
Dimensions (H x W x D)	21mm H x 129mm W x 196mm D (0.83" H x 5.1" W x 7.7" D)
Weight	Approximately 1.14 kg (2.5 lbs.)
Power Requirements	12VDC, 20W (each blade) **Note** IEC 60601-1 Class I and II power supplies are available from Haivision.
Power Connector	On unit: Conxall p/n 17282-3PG-300 Mating connector: Conxall p/n 16282-3SG-318
Temperature	Operating: 0°C to 40°C (32°F to 104°F) Non-operating*: -30°C to 70°C (-22°F 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)

Dual-Height Appliance (Storage Mezzanine)

Dual Height Appliance (#S/B-292E-DVI-FS or -RS, #S/B-292E-SDI2-FS or -RS or #S/B-292E-SDI1-FS or -RS)	
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 1.33 kg (2.9 lbs.)
Power Requirements	12VDC, 25W (each double-height blade) **Note** IEC 60601-1 Class I and II power supplies are available from Haivision.
Power Connector	On unit: Hirose p/n HR30-6R-3P(71) Mating connector: Hirose p/n HR30-6P-3S(71)

Dual Height Appliance (#S/B-292E-DVI-FS or -RS, #S/B-292E-SDI2-FS or -RS or #S/B-292E-SDI1-FS or -RS)	
Temperature	Operating: 0°C to 40°C (32°F to 104°F) Non-operating*: -30°C to 70°C (-22°F 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)

Dual-Height Appliance (HEVC Mezzanine)

Makito X HEVC: Dual-Channel (#S/B-292E-SDI2-HEVC) or Single-Channel (#S/B-292E-SDI1-HEVC)	
Dimensions (H x W x D)	42mm H x 129mm W x 196mm D (1.7" H x 5.1" W x 7.7" D)
Weight	Approximately 1.36 kg (3 lbs.)
Power Requirements	12VDC, 25W (each double-height blade) 100-240VAC 60W external locking power supply
Power Connector	On unit: Hirose p/n HR30-6R-3P(71) Mating connector: Hirose p/n HR30-6P-3S(71)
Temperature	Operating: 0°C to 40°C (32°C to 104°F) Non-operating: 30°C to 70°C (-22° to 158°F) *Limited by the power supply storage: -30°C
Relative Humidity	Up to 95% without condensation
Heat	~25 Watts or 85.4 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, #F-MB6X-DC)	
Dimensions (H x W x D)	19" rack mountable, 1 RU 44.069mm H x 440.004mm W x 420.37mm D (1.735" H x 17.323" W x 16.55" D) Tolerances are +/-0.50mm (+/- 0.020in.)
Weight	6 slot empty chassis: 7.94 kg. (17.5 lbs.) Single blade: Approximately 240 g (0.529 lbs.)
Power Requirements	Single Internal Power Supply: • F-MB6X-RAC (Redundant AC type): 90-264VAC 47Hz-63Hz • F-MB6X-MED (Medical Grade): 90-264VAC 47Hz-63Hz • F-MB6X-DC (DC type): 20-36 VDC 300 watt maximum (all types)
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	155 Watts or 530 BTU/hr

MB6X - 6-Blade Chassis (#F-MB6X-RAC, #F-MB6X-MED, #F-MB6X-DC)	
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)

MB21B - 21-Blade Chassis (#F-MB21B-R)	
Dimensions (H x W x D)	19-inch rack mountable, 4RU *177.29 mm H x †441.35 mm W x 462.55 mm D (6.980 inches H x 17.376 inches W x 18.211 inches D) *186.76 mm / 7.353 inches H with rubber feet installed †482.60 mm / 19.000 inches W including mounting flanges
Weight	Empty 21-slot chassis: 17.24 kg. (38 lbs.) Each blade: 230 g. (0.5 lbs.)
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)

