HAIVISION

Makito X4 Encoder 1.1
User's Guide

HVS-ID-UG-MX4E-11, Issue 01

Edition Notice

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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

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

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

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

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

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

Obtaining Documentation

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

Getting Service Support

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

Introduction

This section provides an overview of the Makito X4 Encoder Family, along with a description of the main hardware components and key features.

Topics Discussed

- New Product Features
- Product Overview
  - Chassis Styles
  - AVC and HEVC Encoding
  - Secure Reliable Transport (SRT)
  - IPv4 and IPv6 Support
- Physical Description
  - System Interfaces
  - Audio/Video Interfaces
  - LED Status Indicators
- Setting Up the Encoder
- Resetting the Encoder
- Hardware Maintenance
  - Replacing the RTC Battery

New Product Features

Makito X4 Version 1.1 introduces the following new features and enhancements to existing capabilities:

Makito X4 Rugged Appliance

The Makito X4 Rugged Appliance features four 3G-SDI input ports (three of which also support Composite video). Designed to operate in the most demanding environments, it complies with MIL-STD-810G, MIL-STD-461G, DO-160 and MIL-STD-1275E, and is an invaluable tool for ISR applications.

Scaling and Cropping

Scaling changes the resolution of encoded content to better match your workflow. (Only progressive content can be scaled at this time.) Cropping center-cuts an image to focus in on important content for encoding and streaming.

De-Interlacing

This feature converts interlaced content to progressive video to better match your workflow and convert sources to alternative formats.

Input Image Filtering

This feature reduces the noise in your source video and enhances the encoding efficiency.

CBR Rate Control

You can now constrain the Makito X4's bitrate for encoded video using the Partial Image Skip tool to inter-operate on constrained bandwidth networks..

Intra-Refresh Coding

This feature reduces your bandwidth fluctuations and lowers latency on constrained bandwidth networks links.

EMS Integration

The Makito X4 Encoder can now be paired with a Haivision EMS (Element Management System) to discover, manage and monitor all of your Makitos from one place.

KLV or CoT over Serial for MX4E Rugged

ISR customers can now capture KLV (SMPTE 336) or CoT metadata from the serial port (Makito X4 Rugged only), manipulate that metadata and transport it within a MPEG-2 TS container as per MISB Sync/Async transport formats 0604.2 and MISB 1402.

HTTP Strict Transport Security

The Makito X now supports HTTP Strict-Transport-Security (abbreviated as HSTS) that forces web browsers to only contact the Web interface over HTTPS, instead of using HTTP.

Current Temperature of the Board Available on Web Interface and via SNMP

Remote SNMP users as well as Web interface users need to read the temperature of the board, in particular, when the cooling has failed for the Makito. The current board temperature is now shown in the Web interface and via SNMP in deg C. (It was already available from the CLI using the temperature command.)

Product Overview

Haivision's Makito X4 is a real-time HEVC/H.265 and AVC/H.264 video encoder, designed for demanding live video applications. It can ingest a full 2160p50/60 4K UHD (Ultra High Definition) video source or up to four 1080p50/60 HD inputs as well as up to 32 channels of digital audio. The Makito X4 is available either as a compact standalone appliance or a rack-mountable blade.

Makito X4 features include the following:

- **4K Broadcast Quality Video** – The Makito X4 can encode live video in HD or 4K for streaming over IP networks in a broad range of applications. It can encode with 8- or 10-bit pixel depth to deliver excellent picture quality, even at low bitrates. For workflows where color precision is needed, it offers 4:2:2 chroma subsampling to maintain color fidelity and prevent artifacts, in downstream workflows.
- **Ultra Low Latency Streaming** – The Makito X4 offers eight encoding cores that can securely deliver simultaneous low latency multi-bitrate streams over challenging networks, including the public internet.
- **High Density HEVC Encoding** – When used in Haivision rack-mountable enclosures, the Makito X4 offers high channel density, providing facilities up to 84 HD or 21 UHD video sources within a single 4RU rack module.
- **Secure Content Encryption and Reliable Streaming** – The Makito X4 can encrypt video streams with up to 256-bit AES key lengths using the SRT protocol. It also adapts to fluctuating network bandwidth in real-time, limiting packet loss and ensuring uninterrupted high-quality video.

Topics **Discussed**

- **Chassis Styles**
- **AVC and HEVC Encoding**
- **Secure Reliable Transport (SRT)**
- **IPv4 and IPv6 Support**

Chassis Styles

The Makito X4 is available in the following chassis styles:

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

In addition, the following ruggedized appliance is available:

- Makito X4 Rugged Video Encoder -- compact, rugged, quad-input H.264 and HEVC video encoder for real-time delivery of motion imagery for ISR platforms.

The Makito X4 appliance and blade, MB6X and MB21 chassis, and Makito X4 Rugged Encoder are shown in the following figures.

Makito X4 Encoder (#S-MX4E-SDI4)

Makito X4 Encoder blade (#B-MX4E-SDI4)

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)
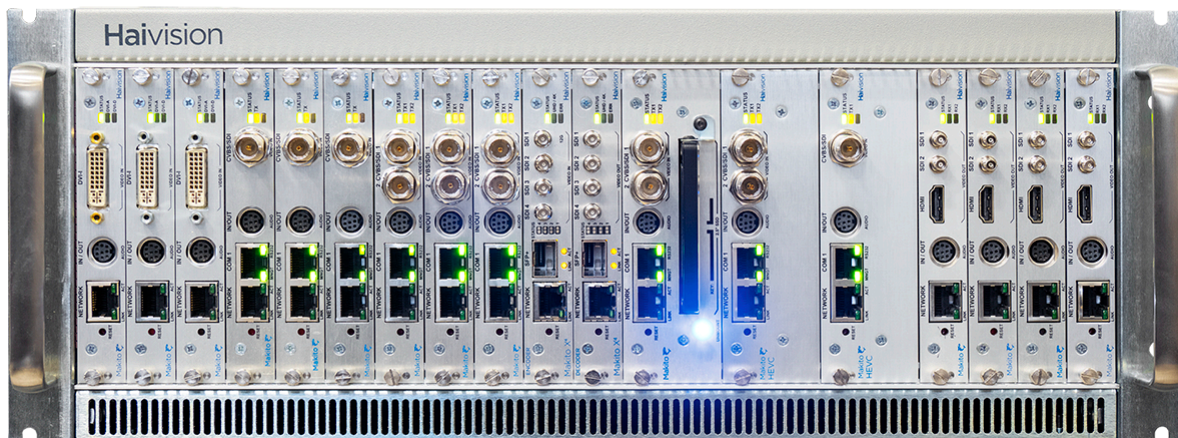
Makito X4 Rugged Encoder (#S-MX4E-R-SDI4-ISR)

> ℹ **Note**
>
> For details, please refer to the Makito X4 Rugged Encoder Installation Guide.

AVC and HEVC Encoding

The Makito X4 supports concurrent AVC/H.264 and HEVC/H.265 video encoding.

High Efficiency Video Coding (**HEVC**), also known as H.265 and MPEG-H Part 2, is a video compression standard. HEVC is designed to improve coding efficiency compared to its precedent, Advanced Video Coding (**AVC**), also known as H.264 or MPEG-4 Part 10.

The Makito X4 supports up to eight encoding cores up to UHD resolutions. Multiple codecs with different parameters may be functional all at the same time. The supported bit depth of each HEVC or H.264 encoding core is 8 or 10 bits. The encoder color space supports 4:2:0 and 4:2:2 chroma coding (as per ITU-R Recommendation BT.709).

Related Topics

- **Configuring Video Encoders**
- **Video Encoding**

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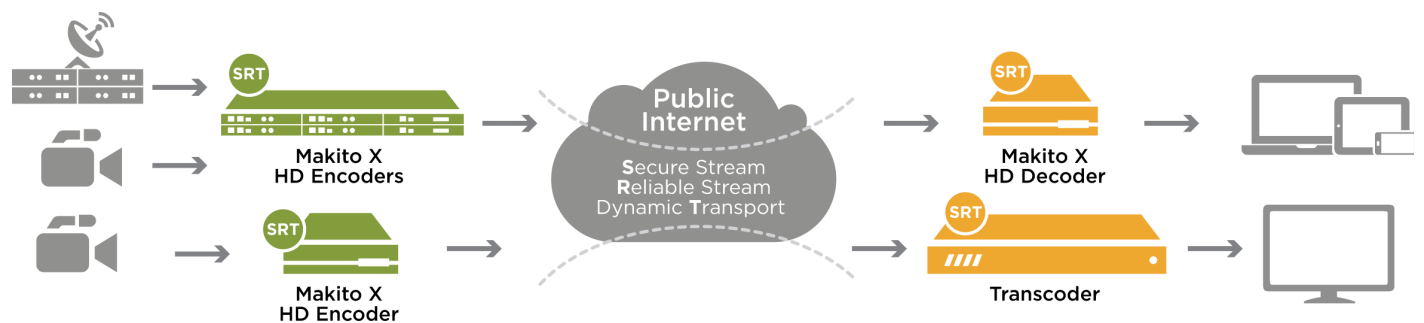
For additional information required to set up and tune SRT streams from the encoder to the decoder, please refer to the **SRT Deployment Guide**.

Related Topics

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

IPv4 and IPv6 Support

The Makito X4 series and Makito FX devices support Internet Protocol Version 4 (IPv4-only) and Version 6 (IPv6-only) as well as dual-stack IPv4/IPv6 networks. You can install the Makito X4 or FX on an IPv4 network, 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.

Makito X4 and FX IPv4-IPv6 capabilities include the following:

- Static and dynamic assignment of IPv6 addresses via DHCPv6 or Stateless Autoconfiguration (SLAAC) to Makito X4/FX products in addition to the existing IPv4 capabilities.
- Dual-stack IPv4 and IPv6 may be used simultaneously for management and video streaming purposes.
- All administration functions may be performed from an IPv4 or IPv6 network client, including upgrade/downgrade, preset import/export, license install, system snapshots and specifying audit servers.
- User functions include creating and starting streams from an IPv4 or IPv6 device.

Related Topics

- **Configuring Network Settings**
- **ipconfig** (CLI command)
- **ipv6config** (CLI command)

Physical Description

> **ⓘ Note**
>
> For details on the Makito X4 Rugged interface, please refer to the **Makito X4 Rugged Encoder Installation Guide**.

System Interfaces

The Makito X4 comes equipped with the following interfaces:

- 10/100/1000 Base-T Gigabit Ethernet Network
- SFP+ (Small Form-factor Pluggable Plus) Expansion Port, 10GbE – future use, will enable (future) ST-2110 input support

Related Topics:

- **Connecting the Encoder to the Network and a Computer**

Audio/Video Interfaces

SDI Video and Embedded Digital Audio Interfaces

The Makito X4 SDI video interface consists of four 75 Ω HD-BNC connectors.

Makito X4 Encoder (#S-MX4E-SDI4)
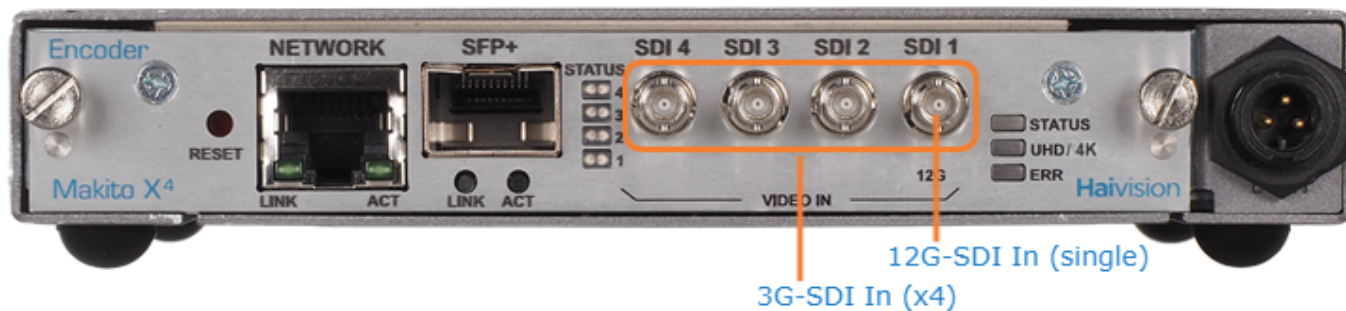
The HD-BNC connector(s) are used for SD-SDI (Serial Digital Interface), HD-SDI, 3G-SDI, 6G-SDI and 12G-SDI video input signals.

> ⚠ **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.

Related Topics:

- **Connecting to A/V Sources**

LED Status Indicators

The LED colors and flashing (blinking) speed indicate the status (operational state) of the Makito X4 encoder.

LED Status Indicators (Rear Panel)

Network Port   SFP+ Port (Future Use)   SDI Input Status   General

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)

Network Port   SFP+ Port (Future Use)   SDI Input Status   General

SFP+ Port (Future Use)

Function	Description	Indication
LINK	Off	Not connected
	Green solid	Connected
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)

Network Port   SFP+ Port (Future Use)   SDI Input Status   General

SDI Input Status

Function	Description	Indication
SDI1/SDI2/SDI3/SDI4	Off	**ⓘ Note** Each **SDI** 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).

Network Port   SFP+ Port (Future Use)   SDI Input Status   General

General

Function	Description	Indication
STATUS	Off	No power
	Green fast blinking	Reset button is pressed for less than four seconds. If the Reset button is not pressed, there is a power fault.
	Green slow blinking	Booting/Initialization
	Green solid	Booting/Initialization sequence is complete (No fault/OK).
	Red fast blinking	Reset button is pressed for more than four seconds (Factory Reset enabled).
	Red slow blinking	Reset button is released after the Red fast blinking state (executing Factory Reset).
UHD/4K	Off	No valid UHD/4K video input is detected for the SDI1 BNC connector. ⓘ **Note** Only SDI1 BNC can support 6/12G-SDI (UHD/4K) video input.
	Green solid	Valid UHD/4K video input detected (i.e., you have UHD/4K signal lock) for the SDI1 BNC connector.
ERR	Off	Future use

Setting Up the Encoder

> 🛈 **Note**
>
> For information on installing and connecting to the Makito X4 appliance, please refer to the **Makito X4 Encoder Quick Start Guide**.

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 *MB Chassis Installation Guide (available at* **https://doc.haivision.com***)*.

Safety First

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

- The Makito X4 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.

> ❗ **Important**
>
> *Refer to the* **Safety Guidelines** *and* **Waste Electrical and Electronic Equipment (WEEE) Disposal** *notice in the* **Preface** *(available at* **https://doc.haivision.com***)*.

Resetting the Encoder

- **Default Network Settings**

This section describes the steps to perform a hardware reset on the Makito X4. 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.

> ℹ️ **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 X4 settings:

1. With the encoder on, insert a small plastic tool into the small opening labeled **Reset** on the Makito X4 faceplate.

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

Related Topics:

- **Default Encoder IP Address**

Hardware Maintenance

The following maintenance tasks are recommended for the Makito X4 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 X4 appliance contains a real-time clock (RTC) powered by the following battery:

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

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

> ⚠ **Note**
>
> The Makito X4 Rugged enclosure does 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).

> ⓘ **Important**
>
> 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.

(5) Disconnect battery connector
(10) Reconnect battery connector

(6) Remove battery
(9) Press new battery
onto PCB

(8) Peel off tape

(7) Clean surface
(TransformerT1)
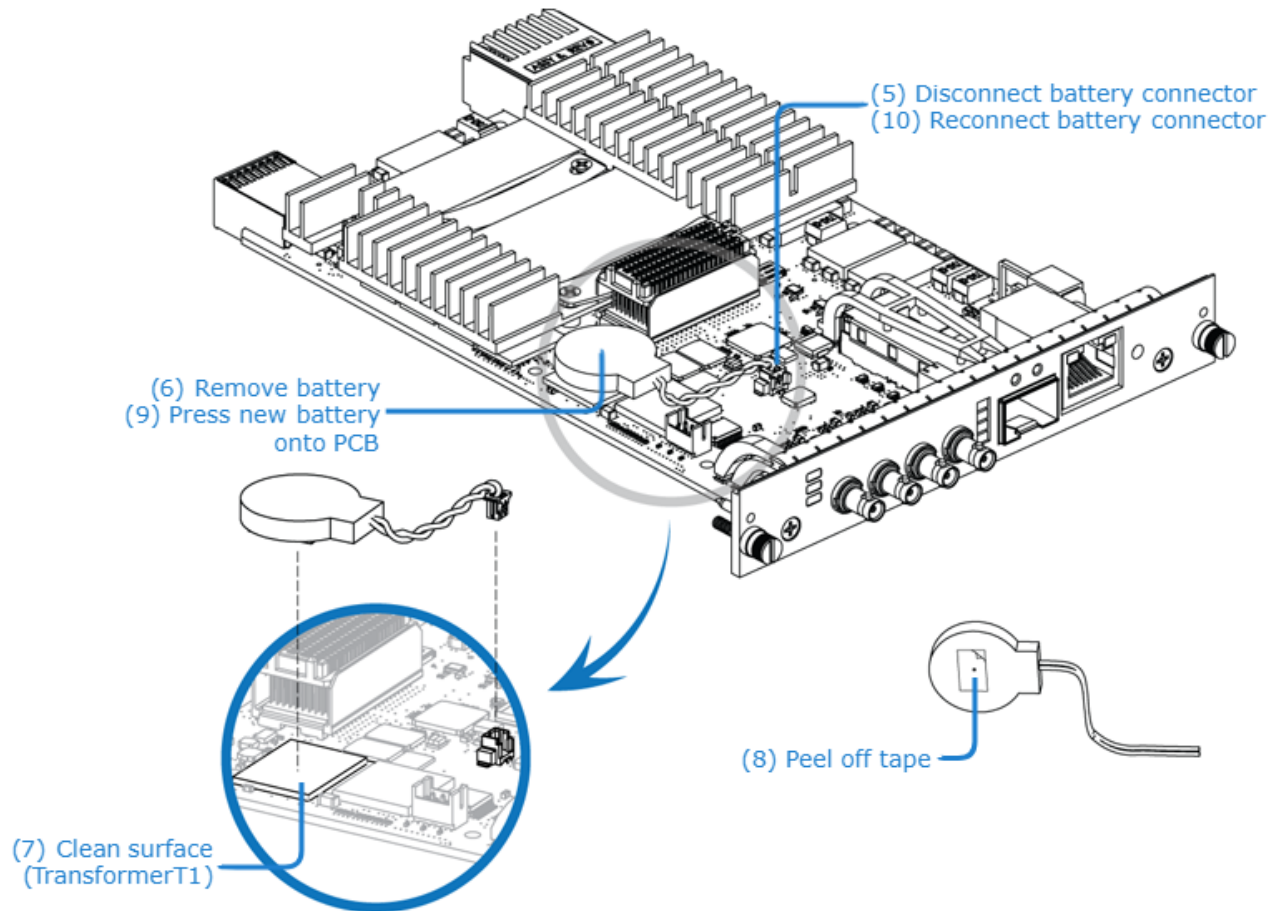
6. Remove the battery by pulling it upward from the PCB.
7. Clean the surface of transformer T1 with alcohol if there is glue residue.
8. Peel off the protective layer on the tape on the new battery.
9. Press the new battery onto the PCB (top of transformer T1) with a force of 3 pounds-force per square 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. For information on installing and connecting to the Makito X4 appliance, please refer to the **Makito X4 Encoder Quick Start Guide**.

All Makito X4 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 X4 through its Ethernet LAN port.

Topics in This Chapter

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

Accessing the Encoder

Managing the Makito X4 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 Makito X4 configuration Web page:

1.
> **ℹ Note**
>
> The Makito X4 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.)

> **✔ Tip**
>
> For a list and description of the CLI commands to configure and manage the Makito X4, see CLI Command Reference.
> For information on SNMP management of the Makito X4, see Using SNMP to Configure A/V Services.

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).

> **ℹ Note**
>
> The Makito X4 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 Makito appliance's IP Address is set by default to: `10.5.1.2` .

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

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

> ✓ **Tip**
>
> After you change the Makito appliance's 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 device to its factory settings, which will return the unit to the default IP address (and you will lose any saved configurations and settings).

Related Topics

- **Resetting the Encoder**

Role-based Authorization

The Makito X Series 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 Series 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.

> ⚠ **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.

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.

Related Topics

- Command Summary and Access Control

Signing In to the Web Interface

To sign in to the Makito X4 configuration Web page:

1. From your Web browser, type the Makito X4'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.
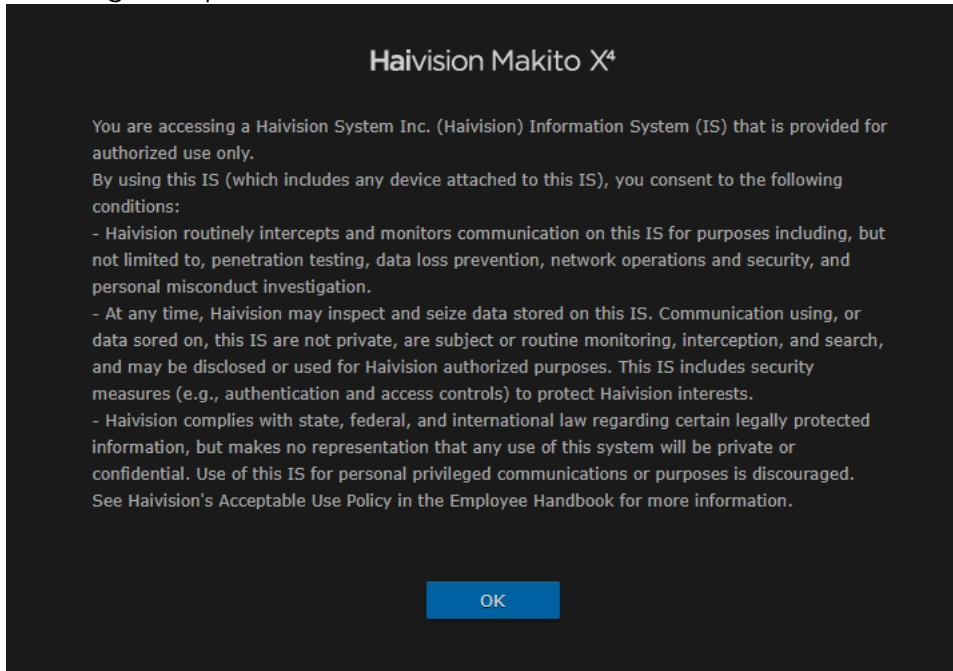
2. Review the Advisory and Consent terms as required for your system and click **OK**.
3. On the Sign-in page, type the Username and Password and click **Sign In** (or press Enter).
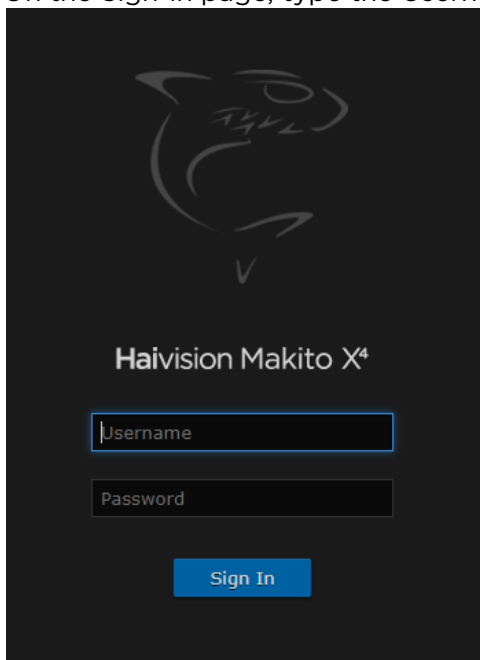
Please refer to the *Important Notice* (postcard shipped with the appliance or available from the **Download Center** on the Haivision Support Portal) for the default sign-in credentials.

Makito X4 provides three pre-defined user accounts. For information, see **Role-based Authorization**.

Exploring the Web Interface

After signing 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 Outputs List View, as shown in the following example. Your account information is displayed on the toolbar (along the top).
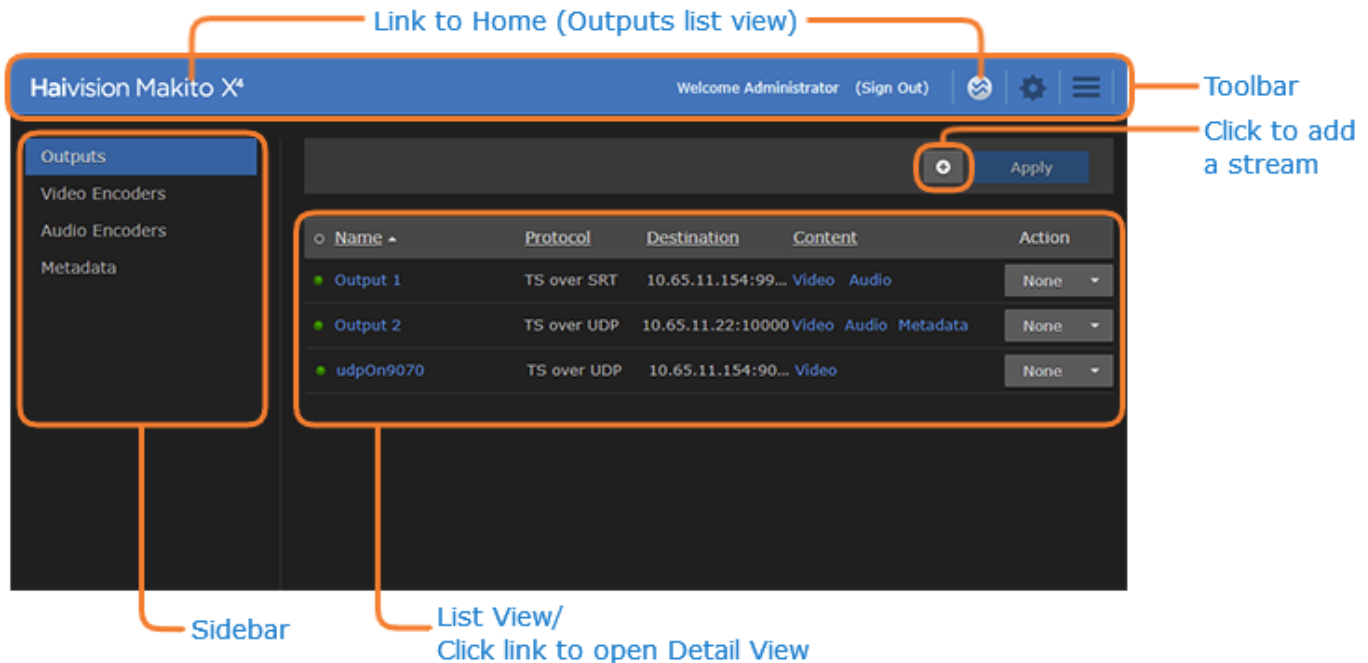
- To set up encoding, select the configuration option from the sidebar, for example, **Video Encoders** or **Audio Encoders**.
- To set up streaming, select **Outputs** from the sidebar.
- To access the encoder administration settings, click the ⚙ **Administration** icon on the toolbar, and then select 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. See **User Preferences**.

- Help — Opens the **Haivision InfoCenter** website that contains the Makito X4 documentation. See How to use the InfoCenter for tips and tricks for browsing the site.
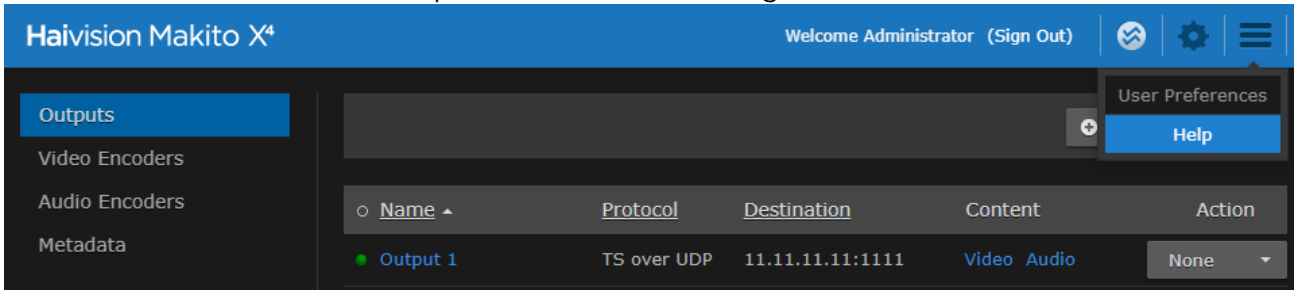
> **ⓘ Note**
>
> If no external internet connection is available, a local Makito X4 Encoder online Help is opened in your Web browser.

- (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.

Click link to open Detail View

User Preferences

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

- Adjust Brightness and Contrast display settings.
- Switch the Color Scheme between dark (default) or light.
- Reset Brightness, Contrast and Color Scheme to default settings.
- Clear Stored Preferences, 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).
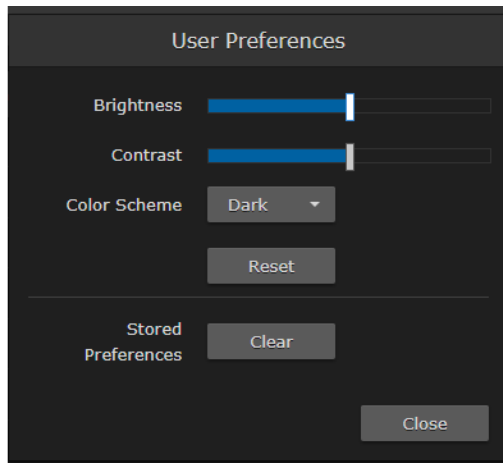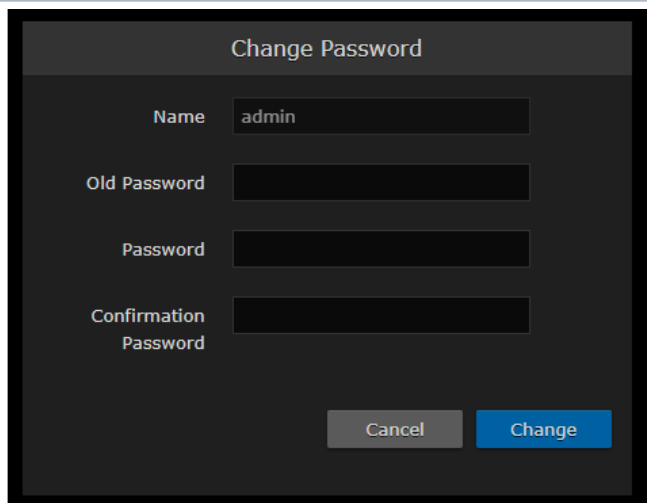
Changing Your Password

- **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 X4 on which the factory defaults have not been changed.
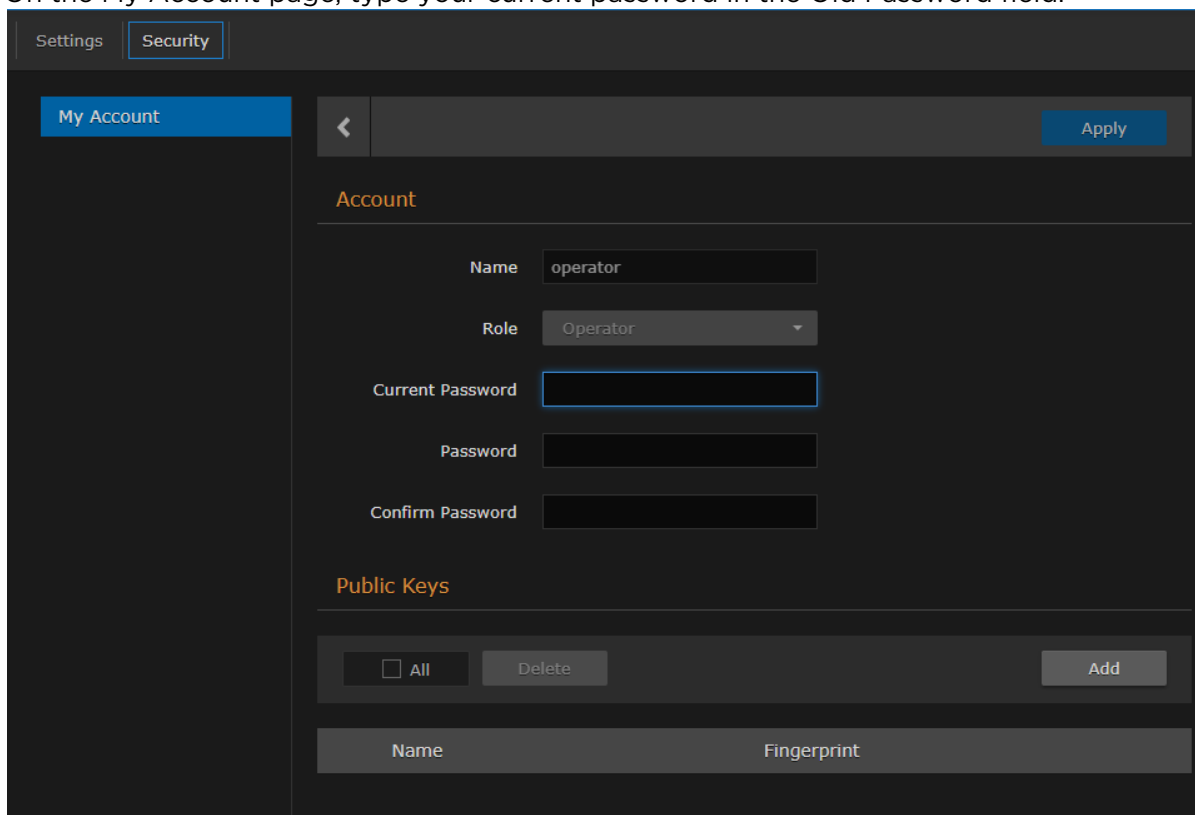
> ⓘ **Note**
>
> Administrative users may change their passwords from the Accounts page.

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 X4, 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

> ℹ️ **Note**
>
> For 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 Video Encoders

From the Video Encoders pages, you can configure up to eight video encoders to apply to streams. Each encoder can be configured independently and assigned to multiple outputs to support multi-bitrate streaming. You can start and stop each video encoder, as well as display statistics.

The Makito X4 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 and click **Video Encoders** on the sidebar.
   The Video Encoders List View opens.
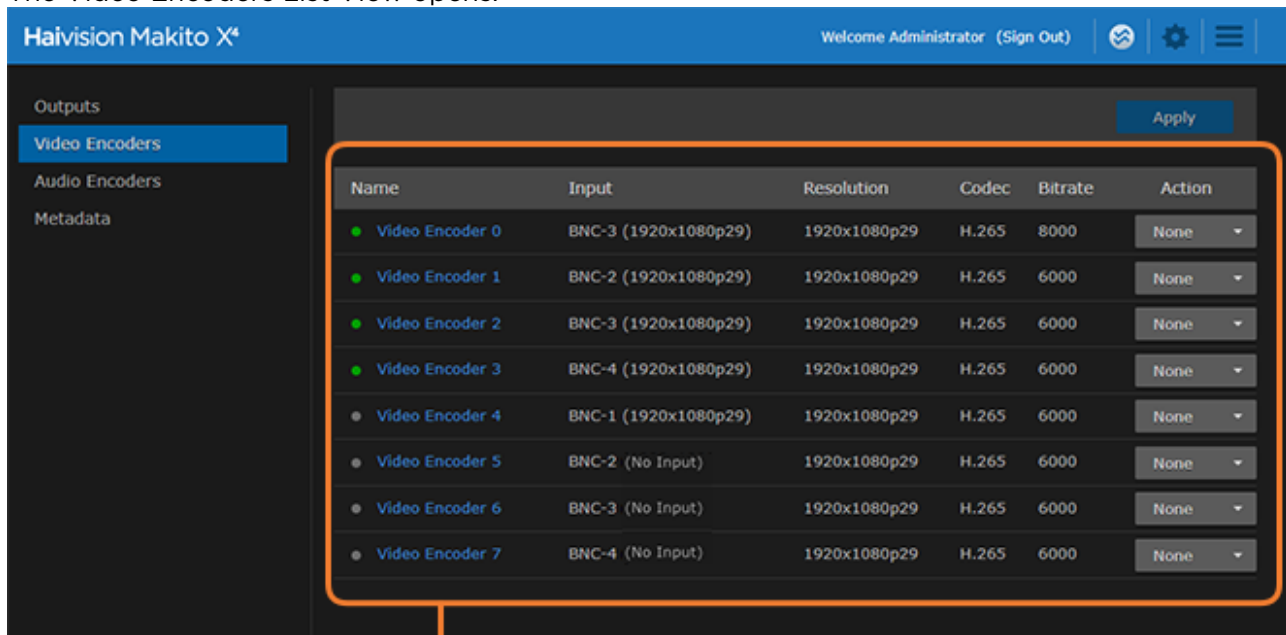
Video Encoders List View/
Click link to open Detail View

   The Video Encoders List View displays the status LED, Name, Input format, Resolution, GOP Size, and Bitrate for each video encoder.
2. From here, you can perform the following tasks:
   • 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 change the status for an encoder, click the drop-down list under **Action** and select either Start or Stop (as applicable).
3. To apply your changes, click **Apply**.

Configuring Video Encoder Settings

From the Video Encoder Detail View, you can define the Input interface and video encoding parameters, such as the Codec Algorithm, Encoding Profile, Bitrate, Frame Rate, and GOP Size.