MB21X - 21-Blade Chassis (#F-MB21X-R)[1]	
Dimensions (H x W x D)	19-inch rack mountable, 4RU *177.29 mm H x †441.35 mm W x 461.92 mm D (6.980 inches H x 17.376 inches W x 18.186 inches D) *186.76 mm / 7.353 inches H with rubber feet installed †482.60 mm / 19.000 inches W including mounting flanges
Weight	Empty 21-slot chassis: 32.5 pounds Single blade: Approximately 240 gm (0.529 lbs.)
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 Series 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/X4 products *only*; excludes classic Makito encoder/decoder or Torpedo blades

Makito XR (Military Spec) Appliance

Makito XR (Military Spec) Appliance (#S-292E-X2R OR #S-292E-X4R)	
Dimensions	99mm H x 216mm W x 170mm D (3.9″ H x 8.5″ W x 6.7″ D)
Weight	3 kg (6.81bs.)
Power	28VDC, 30W MIL-STD-1275D
Temperature	Operating: -40°C to 70°C (-40°F to 158°F) Non-operating: -45°C to 85°C (-49°F to 185°F)
Relative Humidity	0-100% condensing
IP rating	IP67

Makito X Harsh Environment Chassis

Makito X Harsh Environment Chassis Option (#S-292E-X1H, #S-292E-X2H or #S-292D-X2H)	
Fanless operation for high temperature applications	
Dimensions	44mm H x 137mm W x 203mm 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: 0ºC to 70ºC (32ºF to 158ºF) Non-operating: -40ºC to 85ºC (-40ºF to 185ºF)
Relative Humidity	0-95% condensing
IP rating	IP42

Supported Storage Devices

Fixed Storage Mezzanine | Removable Storage Mezzanine | Network Attached Storage

Makito X Fixed Storage Mezzanine (#S/B-292E-DVI-FS, #S/B-292E-SDI2-FS or #S/B-292E-SDI1-FS)	
mSATA SSD - 128 GB to 1 TB Recommended Devices: Samsung SSD 850 EVO Series and Crucial MX200 SSD	
Samsung SSD 850 EVO Series	250GB (MZ-M5E250BW) 500GB (MZ-M5E500BW) 1TB (MZ-M5E1T0BW)
Crucial MX200 SSD	250GB (CT250MX200SSD3) 500GB (CT500MX200SSD3)
Note Maximum 1 amp. USB hubs are not supported	
SD and SDHC devices up to 32 GB	

Fixed Storage Mezzanine | Removable Storage Mezzanine | Network Attached Storage

Makito X Removable Storage Mezzanine (#S/B-292E-DVI-RS, #S/B-292E-SDI2-RS or #S/B-292E-SDI1-RS)	
2.5" x 7mm SATA SSD - 128 GB to 1 TB Recommended Devices: Samsung SSD 850 PRO Series and Crucial MX200 SSD	
Samsung SSD 850 PRO Series	128GB (MZ-7KE128BW) 256GB (MZ-7KE256BW) 512GB (MZ-7KE512BW) 1TB (MZ-7KE1T0BW)
Crucial MX200 SSD	250GB (CT250MX200SSD1) 500GB (CT500MX200SSD1) 1TB (CT1000MX200SSD1)
SATA SSD can be removed or inserted at least 500 times.	

Fixed Storage Mezzanine | Removable Storage Mezzanine | Network Attached Storage

Network Attached Storage devices
Any NFS server up to client side version 3

Note

HDDs (Hard Disk Drives) are not supported.

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
	STANAG 4609 compliant (NATO Digital Motion Imagery Standard)
Compliance with Environmental Regulations	RoHS2, European Union Directive 2011/65/EU
	RoHS, Marking Control for China, Regulation SJ/T 11364-2006
Acoustic Noise	Telcordia GR-63 Section 4.6, Issue 3

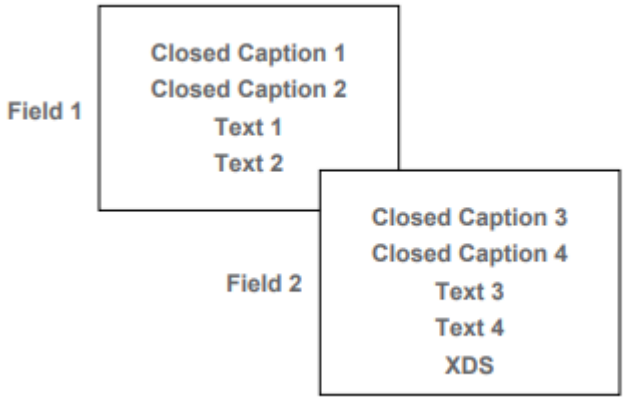
Note

Please refer to the product Declaration of Conformity (DoC) for complete details.