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.
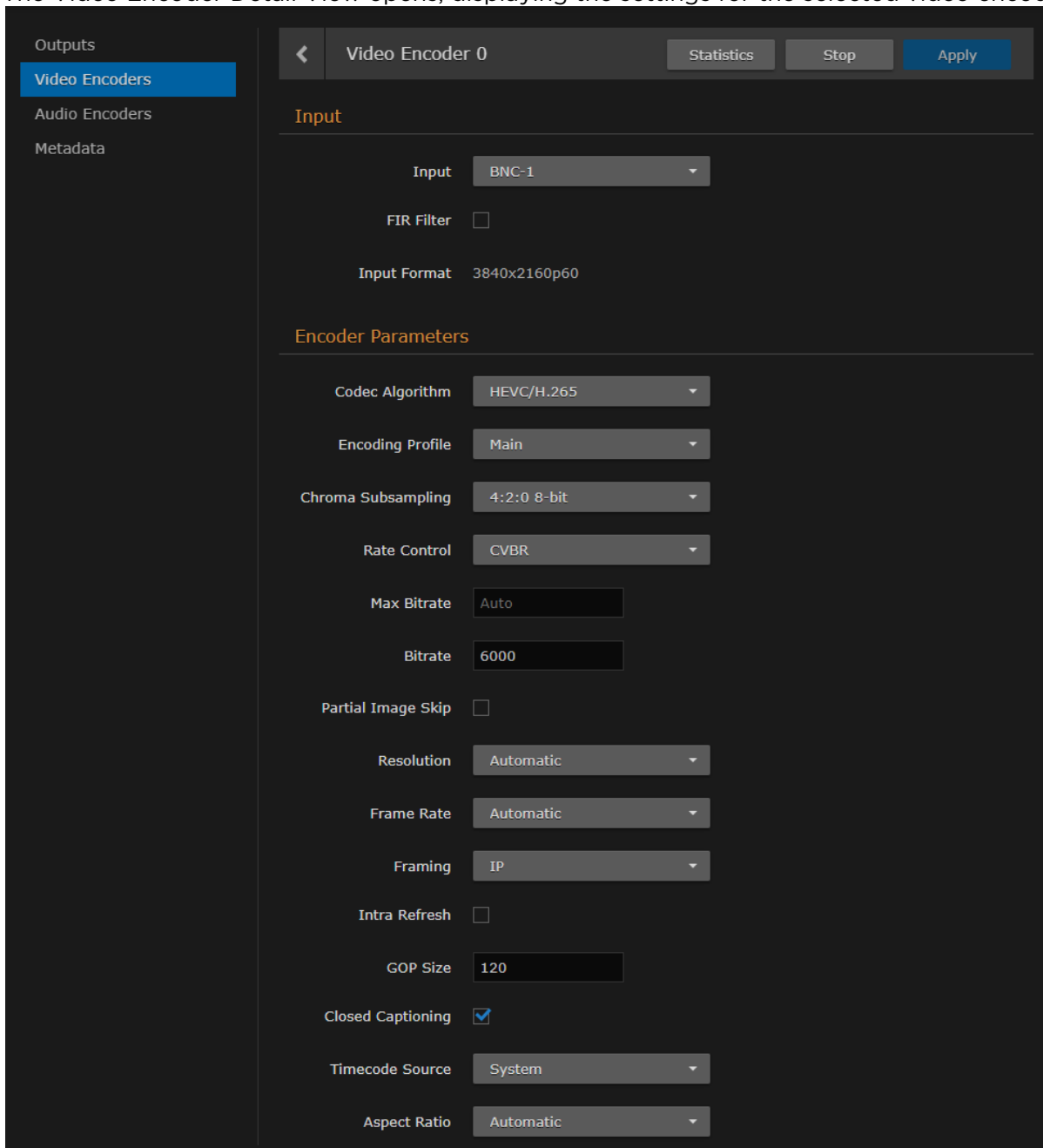
2. Select or enter the new value(s) in the appropriate field(s). See **Video Encoder Settings**.
3. To start or stop the encoder, click **Start** or **Stop** (as applicable).
4. To view statistics for the encoder, click **Statistics**. For details, see **Video Encoder Statistics**.

5. To apply your changes, click **Apply**.
6. To return to List View, scroll up and click **Video Encoders** on the sidebar.

Related Topics

- **Video Encoder Settings**
- **videnc** (CLI Command)

Video Encoder Settings

The following table lists the Video Encoder controls and settings:

Input   **Encoder Parameters**

Input

Video Encoder Setting	Default	Description/Values
Input		Select the Video Input port for the encoder:
	BNC-1	• BNC-1 • BNC-2 • BNC-3 • BNC-4 **❗ Important** Only HD-BNC-1 can support 6/12G-SDI. You must select BNC-1 in order to encode UHD over four (4) cables (in 2SI mode). See **2SI Setup** below.
FIR Filter	Disabled	Check this checkbox to enable Input Image Filtering for the input interface. FIR (Finite Impulse Response) filter refers to a type of digital filter with a finite impact on the data being processed from a temporal or spatial perspective. FIR filters do not employ recursive or other feedback mechanisms. 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. **✅ Tip** Input Image filtering is useful with sources that are monochrome, noisy and difficult to encode because the content is detailed. Enabling this parameter filters the image in order to reduce the amount of noise, resulting in better quality video after the encoding since less noise is being compressed into the stream.

Video Encoder Setting	Default	Description/Values
Input Format	n/a	**ℹ Note** If the signal cannot be detected (or is outside the supported range), the Input Format will be Unknown.

Input   **Encoder Parameters**

Encoder Parameters

Video Encoder Setting	Default	Description/Values
Codec Algorithm	HEVC	Select the codec algorithm for the encoder: (See **AVC and HEVC Encoding**) • AVC/H.264 • HEVC/H.265
Encoding Profile	Main	Select the application profile class for the encoder: (See **Product Overview** "4K Broadcast Quality Video".)
		(AVC/H.264 only) • Baseline • Main • High • High 10 • High 4:2:2
		(HEVC/H.265 only) • Main • Main 10 • Main 4:2:2 10
Chroma Subsampling	4:2:0 8-bit	Select the Chroma Subsampling for the encoder: • 4:2:0 8-bit • 4:2:0 10-bit (Encoding Profile must be Main 10 or Main 4:2:2 10) • 4:2:2 8-bit (Encoding Profile must be Main 10 or Main 4:2:2 10) • 4:2:2 10-bit (Encoding Profile must be Main 10 or Main 4:2:2 10)
Rate Control	CBR	Select the Rate Control for the encoder: • CBR (Constant Bitrate): Strictly respects the specified bitrate, aiming for a constant or unvarying bandwidth level. • CVBR (Capped Variable Bitrate): Allows the bit rate to vary but maintains the generated bitrate between the Maximum Bitrate and the specified Bitrate.
Max Bitrate	Auto	(Rate Control must be CVBR) Enter the maximum video bitrate for the encoder: 32 to 120,000 Kbps
Bitrate	6000 kbps	Enter the video bitrate for the encoder: 32 to 120,000 kbps

Video Encoder Setting	Default	Description/Values
Partial Image Skip	Disabled	(Rate Control must be CBR) Select whether to allow the encoder to skip part of the image in order to respect the bitrate limit. This parameter is used to create streams that are CBR-compliant according to the MPEG-2 TS specification. One aspect of this functionality is to have the video encoder control the total number of bits generated across a GOP sequence so that all the NALs in each GOP have roughly the same amount of bits and to avoid overflowing the coded picture buffer (CPBuf). One method of doing this is the limit the size of individual video NALs associated with a frame when the bit budget is being over-subscribed. In essence the video encoder will skip encoding part of the image in order to not oversubscribe the bit budget for the GOP sequence. ℹ️ **Note** Intra-Refresh is not an option in these situations since they use multiple types of decoders and not all of them support decoding Intra-Refresh content.
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. ℹ️ **Note** Manually selecting a coded picture resolution will increase the video encoder latency by one (1) frame period. For supported video encoding resolutions, see Supported Video Encoding Input and Downscale Resolutions (in Technical Specifications).
Resizing	Scale	(Resolution cannot be set to Automatic and must be less than the Input Format) Select whether to scale or crop the input to the desired resolution: • Scale: Changes the resolution of the encoded image from what is input to what is specified in Resolution parameter without discarding any portion of the image. • Crop: Crops the input and encodes to a rectangle within the input image while discarding the rest of the input image. When Crop is enabled, the output resolution is the portion of the input that is encoded from the center. This may be done instead of down-scaling. By default, input is scaled to the specified output resolution.
Frame Rate	Automatic	Select the coded picture frame rate per second: • Automatic: Encodes at the same frame rate as the input • 60..1 ℹ️ **Note** The frame rate cannot exceed the input frame rate.

Video Encoder Setting	Default	Description/Values
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 • IBBP: I, BB (two B frames in sequence) and P frames • IBBBP: I, BBB (three B frames in sequence) and P frames • IBBBBP: I, BBBB (four B frames in sequence) and P frames (highest delay; highest quality) ℹ **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.
Intra-Refresh	Disabled	Check this checkbox to enable Intra-refresh video encoding support. Intra-refresh minimizes latency, smooths the video bitrate, and minimizes GOP pulsing artifacts. 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 rebuilt (at the decoder) within the number of frames specified as follows: • For H.264/AVC the Intra Refresh Interval = Horizontal Encoded Resolution / 16 • For H.265/HEVC the Intra Refresh Interval = Horizontal Encoded Resolution / 32 The result is rounded up to nearest integer if it is fractional. For example: If the video encoder is encoding an output resolution of 3840x2160p60 using H.264, then the expected refresh interval is: 3840 / 16 = 240 (frames) / (60 frames/sec) = 4 seconds for a full image refresh period. ✓ **Tip** Intra-refresh requires that decoders that do not support random access points be started before the encoder is started. This can be accomplished by establishing a stream from the encoder to the decoder then stopping and starting the video encoder.
GOP Size	120	(Intra-Refresh must be disabled) Enter the Group of Pictures size for the encoded video. 1..1000
Closed Captioning	Disabled	(Optional) Check this checkbox to enable Closed Captioning on the output Stream.
TimeCode Source	None	Timecodes are used to mark video frames, for editing purposes or for multi-channel synchronization. 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 Ancillary Vertical Interval (ATC_VITC) incoming SDI video signal. Please note that Digital (D-VITC) and Linear Timecode (LTC) are not supported. • 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 recommended to enable NTP (see Configuring Network Settings).

Video Encoder Setting	Default	Description/Values
Aspect Ratio	Autom atic	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. ℹ **Note** WSS is only supported with analog PAL video; AFD is only supported with SD-SDI video.

2SI Setup

To configure the encoder in 2SI mode, connect four 1080p60/59/50 sources into the Makito X4 SDI 1, 2, 3 and 4 inputs. The encoder detects them all as one 2160p60 input source and outputs one 2160p60/59/50 stream. You must select BNC-1 as the input for the encoder.

Related Topics

- **Video Encoding** (in **Technical Specifications**)
- **AVC and HEVC Encoding**

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 • AWAIT FRAMING • STOPPED • FAILED
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 or Composite (Makito X4 Rugged Encoder only, future use).
Input Format	The input signal detected from the video source.
Output Resolution	The stream output resolution.
Input 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**.
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.

Video Encoder Statistic	Description/Values
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
UTC	The Coordinated Universal Time, for example, `1555388703053386` `(2019-Apr-16-4h25m3s53386us)`
Reset	Click to reset the Video Encoder statistics.

Makito Decoder Interoperability

The following table lists recommended settings to optimize the Makito X4 encoder configuration to stream to the Makito X decoder (release 2.4 or later):

Video Encoder Parameters	Recommended Settings (H.264/AVC)	Recommended Settings (H.265/HEVC)
Encoding Profile	Baseline, Main, and High	Baseline and Main
GOP Structure	I/IP/IBP/IBBP	I/IP/IBP/IBBP
Chroma sub-sampling / pixel depth	4:2:0 8-bit	4:2:0 or 4:2:2 8-bit or 10-bit
Bitrate	32..25000	32..15000

The following table lists *required* Video Encoder settings when configuring the Makito X4 encoder to interoperate with the Makito Classic (*previous generation*) decoder:

Video Encoder Parameters	Required Settings (H.264 only)
Encoding Profile	Baseline only
GOP Structure	I and IP only
Bitrate	150..15000

Configuring Audio Encoders

From the Audio Encoder pages, you can configure up to sixteen independent audio encoders to apply to streams. You can also start, mute, and stop each audio encoder, as well as display statistics for the encoder.

> ℹ **Note**
>
> The Makito X4 is capable of encoding up to 32 channels of audio in channel pair groups.

Audio Encoders List View

To open the Audio Encoders List View:

1. On the Streaming page, click **Audio Encoders** on the sidebar.
   The Audio Encoders List View opens.
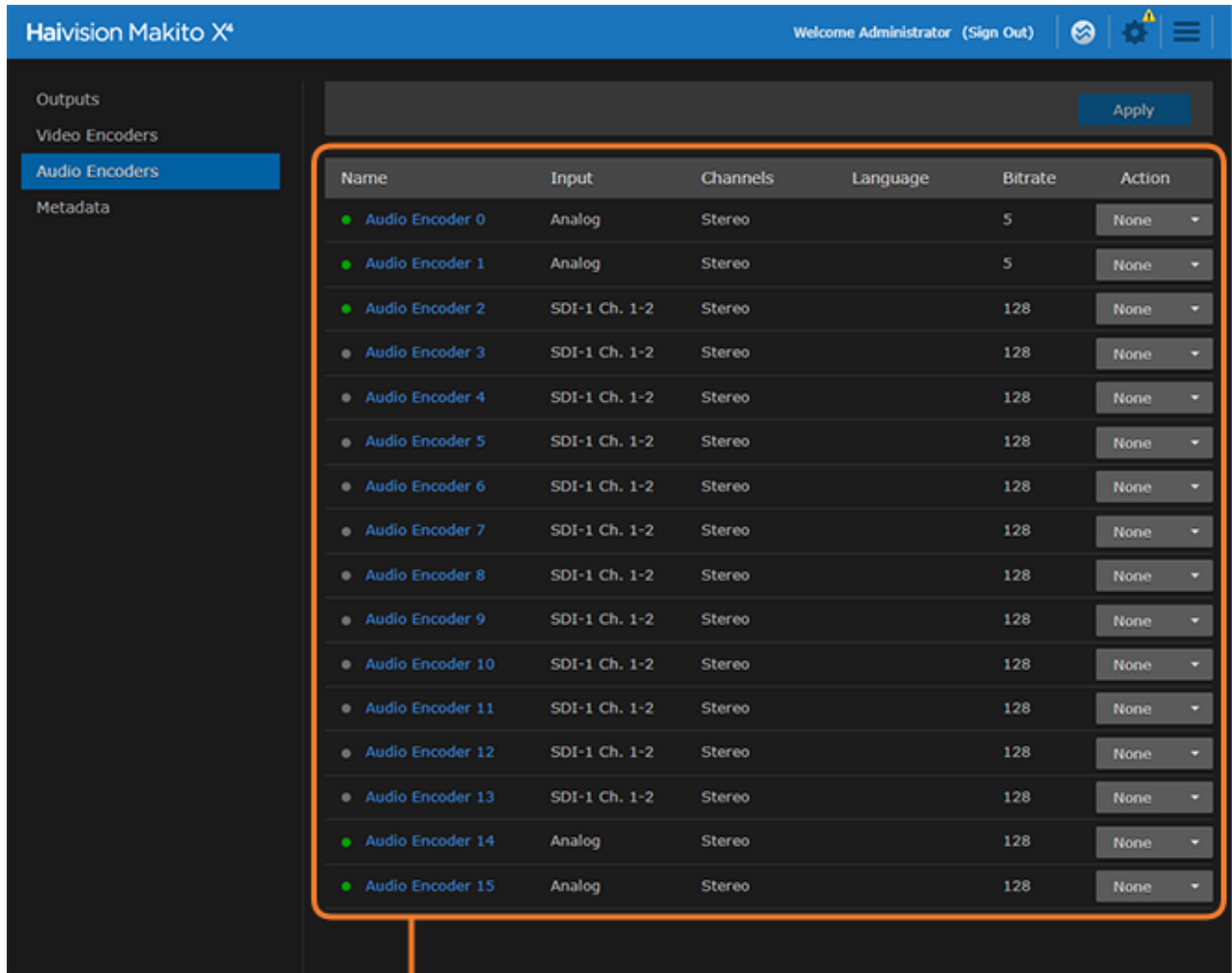
Audio Encoders List View/
Click link to open Detail View

The Audio Encoders List View displays the status LED, Name, Input, Channel Mode, Language, and Bitrate for each audio encoder.

2. From here, you can perform the following tasks:
   - 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 input, click the drop-down list under **Action** and select either Start or Stop (as applicable), or Mute.
3. To apply your changes, click **Apply**.

Configuring Audio Encoder Settings

From the Audio Encoder Detail View, you can configure audio encoding properties such as the bitrate, encoding algorithm, and language for each encoder.

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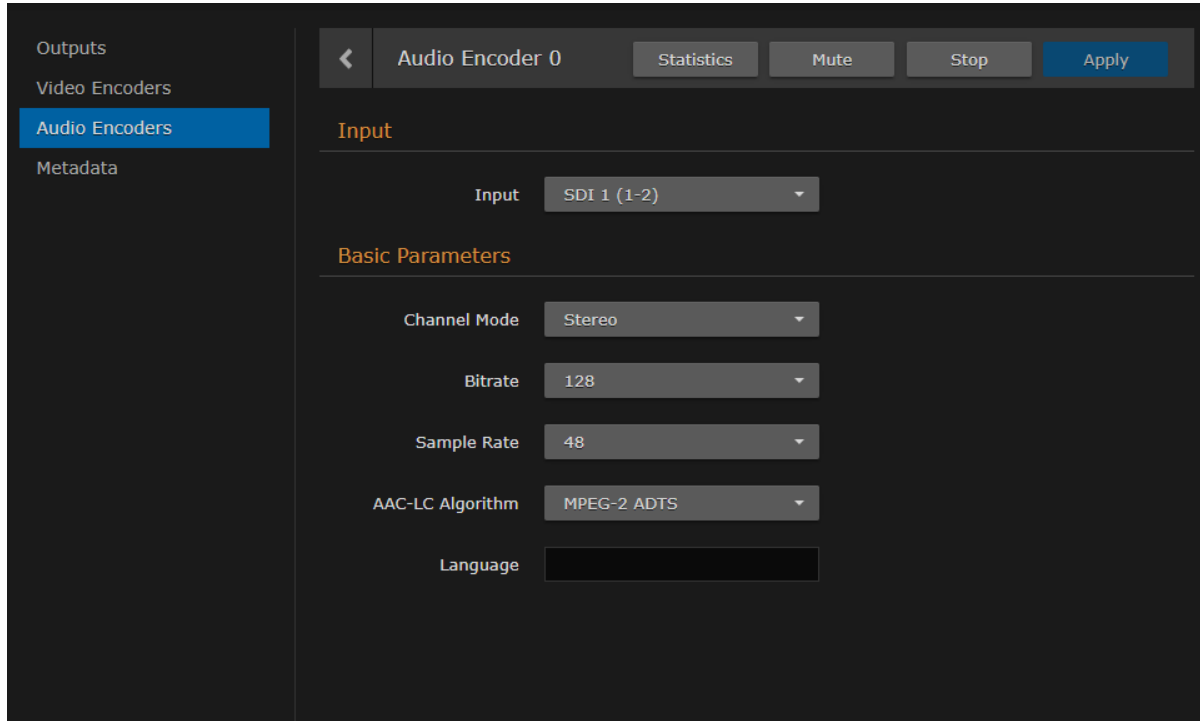
2. Select or enter the new value(s) in the appropriate field(s). See **Audio Encoder Settings**.
3. To start or stop the encoder, click **Start** or **Stop** (as applicable).
4. To mute the audio (when active), click **Mute**.

   > ℹ **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:

- **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	SDI1 (1-2)	Select the Audio Input for the encoder. • SDI1 (1-2). . (15-16) • SDI2 (1-2). . (15-16) • SDI3 (1-2). . (15-16) • SDI4 (1-2). . (15-16)

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.
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.
Language	n/a	(Optional) To specify the language of the input, start typing letters and select the language from the list. The language values are three-letter codes, defined in ISO 639-2 (**https://www.loc.gov/standards/iso639-2/php/code_list.php**).
Statistics	n/a	Click Statistics to view statistics for the encoder. See **Audio Encoder Statistics**.

Audio Setting	Default	Description/Values
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.

Related Topics

- **Audio Encoding** (in **Technical Specifications**)

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).
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, BNC-2, BNC-3 or BNC-4.
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

From the Metadata pages, you can configure the Makito X4 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 X4 supports up to three metadata input types:

Input Type	Description
SDI	The Makito X4 extracts KLV metadata packets from the HD-SDI interface as per MISB RP 0605.2. See **Configuring HD-SDI Metadata Sources**.
Network	The Makito X4 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**.
Serial port	**(Makito X4 Rugged only)** The Makito X4 Rugged extracts either KLV or CoT metadata packets from the COM1 serial port (Release 1.1 and greater). See **Configuring Serial Metadata Sources**.

The Makito X4 auto-detects the hardware setup of the encoder. SDI metadata sources are created automatically at startup by the system. UDP sources must be manually created by the user. The Makito X4 supports insertion of multiple metadata sources into the same KLV Elementary Stream.

The Makito X4 supports both synchronous and asynchronous KLV metadata stream signaling and AU (Access Unit) transport support. When configuring an (Output) stream, you can select the encapsulation type to use for the associated KLV metadata source.

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 Relaying**.

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 **Mission ID/Security Data Set 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 four SDI metadata sources are provided by default.

Click to add a Network or HD-SDI source

Metadata Sources List View/ Click link to open Detail View
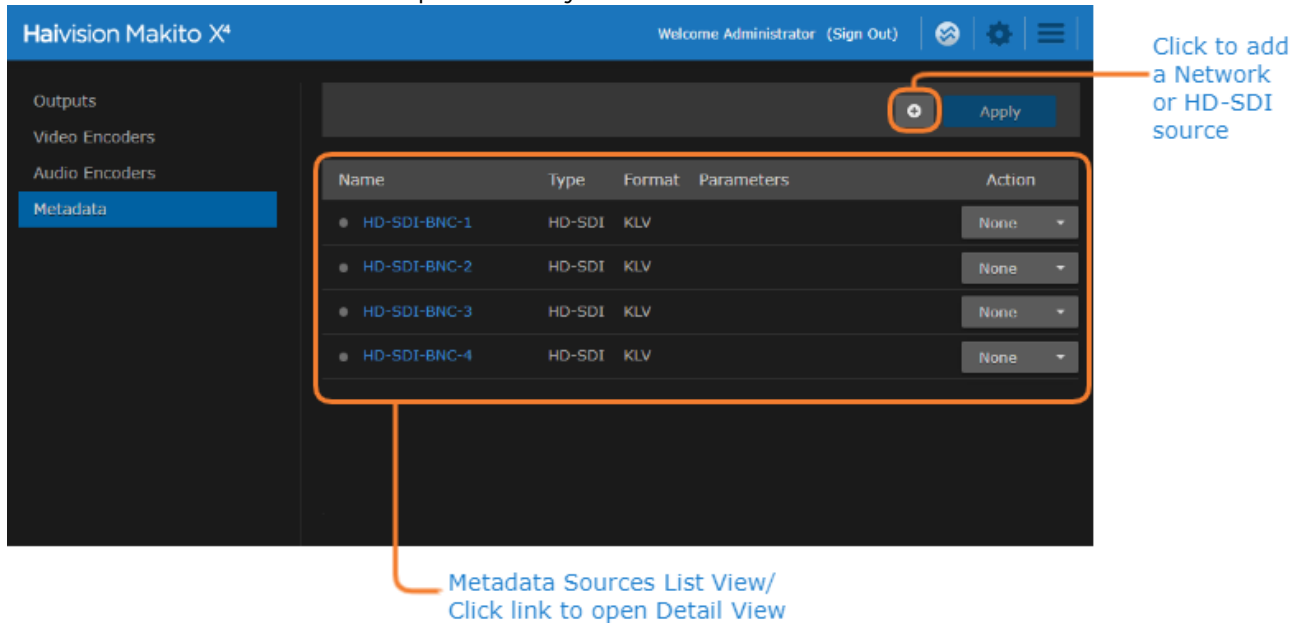
The Metadata List View displays the Status LED, source Name, Type, Format, and selected Parameters for each source.

2. From here, you can perform the following tasks:
   - 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 the ➕ **Add** button.
   - 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.
3. To apply your changes, click **Apply**.
   The following example shows the Metadata List View with serial and network sources added (Makito X4 Rugged).

Haivision Makito X⁴

Welcome Administrator (Sign Out)

Outputs						
Video Encoders						
Audio Encoders						
Metadata						

Name	Type	Format	Parameters		Action	
● (None)	Serial	CoT	Max AirCraft-SPI Delta 0 ms		None ▼	
● HD-SDI-BNC-1	HD-SDI	KLV			None ▼	
● HD-SDI-BNC-2	HD-SDI	KLV			None ▼	
● HD-SDI-BNC-3	HD-SDI	KLV			None ▼	
● HD-SDI-BNC-4	HD-SDI	KLV			None ▼	
● KLV_UDP	Network	KLV	udp://@(any):4800		None ▼	
● CoT_UDP	Network	CoT	udp://@10.65.11.149:25000		None ▼	

Configuring HD-SDI Metadata Sources

The Makito X4 auto-detects the hardware setup of the encoder and automatically creates the source(s) if SDI video is connected.

> ℹ **Note**
>
> Only progressive scan formats are supported (i.e., 1280x720p and 1920x1080p). The Makito X4 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.
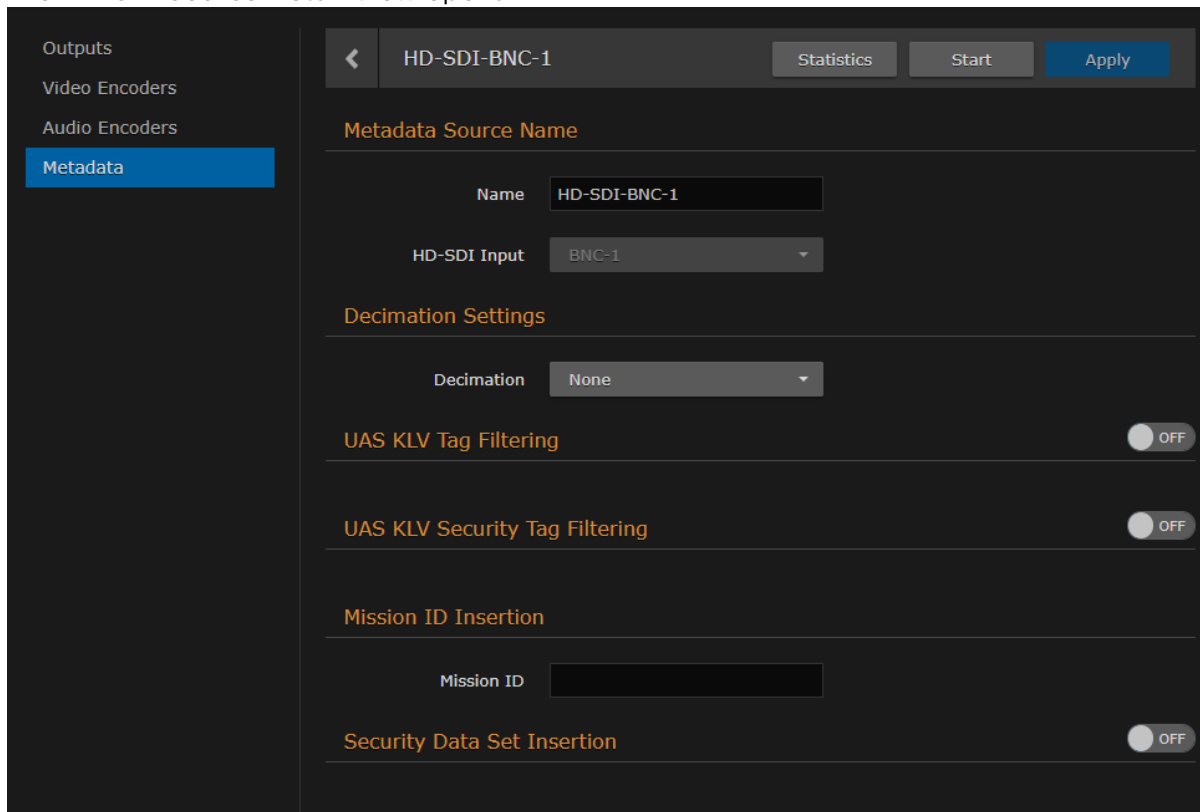
   or
2. To create an additional HD-SDI source, from the Metadata List View, click the ⊕ **Add** button.

3. On the New Metadata Source dialog, select HD-SDI for the Metadata Type and click **Continue**.
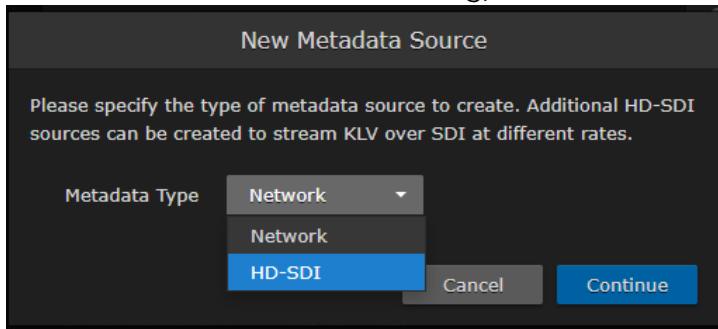
The Create New Metadata Source page opens.
4. Type in the Name for the source.

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 UAS KLV Tag Filtering.

Mission ID/Security Data Set Insertion:
8. To configure a mission ID or security data to replace or insert, see Mission ID/Security Data Set 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 X4 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 X4 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 the ⊕ **Add** button.
2. On the New Metadata Source dialog, select Network for the Metadata Type and click **Continue**.
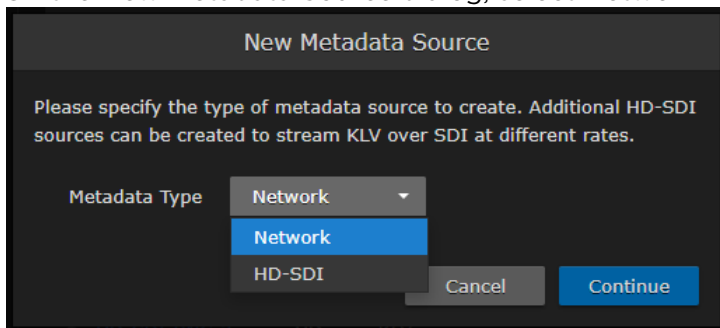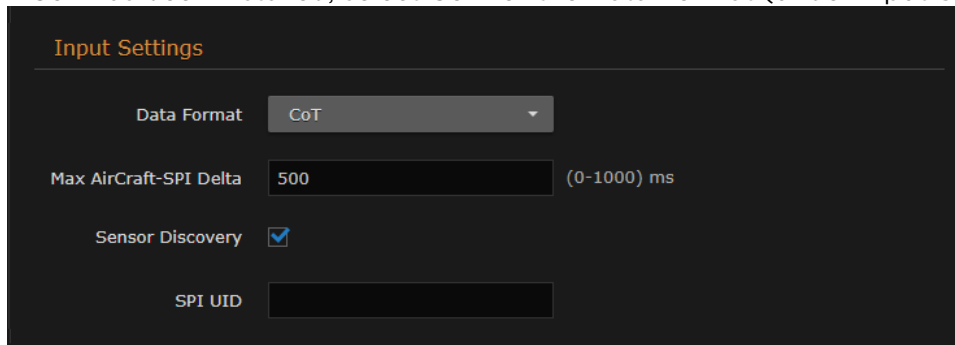
3. On the Create New Metadata Source page, type in the Name for the source.
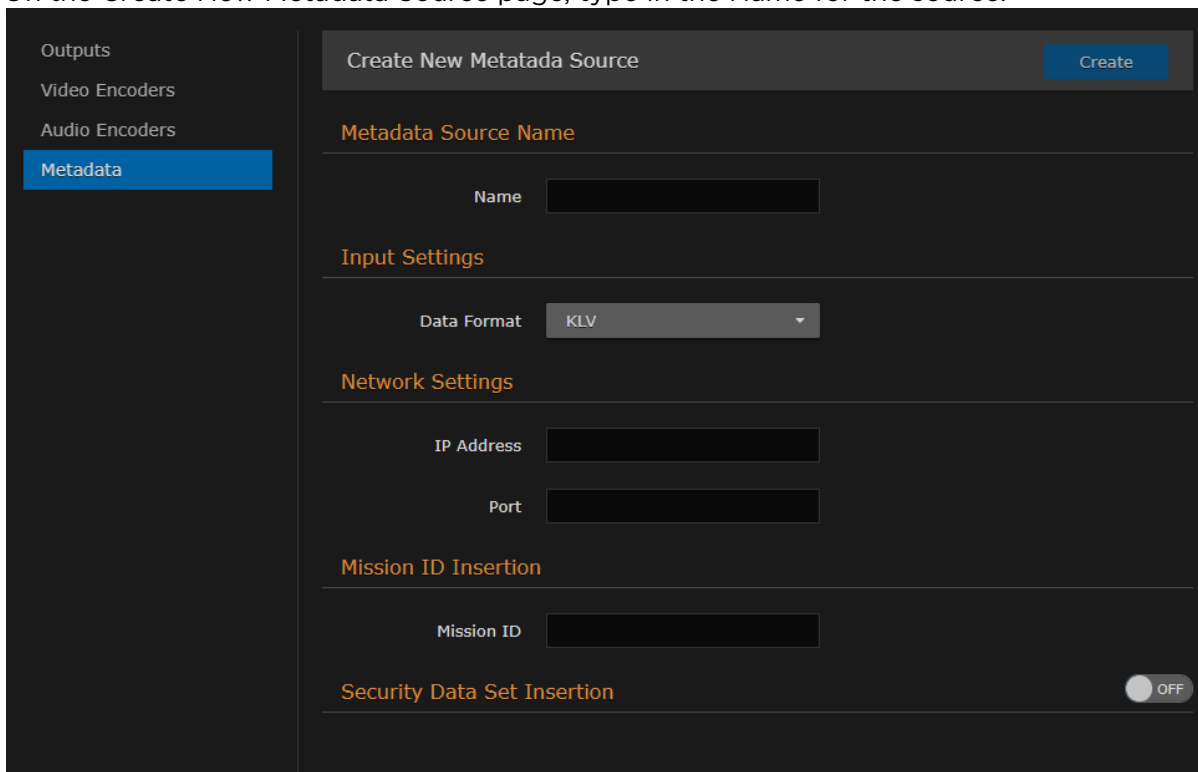
Input and Serial Settings

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.

CoT Relaying

6. (Optional) To set up CoT retransmission, see CoT Relaying.

Mission ID/Security Data Set Insertion

7. (Optional) To configure a mission ID or security data to replace or insert, see Mission ID/Security Data Set 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)

Configuring Serial Metadata Sources

> **ℹ Note**
>
> The Makito X4 Rugged automatically creates the Serial metadata source if the COM Port Mode is set to Metadata.

You can configure the Makito X4 Rugged 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.
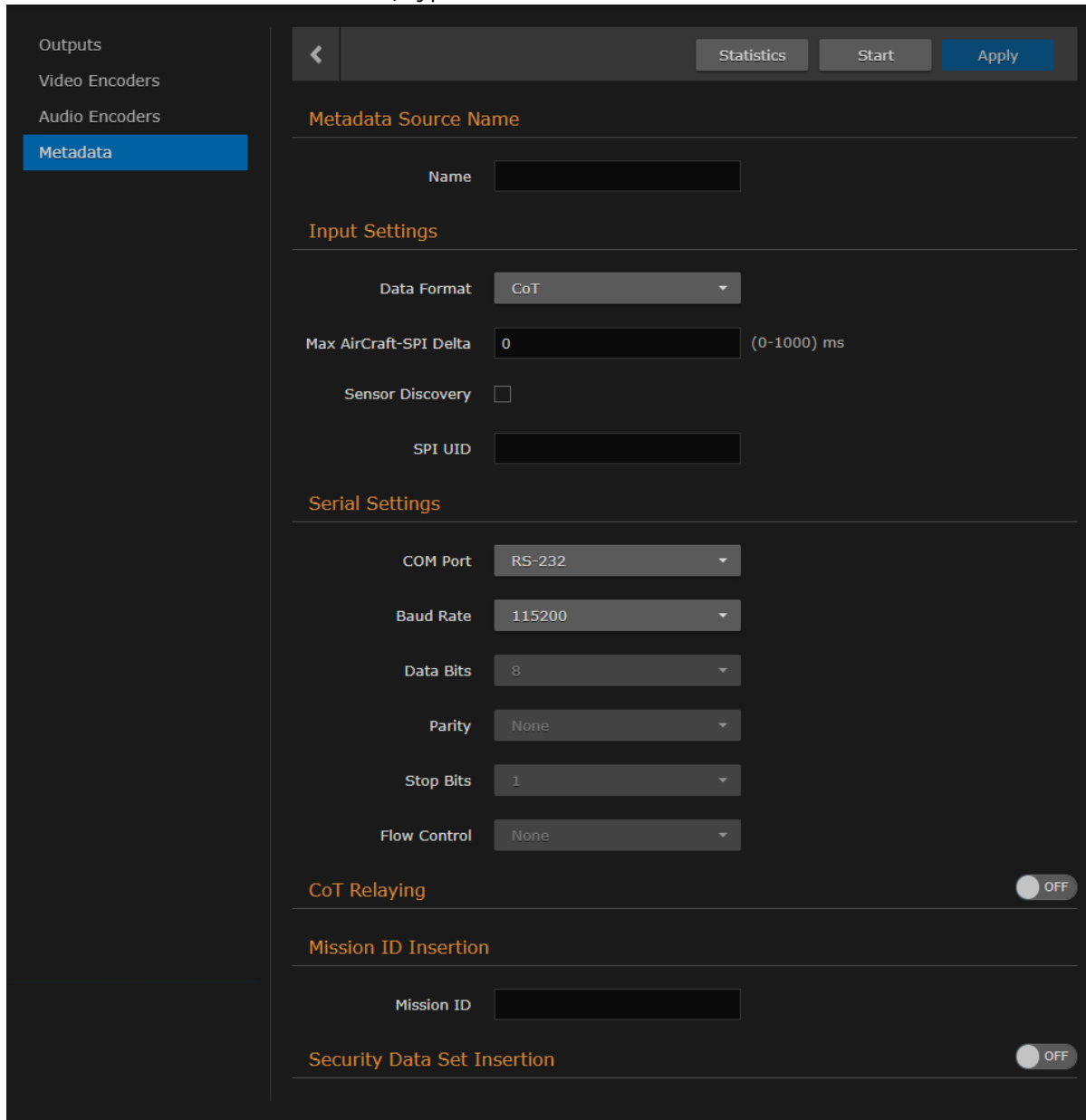
Input and Serial Settings
3. If CoT has been installed, select CoT for the Data Format (under Input Settings).
4. Select or enter the remaining value(s). For details on the Metadata fields, see **Metadata Settings**.
CoT Relaying
5. (Optional) To set up CoT retransmission, see **CoT Relaying**.
Mission ID/Security Data Set Insertion
6. (Optional) To configure a mission ID or security data to replace or insert, see **Mission ID/Security Data Set 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)

Metadata Settings

The following table lists the encoder Metadata controls and settings:

HD-SDI Sources   Network Sources   Serial Sources (Rugged Encoder only)

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	(From the List View) Select the Input port for the metadata source. • BNC-1 • BNC-2 • BNC-3 • BNC-4
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` > ℹ️ **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.
UAS KLV Tag Filtering (See UAS KLV Tag Filtering)		
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 Mission ID/Security Data Set 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 Classificatio n	uncla ssifie d	Specifies the classification of the security data set. Select either: • `unclassified, restricted, confidential, secret, topsecret`
Country Coding Method	ISO 3166-1 alph a-3	Specifies the use of 3-letter country codes.
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.