Closed Captioning

The Makito X supports capture, multiplexing and transport of Closed Captioning (CC) and other Line 21 information over Composite (with no 7.5 IRE setup on Line 21), as well as HD/SD SDI input interfaces.

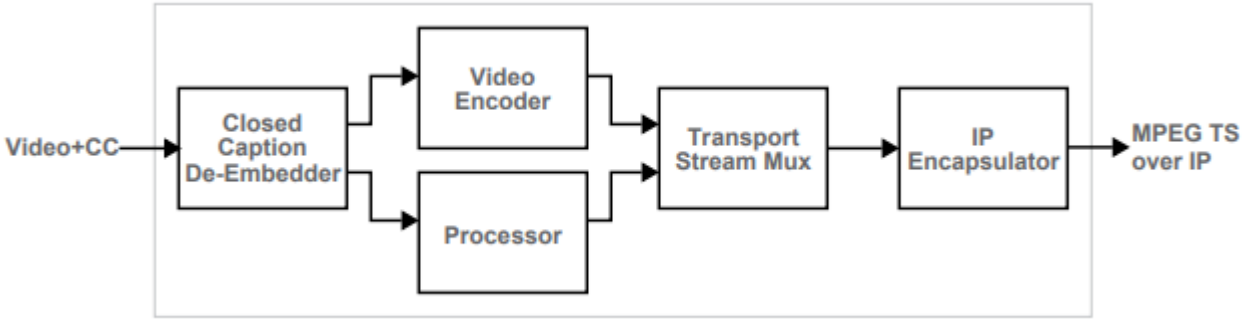
Closed Captioning data, as defined by the EIA-608-B standard, includes the following services over Line 21 Fields 1 and 2 of an NTSC analog video signal: CC1, CC2, CC3, CC4, Text1, Text2, Text3, Text4, and XDS (see Figure B-1 below). The Makito X encoder supports transport of all these services. [Note that Closed Captioning as specified by EIA608-B does not exist over PAL.]



Line 21 of each field can contain up to 2 bytes of information, which can be used by any of the above services (not simultaneously but rather successively). With NTSC video at 30fps, the maximum EIA-608-B mandated throughput represents:

```
2 bytes x 2 Fields x 30fps x 8 bit/byte = 960 bps
```

The block diagram below shows the workflow for video and CC data into the encoder.



Note

The extracted CC information from Line 21 is embedded in the MPEG stream as per ATSC A/72 Part 1:2008 (ATSC A/53 Part 4:2007).
Unicast and Multicast streams all carry the same CC data.

The Makito X encoder supports the capture of EIA-608 and EIA-708 closed captions from the video input at the HD/SD SDI interface and encodes it in the Makito X Transport Stream using the encapsulation format specified in ATSC A/72.

Note

The Makito X only supports a maximum of three (3) Caption active services at a time plus CC1-4 Text1-4 and XDS.
SMPTE 334-2 defines a Caption Distribution Packet (CDP) consisting of a sequence of bytes that can hold: the CEA-708 DTV caption data, CEA-608 caption data, caption service information, and SMPTE 12M-1 time code. CDP also includes the Caption Service Descriptor (CSD). As defined in ATSC A/65.

With the support of EIA-708, ATSC A/72 mandates a dedicated link bitrate of 9600 bits/sec. (1200 bytes/sec or 20 bytes per frame for a p60 SDI signal). Of the 9600 bits/sec, 960 bits/sec are reserved for EIA-608 captions. 8640 bits/s are dedicated to 708-CC. This is a dedicated channel, so it has to be filled with filler data if no captioning information is present.

Supported resolutions include 1080p, 720p, 1080i, 480i, and 576i.