HD-SDI Sources   **Network Sources**   Serial Sources (Rugged Encoder only)

Network Sources

Metadata Setting	Defa ult	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)
Max AirCraft-SPI Delta	0 ms	ℹ️ **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 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 CoT Relaying 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) ℹ️ **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 Mission ID/Security Data Set 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. Select either: • `unclassified, restricted, confidential, secret, topsecret`
Country Coding Method	ISO 3166-1 alpha-3	Specifies the use of 3-letter country codes.
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.

HD-SDI Sources   Network Sources   **Serial Sources (Rugged Encoder only)**

Serial Sources (Rugged Encoder only)

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)
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 (See 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 **CoT Relaying** 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 Mission ID/Security Data Set 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. Select either: • `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.

Related Topics

- **ISR Metadata (Optional)** (in **Technical Specifications**)

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.
KLV Bitrate	The bitrate used for the metadata source (in kbps).
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.

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)

CoT Relaying

From the Metadata Detail View, you can configure retransmission of COT metadata received over the UDP or Serial (Makito X4 Rugged only) 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 Outputs**.
2. On the Metadata Detail View, if necessary, scroll down the page and toggle the CoT Relaying button to **On**.
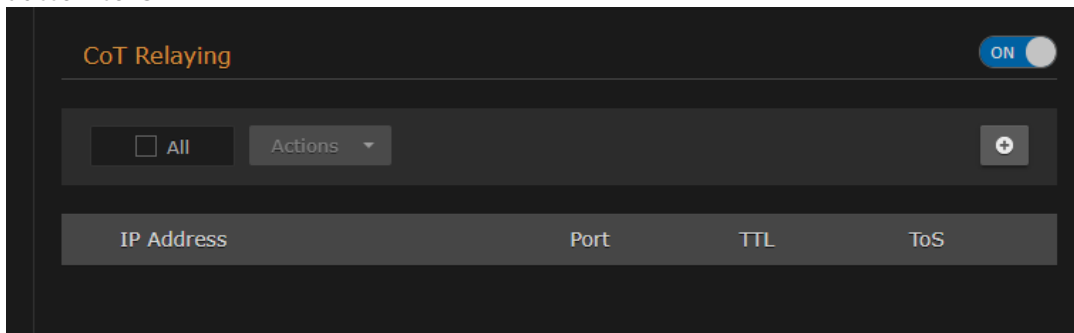
3. To add a CoT retransmission destination, click **+Relay**.
4. On the Add CoT Relay dialog, enter the IP Address and Port for the destination. Adjust the TTL and TOS values if required.
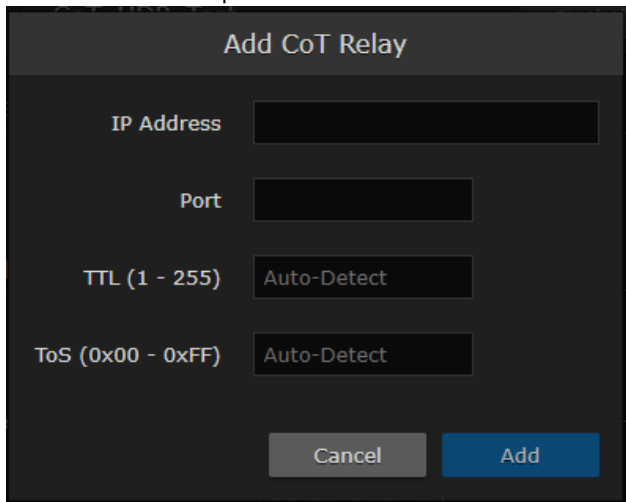
5. Click **Add**.
   The stream is added to the list:
6. To edit or delete a CoT relay destination, select the relay from the list and select **Edit** or **Delete** from the Actions drop-down menu.

Related Topics

- **Metadata Settings**
- **metadata** (CLI Command)

UAS KLV 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.

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.
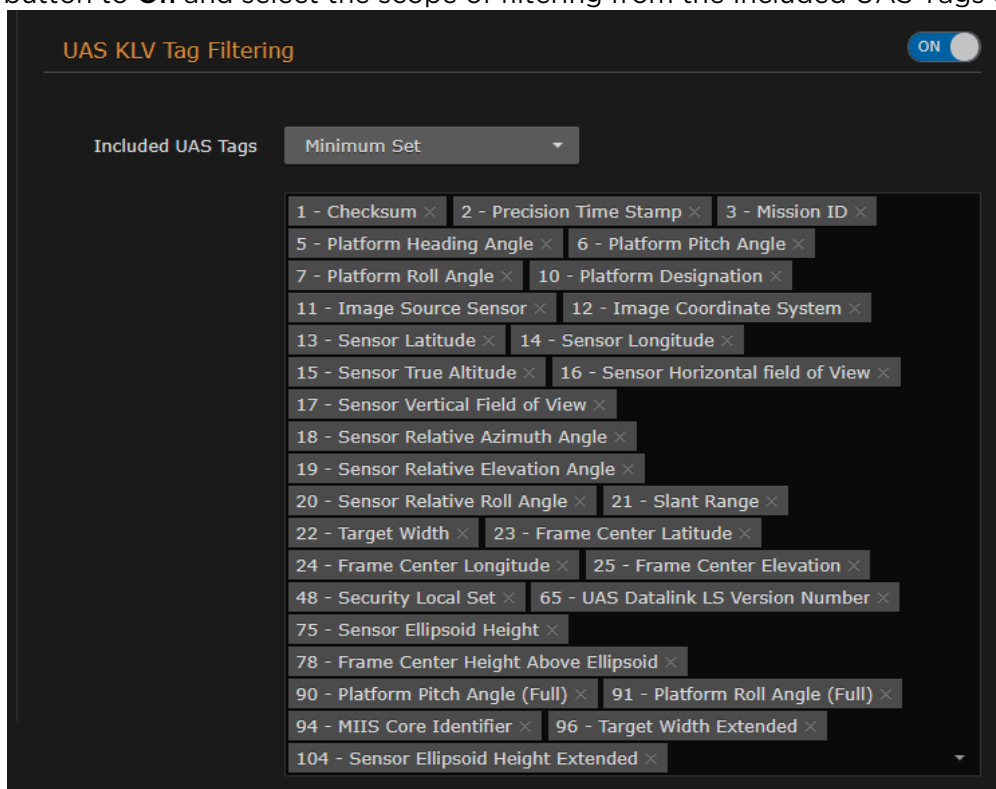
- To fine-tune the list on a per tag basis, as you browse through the list, click **X** next to a tag number/label to exclude the tag, i.e., filter it out of the metadata. This creates a new option "Custom Set" on the Included UAS Tags drop-down list.
-

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

(Optional) To filter the security metadata tags defined in MISB 0102:

1. On the Metadata Detail View, toggle the UAS KLV Security Tag Filtering button to **On** and select the scope of filtering from the Included Security Tags drop-down list.
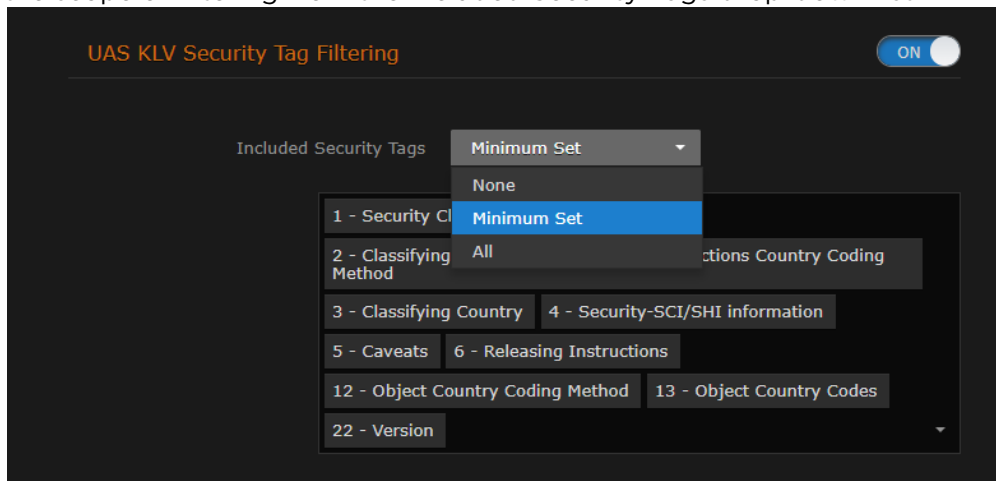
2. Fill in the remaining Metadata Detail fields and click **Apply**.

Related Topics

- **Metadata Settings**
- **metadata** (CLI Command)

Mission ID/Security Data Set 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. The following options are available:

- **Mission ID Insertion:** 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.
- **Security Data Set Insertion:** 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).
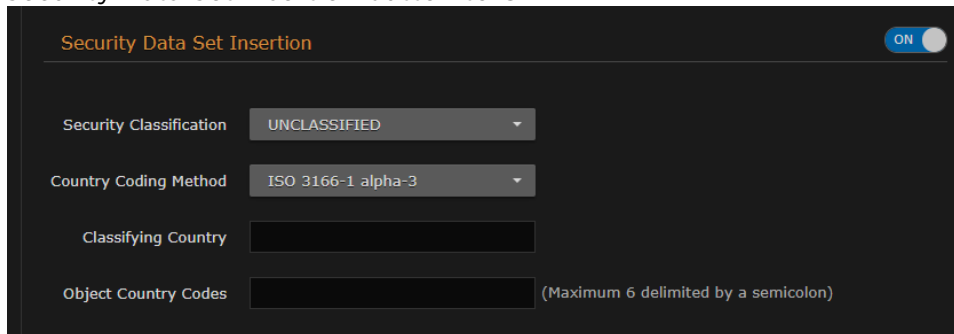
In both cases, the mission ID or security data will get replaced or inserted with the ones created by the Makito X4 based on the configuration.

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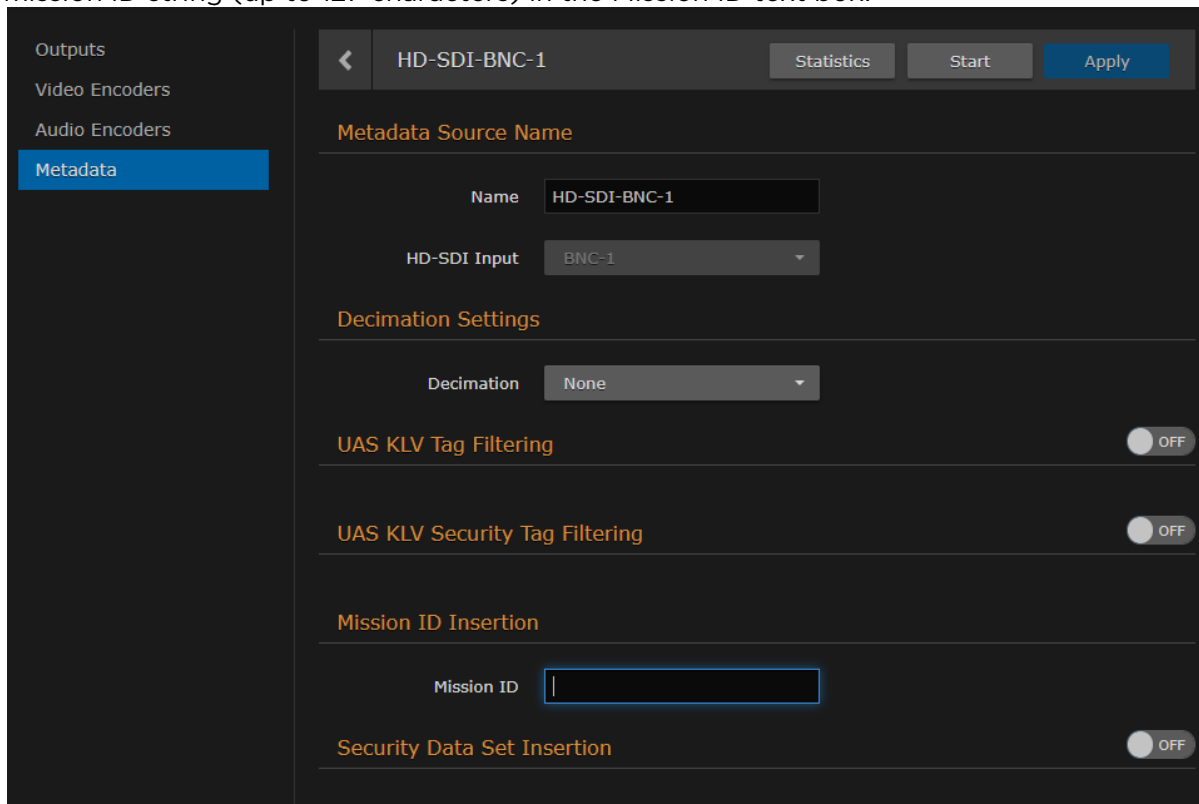
3. (Optional) To enable the update/generation of the security data set in UAS messages, toggle the Security Data Set Insertion button to **On**.

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

Related Topics

- **Metadata Settings**
- **metadata** (CLI Command)

Configuring Streaming Outputs

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**

Outputs List View

To open the Outputs List View:

1. On the Streaming page, click **Outputs** on the sidebar.
   The Outputs List View opens, displaying the list of defined streams for the encoder.
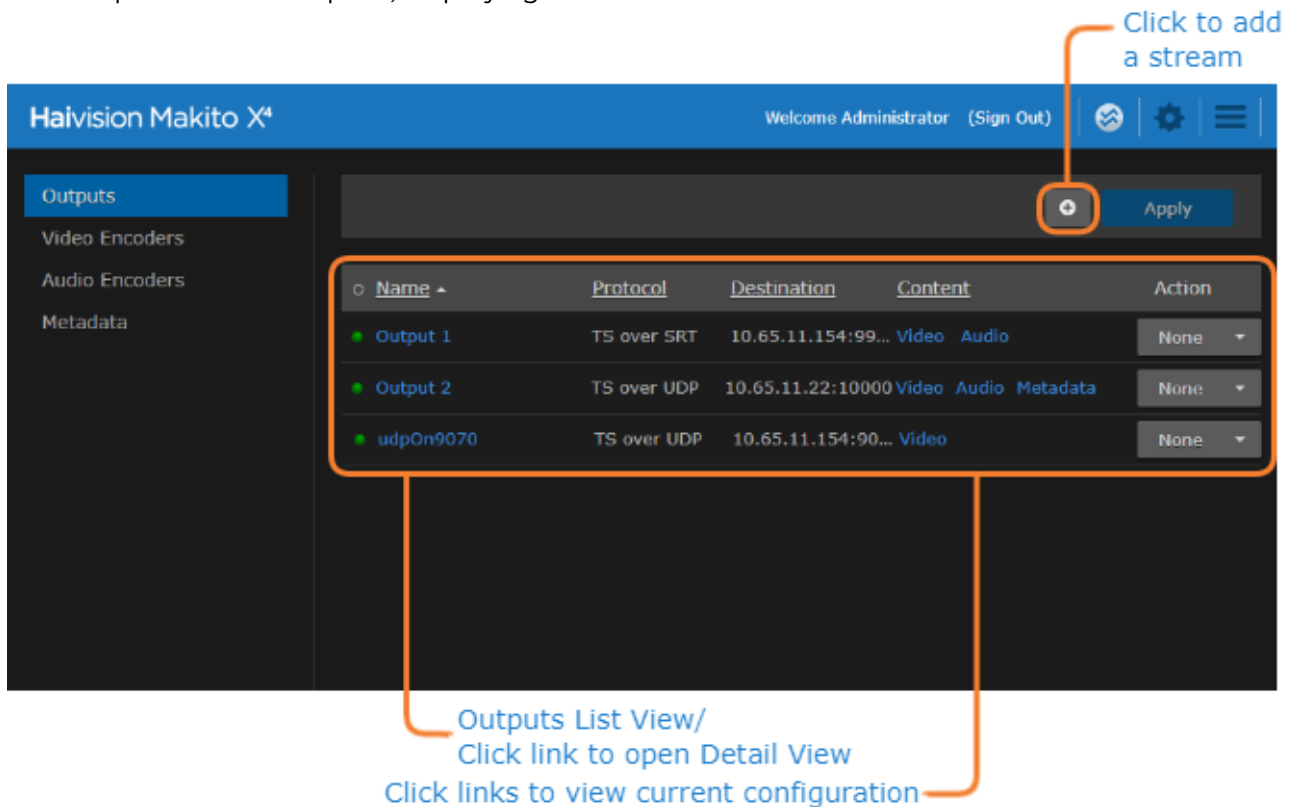
The Outputs List View displays the status LED, Stream Name, Protocol, Destination (IP Address and Port), and selected Content (Video/Audio Encoders and Metadata source) for each stream.

2. From here, you can perform the following tasks:
   - To create an output stream, click the ⊕ **Add** button.
   - To view details or modify the settings for a stream, 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, hover over the status LED (to the left of the row).

- To change the status for an existing stream, click the drop-down list under **Action** and select either Start or Stop (as applicable), or Delete.
- 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.
3. To apply your changes, click **Apply**.

Setting Up Streaming Outputs

From the Outputs Detail View, you can create and configure streams, start and stop streaming, and display statistics for streams. When creating a stream, you begin by selecting the content sources and then configure broadcasting, destination, link, and other streaming parameters.

To configure Output Steaming parameters:

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

The Outputs Detail View opens.

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 the ➕ **Add** button next to the Audio field and select the next Audio Encoder to add to the stream.
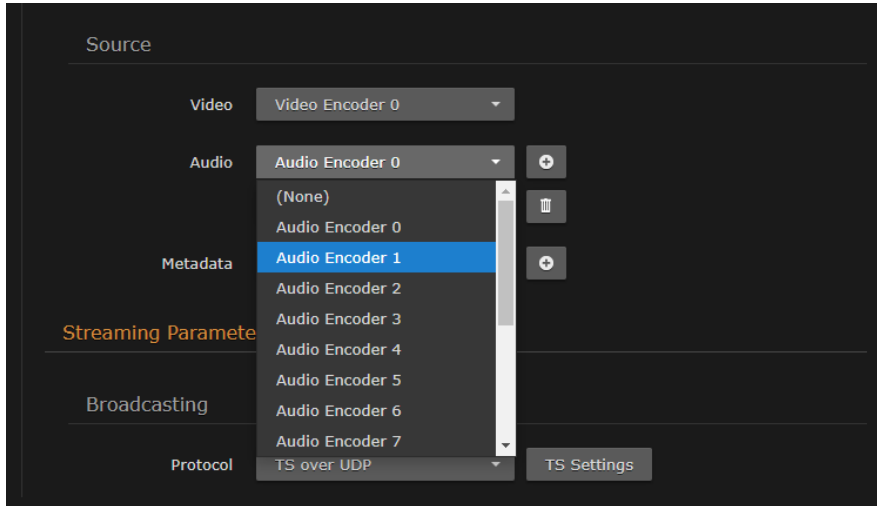
> ❗ **Important**
>
> Audio sources should always be associated with the same video interface for the dual channel SDI encoder. Selecting Analog or SDI audio sources that do not originate from the same video source is not recommended as audio artifacts will result at the decoder. For example, selecting 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).
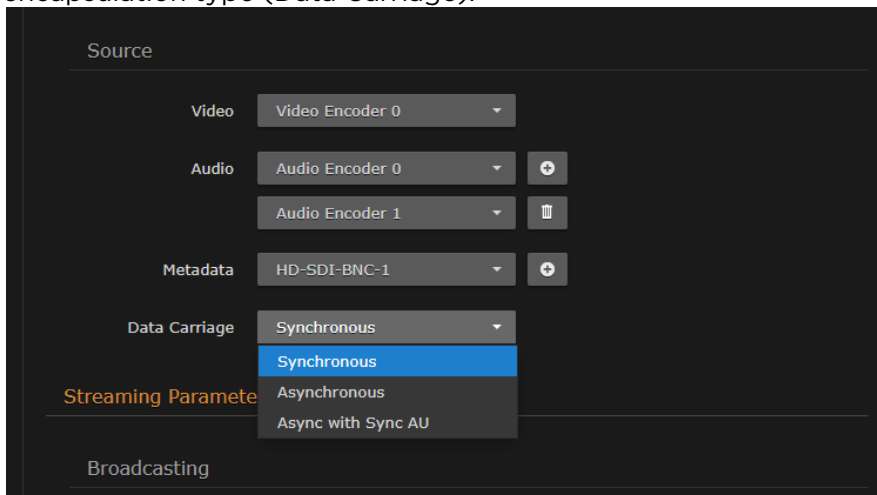
5. To stream metadata from multiple sources, click the ➕ **Add** button next to the Metadata field and select the next metadata source to add to the stream.
6. Under Broadcasting, select the Protocol.

7. To configure the Transport Stream settings (for TS over UDP, RTP, or SRT), click **TS Settings** and enter the values.
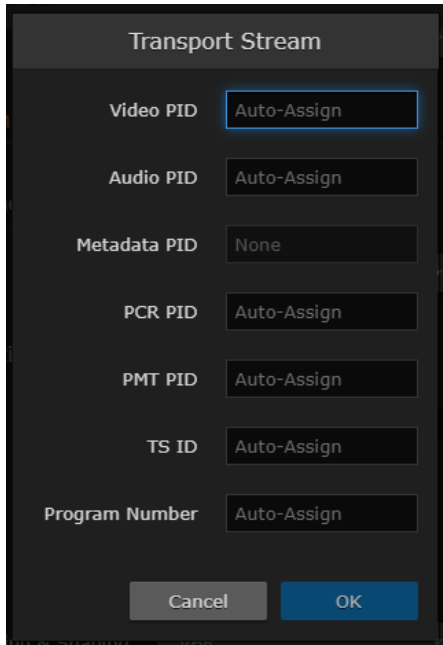
8.
> ⊕ **Important**
>
> The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network.

9. 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)**.

10. To configure SAP network announcements, check the "Transmit SAP" checkbox and fill in the SAP fields. For details, see **Session Announcement Protocol (SAP)**.
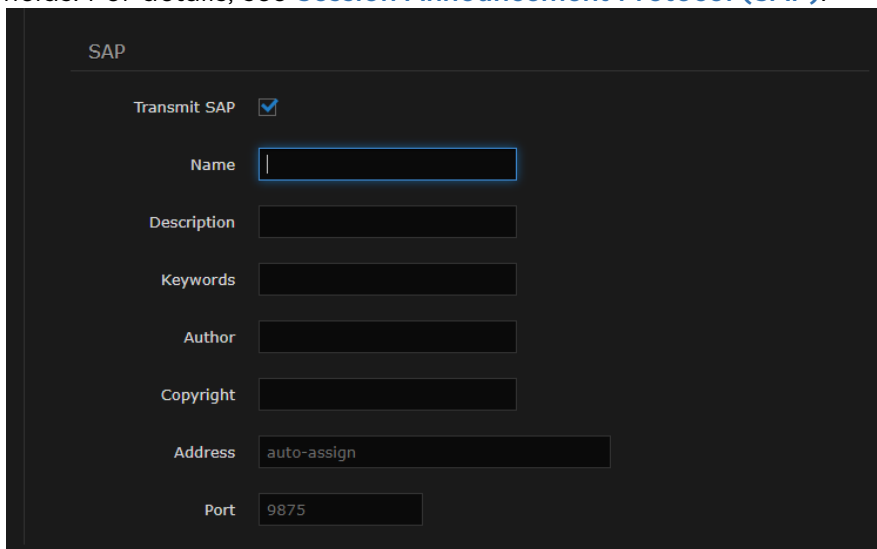
11. Click **Apply** to apply your changes and start streaming.

12. To start or stop streaming, click **Start** or **Stop** (as applicable).
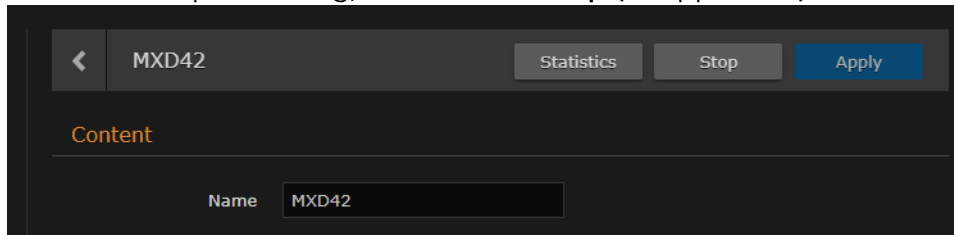
13. To view streaming statistics, click **Statistics**. For details, see Output Statistics.
14. To return to List View, click **Outputs** on the sidebar.

Related Topics

- Output Settings
- stream (CLI Command)

Setting Up a Second Stream

To create a second stream:

1. On the Outputs List View, click the ✚ **Add** button again.
2. Follow the steps in **Setting Up Streaming Outputs** 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).
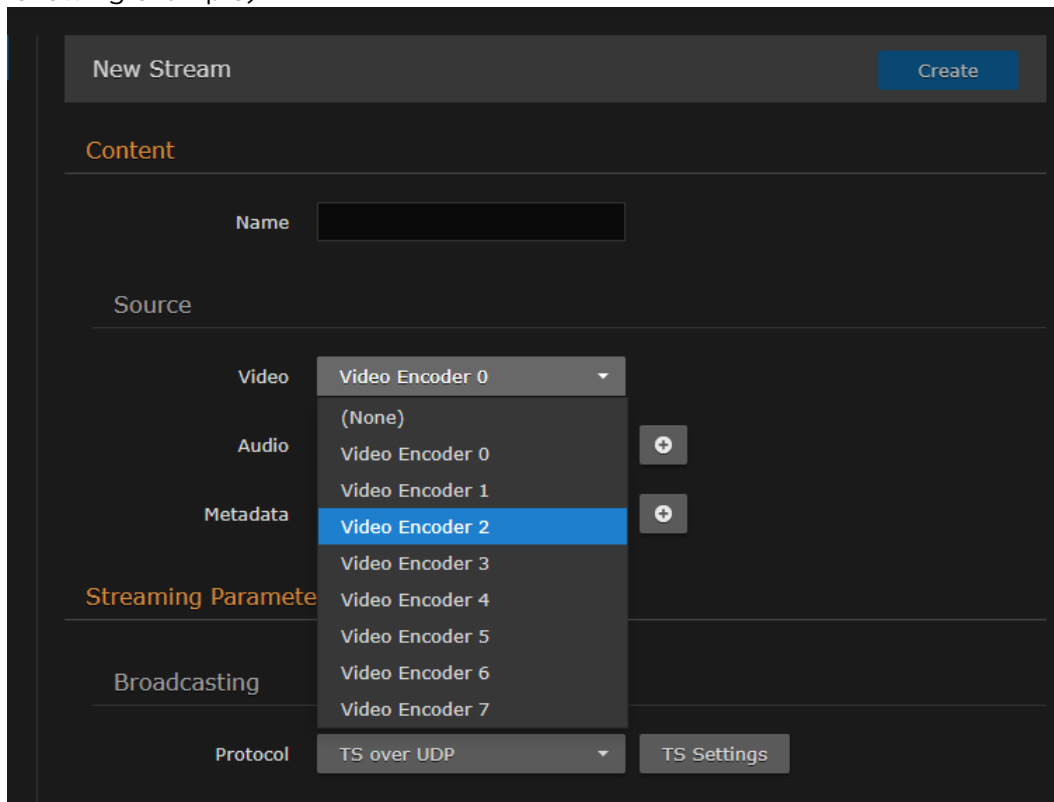
3. Also, under Streaming Parameters Destination, use a different Port number, for example, `2400`.
4. Click **Apply** to start streaming.

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 **Output Settings**
- **session** (CLI command)

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.
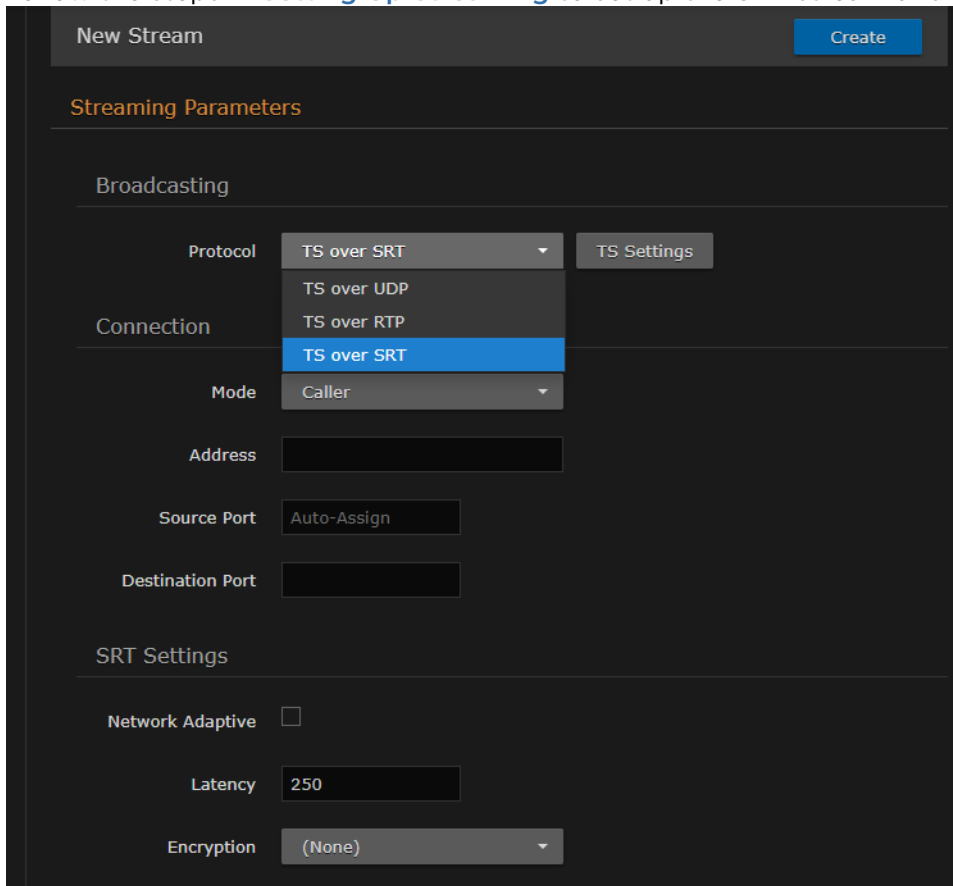
3. Once you establish the SRT stream, check the statistics and make adjustments to fine-tune the stream. On the Output Streams page, click the **Statistics** button to see how the SRT stream is performing.
4. Monitor the link statistics to see if the link is over-subscribed (and adjust the video encoder 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 Settings" in **Output Settings**

- For SRT-specific statistics and graphical display, see **Output Statistics**

Output Settings

The following table lists the Streaming Output controls and settings:

Content   **Streaming Parameters**   **SRT Settings**   **SAP**   **General**

Content

Streaming Setting	Default	Description/Values
Name	n/a	(Optional) Enter a unique name for the stream.
Source		
Video	Video Encoder 0	Select the Video Encoder to assign to the stream: • None (no content source selected) • Video Encoder 0 . . 7
Audio	Audio Encoder 0	Select the Audio Encoder to assign to the stream. • None (no content source selected) • Audio Encoder 0 . . 15 ℹ **Note** To configure multi-track audio, click the ➕ button 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., HD-SDI-BNC-1, HD-SDI-BNC-2, HD-SDI-BNC-3, or HD-SDI-BNC-4 ℹ **Note** To stream metadata from multiple sources, click the ➕ button 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**   **SRT Settings**   **SAP**   **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).
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`).
Port	n/a	Enter the destination UDP port(s). Enter a number in the range 1025..65,535. Note that RTP streams use even numbers only within this range.
Link Parameters		
Average Bandwidth	n/a	(Read-only) The average transmit bandwidth for the unit in kbps.

Timing & Shaping	VBR	Controls the timing characteristics of packets transmitted on the network (See Note below). Select either: • VBR (Variable Bitrate): The stream is not controlled and packets are transmitted as they become available. • CVBR (Capped Variable Bitrate): The maximum stream bitrate transmitted is limited by the Bandwidth Overhead parameter. • CBR (Constant Bitrate): The stream bitrate, packet timing, and audio/video timing comply with MPEG-2 TS CBR definition. The maximum stream bitrate transmitted is limited by the Bandwidth Overhead parameter. If no data is available, idle cells may be inserted.
Bandwidth Overhead (%)	15%	(Timing & Shaping must be CVBR or CBR) Specifies the percentage of network bandwidth beyond the average rate that the encoder is allowed to use if needed. ℹ️ **Note** To configure the Bandwidth Overhead for CBR streams with metadata, see **Bandwidth Overhead for CBR Streams with Metadata**.
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	128 or 0x80 (CS4)	(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) ℹ️ **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). ℹ️ **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.

ℹ️ **Note**

Timing & Shaping settings combine and replace the Traffic Shaping, Idle Cells and Delayed Audio parameters from the Makito X:
• VBR: Shaping=Off, Idle Cells=Off, Delayed Audio=Off
• CVBR: Shaping=On, Idle Cells=Off, Delayed Audio=Off
• CBR: Shaping=On, Idle Cells=On, Delayed Audio=On

Content   **Streaming Parameters**   **SRT Settings**   **SAP**   **General**

SRT Settings

Streaming Setting	Default	Description
Connection		

Mode	Caller	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.
		• ℹ️ **Note**
		
		    The firewall must be configured to allow incoming Caller connections to reach the Listening device.
		
		• ℹ️ **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	n/a	✅ **Tip** You can also enter a Fully Qualified Domain Name (FQDN).
Source Port	n/a	ℹ️ **Note** This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.

Destination Port	n/a	(Caller and Rendezvous modes) Specifies the UDP destination port for the SRT stream.
Port	n/a	(Listener mode only) Specifies the UDP local port for the SRT stream.
SRT		
Network Adaptive	Disabled	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.
(Buffering) Latency	250 ms	Specifies the SRT receiver buffer that permits lost packet recovery. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20 - 8000 ms ℹ️ **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	None	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) Specifies a string used to generate the encryption keys to protect the stream. Range = 10-79 UTF8 characters
Bandwidth Overhead (%)	25 %	Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-50% ℹ️ **Note** SRT streams may temporarily overshoot the defined bandwidth overhead limit.

Content   **Streaming Parameters**   **SRT Settings**   **SAP**   **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.

Streaming Setting	Default	Description/Values
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   SRT Settings   SAP   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.
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.

Related Topics

- Network and Management Interfaces (in Technical Specifications)

Output Statistics

The following table lists the Streaming Output statistics:

Output   SRT

Output

Output Statistic	Description/Values
State	The current operating status of the stream, either: • STREAMING • CONNECTING • STOPPED
Up Time	(only available when State is STREAMING) The length of time the stream is actively streaming (e.g., 1d22h5m41s).
Source Port	The UDP source port for an SRT stream, i.e., the port from which the encoder is sending the SRT stream.
Sent Packets	Number of RTP or UDP packets sent for that stream.
Sent Bytes	Number of Bytes sent for that stream.
Bitrate	The stream bitrate (in kbps).
Reset	Click to reset the Output statistics.

Output   **SRT**

SRT

SRT 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).
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.

SRT 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.
MTU	(Maximum Transmission Unit) The maximum allowed size of IP packets for the outgoing RTP data stream.
RTT	Measured Round Trip Time.
Local Buffer Level	✅ **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:

Stream 3	Reset

Statistics

Output

State	STREAMING
Up Time	7h7m26s
Source Port	48268
Sent Packets	16,861,499
Sent Bytes	20,901,480,408
Bitrate	6,087 kbps

SRT

Peer Version	1.3.1
Reconnections	1
AES Encryption	Off
Resent Packets	0
Resent Bytes	0
Dropped Packets	0
Dropped Bytes	0
Received ACKs	1,645,245
Received NAKs	0
Max Bandwidth	8,828 kbps
Path Max Bandwidth	148,714 kbps
RTT	< 1 ms
Local Buffer Level	132
Latency	250

SRT   Last 5 Minutes ▼   Download CSV File

Delays (msec)

☑ Send Buffer   ☑ Round Trip   ☑ Latency

Bandwidth Used (kbps)

☑ Send Rate   ☐ Link Bandwidth   ☑ Retransmit Rate

> ℹ **Note**
>
> The Link Bandwidth is an estimate of the actual link bandwidth.