Open Source Software Credits

This appendix lists the Open Source software packages currently deployed on the Makito X encoder 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. S ee: Permissive free software licence wikipedia entry for more information.

Topics in This Chapter

- Open Source Software Credits List
- Third Party License Information

Open Source Software Credits List

Haivision is grateful to the following organizations for making available their Open Source software packages:

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	GPL v2, June 1991
busybox	1.17.3	Common unix fixes	GPL v2, June 1991
chkconfig	1.3.30c	Service run level configuration	GPL v2, June 1991
chrony	3.2.1	Alternate Network Time Protocol (NTP) alternative	GPL v2, June 1991
coreutils	8.9	Basic shell, file and text manipulation	GPL v3, June 2007
cracklib	2.8.18	2.8.18	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
e2fsprog	1.41.14	Second Extended File System Management Programs	GPLv2 (applications) LGPL v2 (libraries) BSD (uuid library) MIT (ss library)
ethtool	2.6.38	Network interface controller configuration	GPL v2, June 1991

Package	Version	Description	License
exfat-fuse	1.1.0	exFAT File System in User Space (FUSE) utilities	GPLv2
expat	2.0.1	XML Parsing Library	Custom License See “expat Custom License” in Third Party License Information
fuse	2.9.3	File System in User Space utilities	GPLv2, June 1991
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 iperf3	2.0.5 3.1	Internet Bandwidth Measurement Tool	University of Illinois - permissive free software license
iproute2	2.6.38	Linux TCP/IP traffic control	GPL v2, June 1991
jpeg	8b	JPEG Software Tools	Lane & Vollbeding - permissive free software license
lftp	4.6.1	File Transfer Program	GPLv3, June 2007
libevent	2.0.17	Event notification library	3-clause (“modified”) BSD License
libuuid	1.0.3	Universal Unique Identifier support library	Modified BSD
lighttpd	1.4.41	Lightweight open-source web server	Jan Kneschke, 2004 - permissive free software license
mDNSResponder	320.10.80	Multicast DNS Responder (Bonjour component)	Apache 2.0 Three-Clause BSD National ICT Australia Limited (NICTA) Public Software
mtd-utils	2.0	Memory Technology Device (MTD) utilities for nor, nand access and UBI & JFFS2	GPL v2, June 1991
mtr	0.92	MyTraceroute network diagnostic tool	BSD license {C} 1991, 1993
ncurses	5.5	Text-base UI library	Permissive free software license

Package	Version	Description	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	5.5.2.1	Simple Network Management Protocol	Multiple BSD Licenses
ntfs-3g	2014.2.15	NTFS driver	GPL v2, June 1991
ntpd	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
parted	3.2	GNU Partition Table Editing	GPLv3, June 2007
pcre	8.21	Perl Compatible Regular Expression Library	BSD License
popt	1.16	Command Line Parsing Library	Permissive free software 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

Package	Version	Description	License
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 Data Acquisition Tool	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 See Third Party License Information
zlib	1.2.5	Compression library	Jean-Loup Gailly - Permissive free software license

Third Party License Information

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

Copyright (c) 2001 - 2011, The Board of Trustees of the University of Illinois. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 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)

Copyright (C) 1998, 1999 Theodore Ts'o
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS"' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR 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 NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Warranties

1-Year Limited Hardware Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

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

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

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

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

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

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

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

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

OBTAINING WARRANTY SERVICE

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

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

APPLICABLE LAW

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

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

EULA - End User License Agreement

READ BEFORE USING

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

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

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

SLA - Service Level Agreement

1. Introduction

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

2. Definitions

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

3. Service Levels for the Video Content Management System

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

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

4. Exceptions to Availability for the VCMS

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

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

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

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

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

5. Credits for Downtime for the VCMS

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

6. Support Services for the VCMS

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

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

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

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

7. Service Levels for Haivision Streaming Media Service

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

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

Agents and Polling Frequency

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

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

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

8. Credits for Outages of Haivision Streaming Media Service

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

9. No Secondary End User Support

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

Getting Help

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

info@haivision.com
www.haivision.com

North America: 1.877.224.5445
International: +1.514.334.5445

HAIVISION