System Administration

> **ℹ Note**
>
> Unless otherwise indicated, the Administration Settings pages are only accessible to administrators. The exceptions are as follows:
> - Status is accessible to all users.
> - Presets is accessible to Operators as well as Administrators.

Topics in This Chapter

- **Viewing System Status Information**
- **Saving and Loading Presets**
- **Installing Firmware Updates**
- **Configuring Network Settings**
- **Configuring Date and Time**
- **Enabling and Disabling Network Services**
- **Managing Licenses**
- **Managing the COM Port**

Viewing System Status Information

From the Status page, you can view status information about the Makito X4, 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.
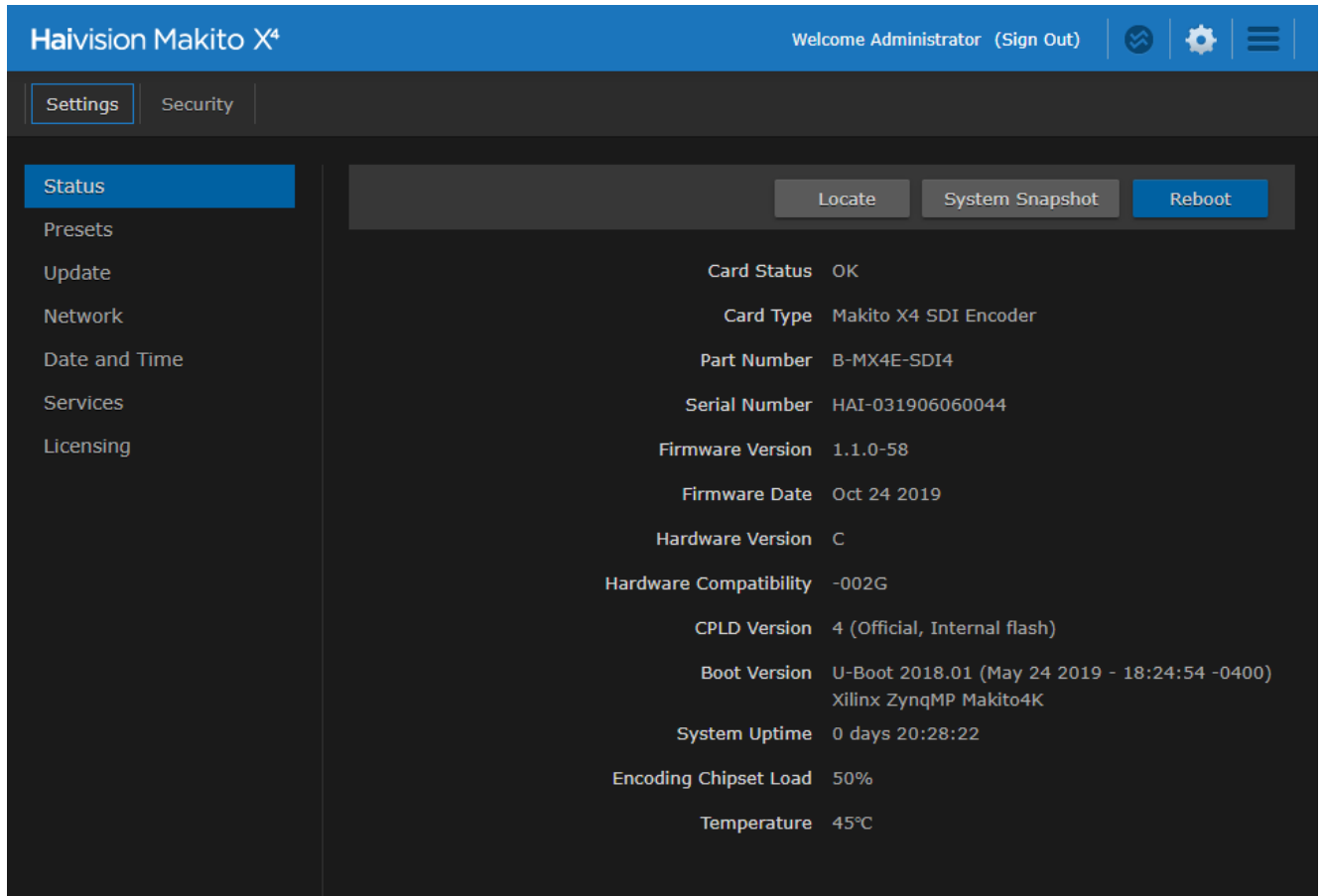
The Status settings are read-only. For details, see **Status Settings**.

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**.
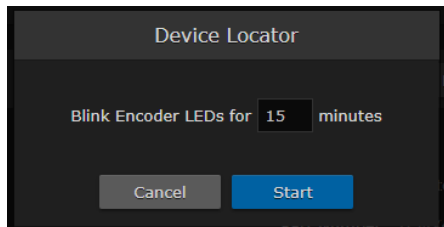
> ℹ️ **Note**
>
> The blinking can last from 1 minute to 1 hour; the default is 15 minutes.
> The Locate feature is not available on the Makito X4 Rugged.

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
Personality	Select between SDI, SQD (version 1.6 and later), DEFENSE (version 1.7 and later) and SMPTE 2110 (version 1.4 and later). This setting will take effect upon the next reboot.
Card Status	OK (or error message if applicable).
Card Type	The type of device, e.g., Makito X4 SDI Encoder.
Part Number	The Haivision part number for the encoder or decoder, e.g., B-MX4E-SDI4 or S-MX4D-SDI.
Serial Number	The serial number for this appliance or card.
Firmware Version	The firmware version of the device, e.g., 1.0.0-23.
Firmware Date	The firmware release date.
Hardware Version	The hardware version of the device.
Hardware Compatibility	-001G or -002G (basic card assembly).
Carrier Type	(Makito X4 Rugged Encoder only) The interface carrier board. ⚠ **Note** In Release 1.2, the number of CVBS inputs supported depends on the Carrier Type. ″**Makito 4KR**″ indicates the three-input variant, whereas ″**Makito 4KR 12G**″ indicates the four-input variant.
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., 4 days 17:42:03).
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**.

> ✅ **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=511(haiadmin),510(haisecur),512(haioper)


--------------------------------------------------------------------------------
Local Time:
--------------------------------------------------------------------------------
Wed Mar 13 14:47:32 EDT 2019


--------------------------------------------------------------------------------
Universal Time:
--------------------------------------------------------------------------------
Wed Mar 13 18:47:32 UTC 2019


--------------------------------------------------------------------------------
System UP Time:
--------------------------------------------------------------------------------
 14:47:32 up 47 min,  0 users,  load average: 0.30, 0.17, 0.11


--------------------------------------------------------------------------------
Manufacturing Information:
--------------------------------------------------------------------------------
MAC Address   : 5c:77:57:00:b3:dc
Serial Number : HAI-031809050009
Boot Revision :


--------------------------------------------------------------------------------
Card Temperature:
--------------------------------------------------------------------------------
Temperature Status:
  Current Temperature : 51 Celsius measured 1s ago
  Maximum Temperature : 52 Celsius measured 37m36s ago
  Minimum Temperature : 50 Celsius measured 47m10s ago
Debug Statistics:
  Invalid Readings     : 0
  Discarded Deltas     : 0


--------------------------------------------------------------------------------
System Information:
--------------------------------------------------------------------------------
Card Type            : "Makito X4 SDI Encoder"
Part Number          : B-MX4E-SDI4
Serial Number        : HAI-031809050009
MAC Address          : 5c:77:57:00:b3:dc
Firmware Version      : 1.0.0-23
Firmware Date        : "Mar 14 2019"
Firmware Time        : "15:42:07"
Hardware Version     : A
Hardware Compatibility : -001G
CPLD Version         : 3 (Official, Internal flash)
Boot Version         : "U-Boot 2020.06 (Feb 26 2020 - 10:41:13)-Makito4K 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
+++-==============================-============-========================
```

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 Series device is configured by users' selecting and setting values of applicable encoder or decoder settings, such as Video and Audio Encoder, Streaming Output, and (if licensed) Metadata settings; or Decoder Output and Stream settings. 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.

The Preset Manager displays a list of saved presets. From here you can load, rename, duplicate, or delete a saved preset, as well as view the contents of a preset file and select a preset to load at startup.

> ℹ **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 X4 when the current configuration has not been saved in a preset.
>
>
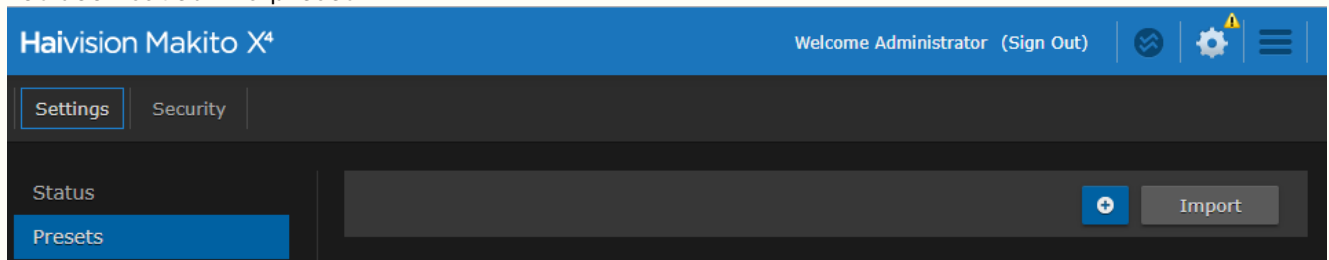
To view and manage presets:

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 green check mark.
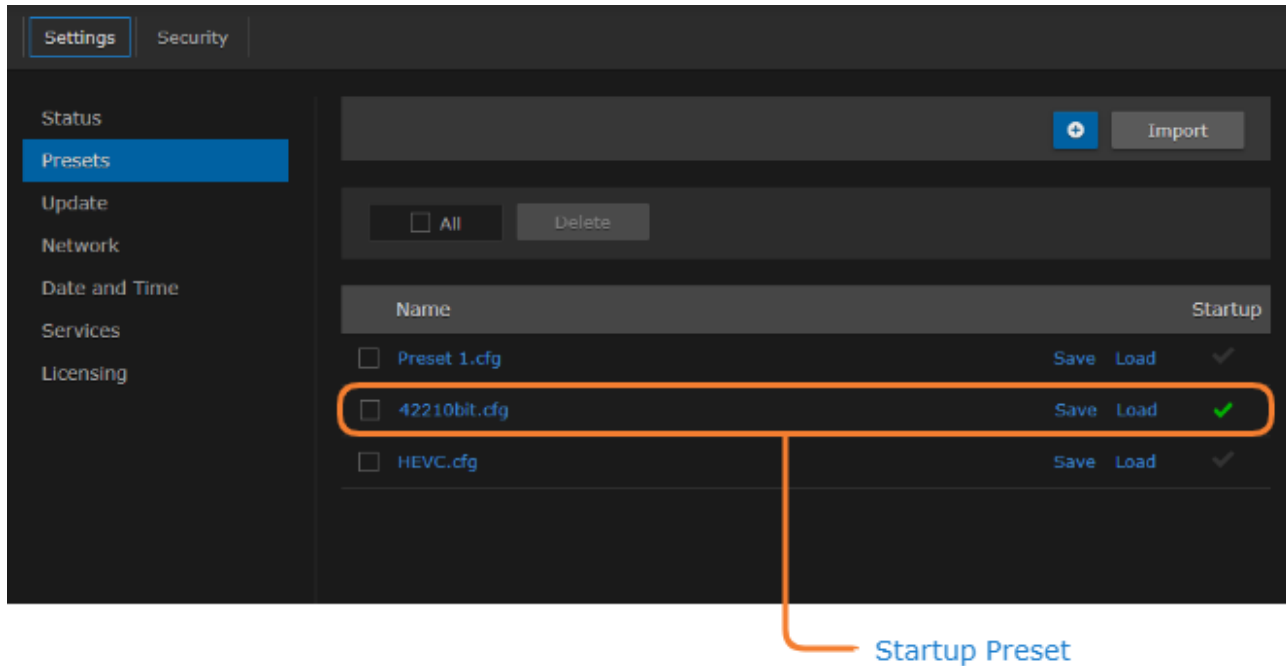
Startup Preset

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

4. To select an existing preset to load at startup, hover over the preset row and click the (grayed out) check mark under **Startup**.
5. To save the current settings as a new preset, click the **+** button.
   a. In the New Preset dialog, type a new filename in the Name text box.
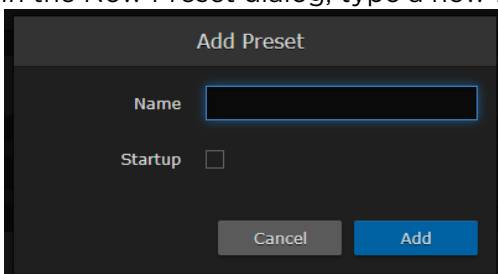
   b. To select this preset to load at startup, check the Startup checkbox.
   c. Click Create.
6. To save the current settings as an existing preset, hover over the preset row and click **Save**. You can (optionally) check the **Startup** check mark.

7. To save the preset as a text file to view or export to other Makito X4 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 X4 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**.
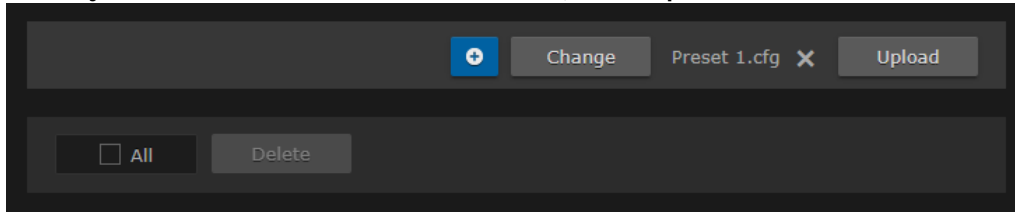
> ✅ **Tip**
>
> To select a different preset file, click Change. To remove the selection, click the ✖ icon.

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

Installing Firmware Updates

> ℹ️ **Note**
>
> Before you can install a firmware update on the Makito X4, you may need to obtain and install an updated license (depending on the version limit and expiration date of the currently installed license). For more information, see **Managing Licenses**.

When you first receive the Makito X Series appliance, the necessary firmware is pre-installed on it. Firmware updates and licenses 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 update becomes available, you can easily install it from the Web interface. You will first need to copy the update file to your local computer or network.

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

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

To install a firmware update:

1. On the Administration page, click **Settings** on the navigation bar and **Update** on the sidebar. The Update page opens.
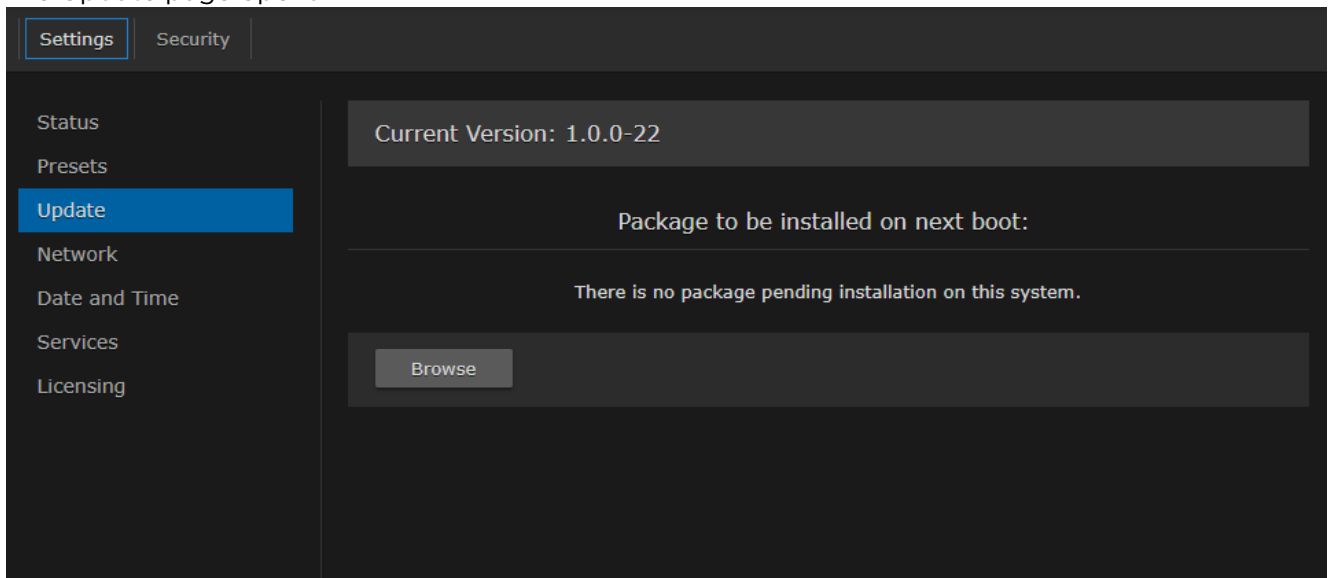
2. Click **Browse** and select the file in the Open File dialog box.

3. When you see the filename in the text box, click **Upload**.
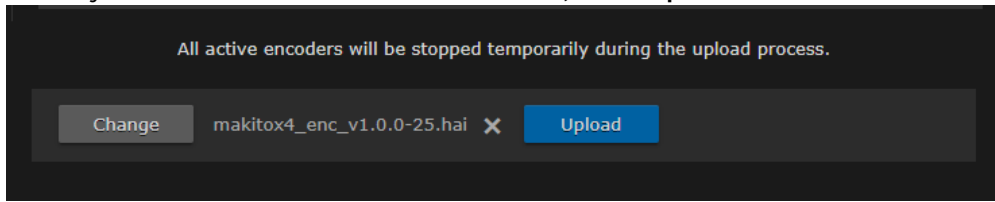
4. Wait for the file to be uploaded and verified and the file system synced.

> ❗ **Important**
>
> Remain on this page and do not click anything else in the Makito X4 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).
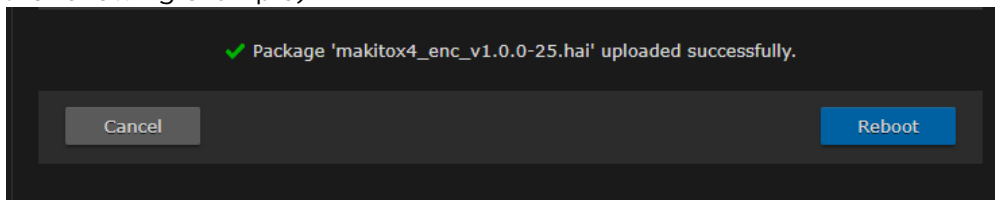
5. Click **Reboot**.
While the unit is rebooting, the Status LEDs will flash, and you will see a warning page (as shown following).
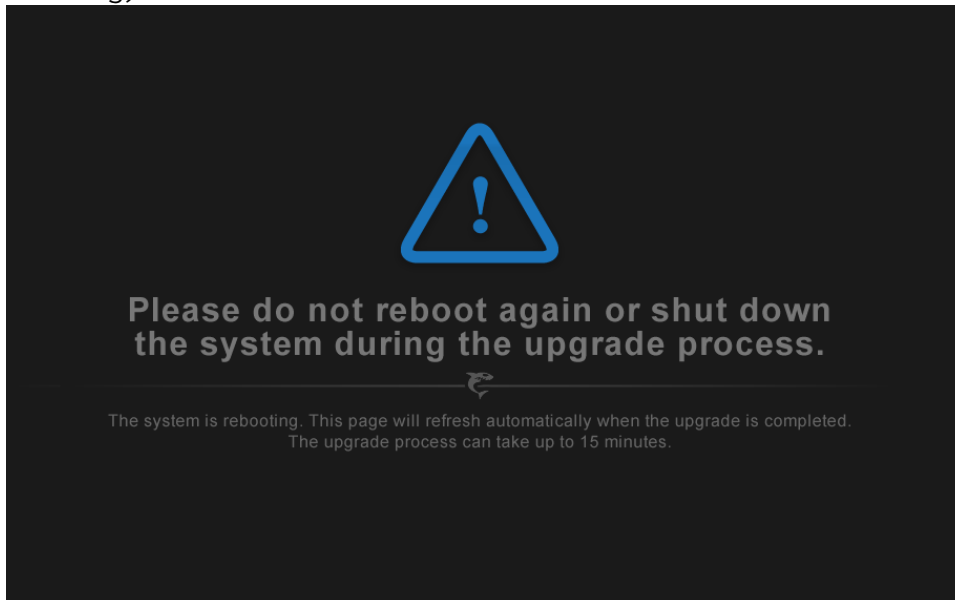
> ⚠️ **Caution**
>
> Do not proceed or shut down the system while the Status LEDs are still flashing. Failure to wait could result in damage to your system.

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

6. Clear your browser cache after the firmware upgrade.

7. 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. See **Managing Messages**.

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 encoder through an IPv4 connection, disabling the IPv4 interface will drop your connection after a reboot. You will need to reconnect using IPv6 or the serial interface (if available).

To view and configure the Network settings:

1. On the Administration page, click **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 IPv6 addressing, toggle the IPv6 button to **On** and select the Addressing option. Enter the new value(s) as required.
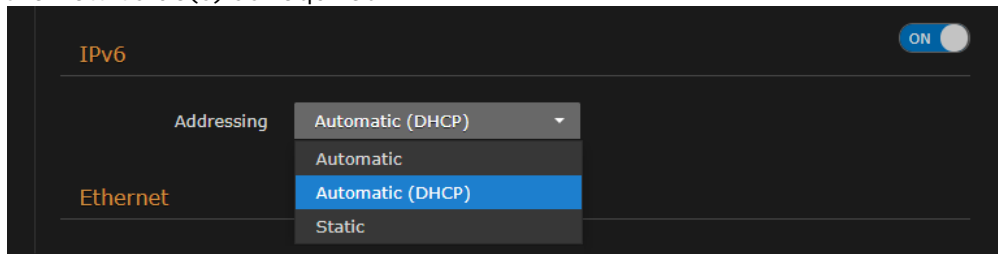
4. Click **Apply**.
5. Click **Reboot**.

> **ⓘ 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 address(es) obtained by the system.
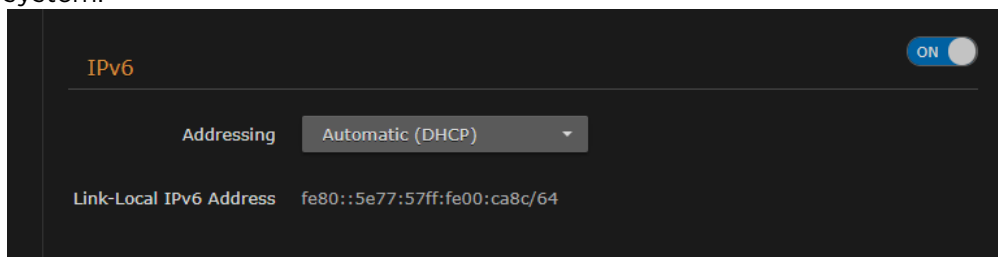
Network Settings

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

General

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

Interfaces

Network Setting	Description/Values
eth0 | eth1	(Encoder-only) Allows for multiple network interfaces. Select the appropriate tab to view and configure.

IPv4

Network 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 and 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 is "Haivision Makito X4 Encoder" or "Haivision Makito X4 Decoder" for the Makito X4 encoder or decoder, and "Haivision Makito X1 Encoder" the for Makito X1 encoder.
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.

IPv6

Network Setting	Description/Values
Addressing	Select one of the following options to obtain an IPv6 address for the unit: • Automatic: Uses SLAAC (Stateless Address Autoconfiguration) to obtain IP addresses automatically without the need for a DHCP server • Automatic (DHCP): Enables the Dynamic Host Configuration Protocol to get an IP address from a DHCP server on the network • Static: Use to manually configure the device's IP and gateway addresses.
Global IPv6 Address	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	(**Static** Addressing only) The Prefix Length in IPv6 is the equivalent of the Subnet Mask in IPv4. However, instead of being expressed in four octets as it is in IPv4, it is expressed as an integer between 1 through 128.
Gateway	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	(Read-only) A link-local address is an Internet Protocol (IP) unicast address intended to be used only to connect to the hosts on the same network. A link-local address starts with fe80: and is always automatically assigned.

Ethernet

Network 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-only	
Total TX Bandwidth (Limit)	(Encoder only) The maximum transmit bandwidth for the encoder in kbps. Specifies the bandwidth "ceiling" for the Ethernet port.

DNS Settings

Network 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.

Network Setting	Description/Values
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 X4. 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 X4. 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.
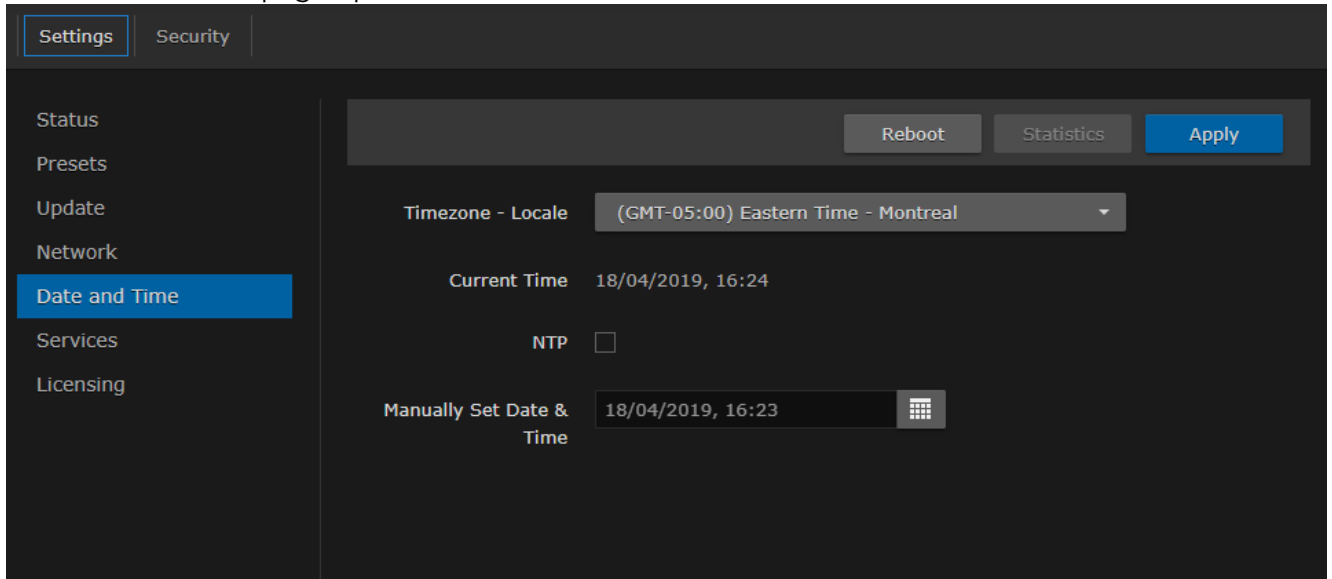
2. Select or enter the new value(s) in the appropriate field(s). For details, see Date and Time Settings.
3. To apply your changes, click **Apply**.
4. To validate that the NTP server is reachable, click **Test** (below the NTP server field).
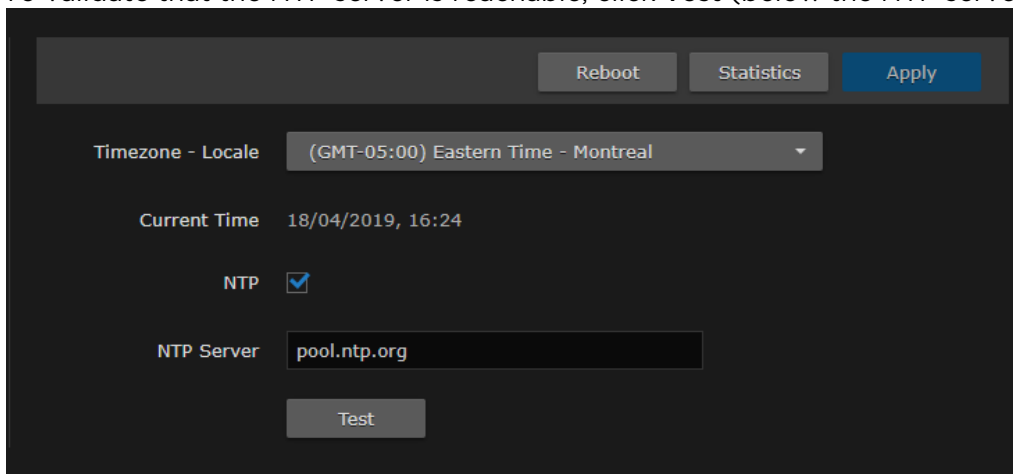
5. To view statistics for the NTP server, click **Statistics**. For details, see NTP Statistics.

Date and Time Settings

The following table lists the Date and Time settings:

Date and Time Setting	Description/Values
Timezone	
Time Zone	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.
Server	
Use NTP	Toggle on 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.
Reboot	If changes have been made to the date and time settings, click to apply changes.

Related Topics

- **NTP Statistics**

NTP Statistics

Following is an example of the NTP Statistics:

```
Statistics
  Tracking

Reference ID    : 00000000 ()
Stratum         : 0
Ref time (UTC)  : Thu Jan 01 00:00:00 1970
System time     : 0.000000011 seconds fast of NTP time
Last offset     : +0.000000000 seconds
RMS offset      : 0.000000000 seconds
Frequency       : 14.546 ppm fast
Residual freq   : +0.000 ppm
Skew            : 0.000 ppm
Root delay      : 1.000000000 seconds
Root dispersion : 1.000000000 seconds
Update interval : 0.0 seconds
Leap status     : Not synchronised

  Sources

210 Number of sources = 1
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? 10.65.154.200               0   10    0     -     +0ns[  +0ns] +/-    0ns

  Source Statistics

210 Number of sources = 1
Name/IP Address          NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
===============================================================================
10.65.154.200             0   0    0    +0.000     2000.000    +0ns  4000ms
```

Enabling and Disabling Network Services

For security purposes, an administrator may need to stop one or more network services from accessing the Makito X4. From the Services page, you can enable and disable network services, including HTTP, SSH, Telnet, SNMP, and Haivision EMS.On the Makito X4 Rugged, you can also enable bi-directional serial pass-through for controlling serially attached devices such as PTZ controlled cameras. Both RS-232 and RS422 are supported.

> **ⓘ 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.

> **⚠ Caution**
>
> Take care *not* to disable all network services; you must at least keep `http` (Web interface), `telnet`, or `ssh` active. Otherwise you will lose access control to the unit, and the only way to re-enable these services is by a Factory Reset (For details, see **Resetting the Encoder**).

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.
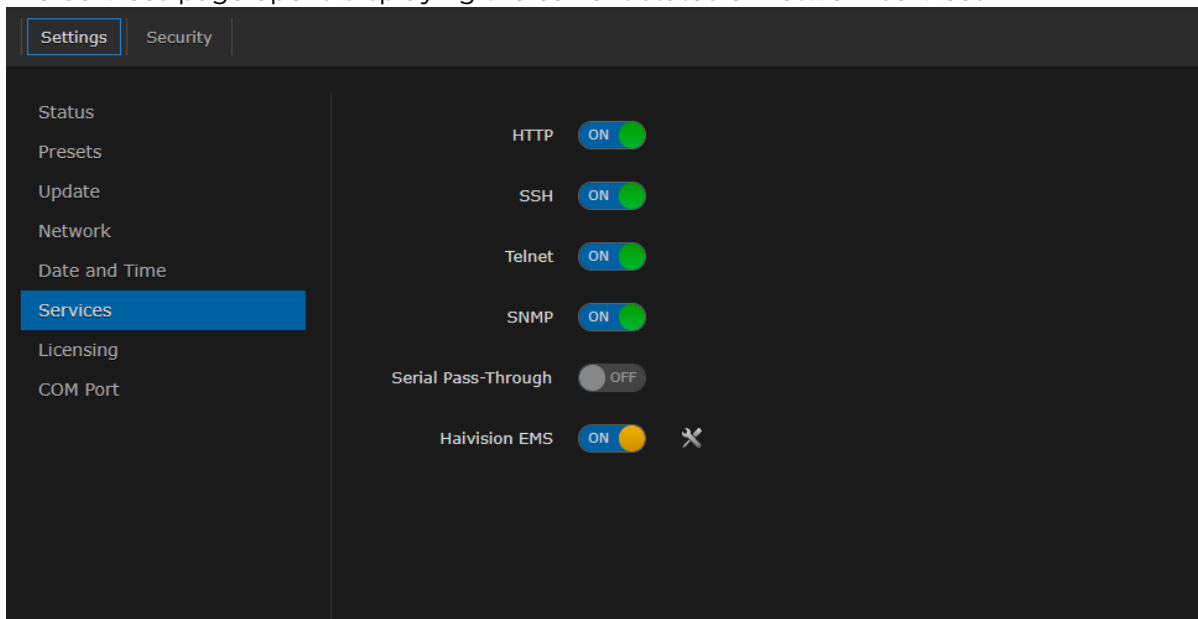
> ℹ **Note**
>
> The On-Off button color indicates the service status:
>
> | Color | Indication |
> |-------|------------|
> | Green | Service is operating. |
> | Red | Service is not operating correctly, for example, telnet daemon failed to start. |
> | Orange | Problems were encountered performing a service, for example, EMS failed to pair. |
> | Grey | Service is disabled. |

2. To enable or disable a service, toggle the associated Service button to **On** or **Off**. For details, see **Services Settings**.
3. To pair the encoder with Haivision-EMS, toggle the Haivision-EMS button to **On** and click **Configure**. See **Pairing the Encoder with Haivision EMS**.

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

> ✅ **Tip**
>
> Network services can also be enabled/disabled using the CLI **service** command.

Services 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.
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.
Product Analytics	Toggle **Enable Anonymous Product Analytics** on or off to enable or disable the collection of anonymous product analytics.
Thumbnail Preview	Preview Thumbnails provide a visual reference of each video encoder's input. By default, previews are enabled and set to 10 second intervals.

Encoder-only

Service	Description/Values
Serial Pass-Through	(Makito X Series Rugged Encoders only) 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.
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 .

Related Topics

- **Managing Certificates** (to manage HTTP TLS certificates)

Pairing the Encoder with Haivision EMS

Haivision EMS (Element Management System) allows simple management of Haivision-only devices. To get started, you enable the EMS service on the Makito X Encoder and then pair the encoder with Haivision-EMS. This allows the EMS to communicate with the encoder, for example, to monitor the connection status.

To manage a Makito X Series device through Haivision-EMS, the device must first be discovered and paired with the system.

> ⚠ **Note**
>
> For device discovery to work, mDNS must be enabled on each of the Makito X devices you wish to pair.

To pair the Makito X device with Haivision-EMS:

1. On the Services page, toggle the Haivision-EMS button to **On**.
2. Hover over Haivision-EMS and click **Configure** next to the tools icon.
3. On the Haivision EMS dialog, enter the passcode (copied and pasted from Haivision EMS).
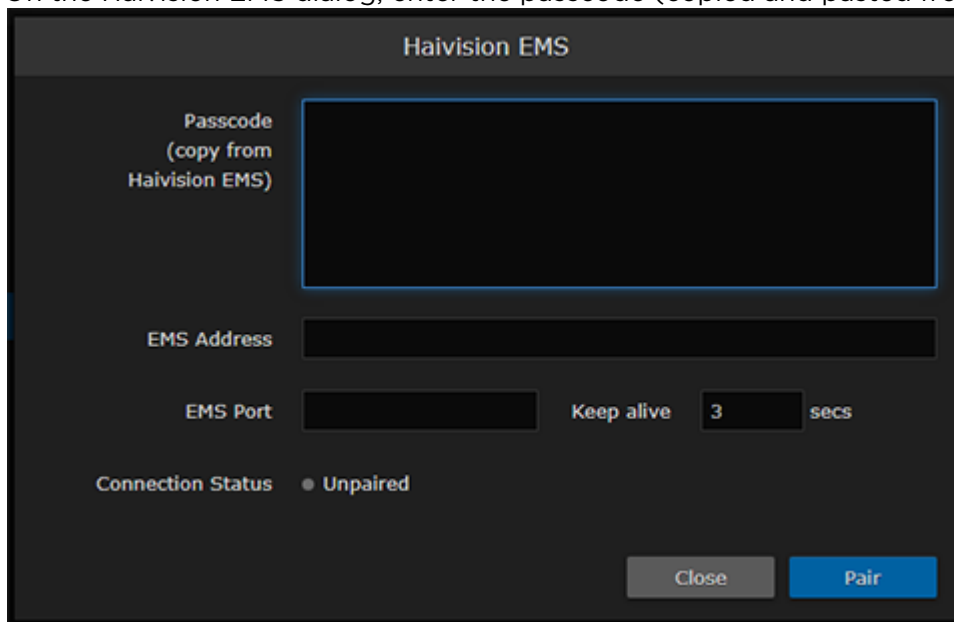
> ⚠ **Note**
>
> On a new system, the EMS Address and Port are blank. When a pairing code is pasted in, the address and port are automatically filled in to reflect the IP address and port contained in the pairing code.
> (Optional) You may change the EMS Address and Port in order to override the defaults extracted from the paring code, for example, to accommodate network security requirements.

4. (Optional) Increase the value in the Keep Alive field to ensure the Makito X can be paired with EMS and remain connected during file transfer.

The Keep Alive value is also filled in when the pairing code is pasted in. "Keep Alive" is the time interval in seconds in which the device will ping the EMS server to maintain its connection.

5. Click **Pair**.
   This initiates the pairing and communication with the EMS server.

To unpair the Makito X device from Haivision-EMS:

1. On the Haivision EMS dialog, click **Unpair**.
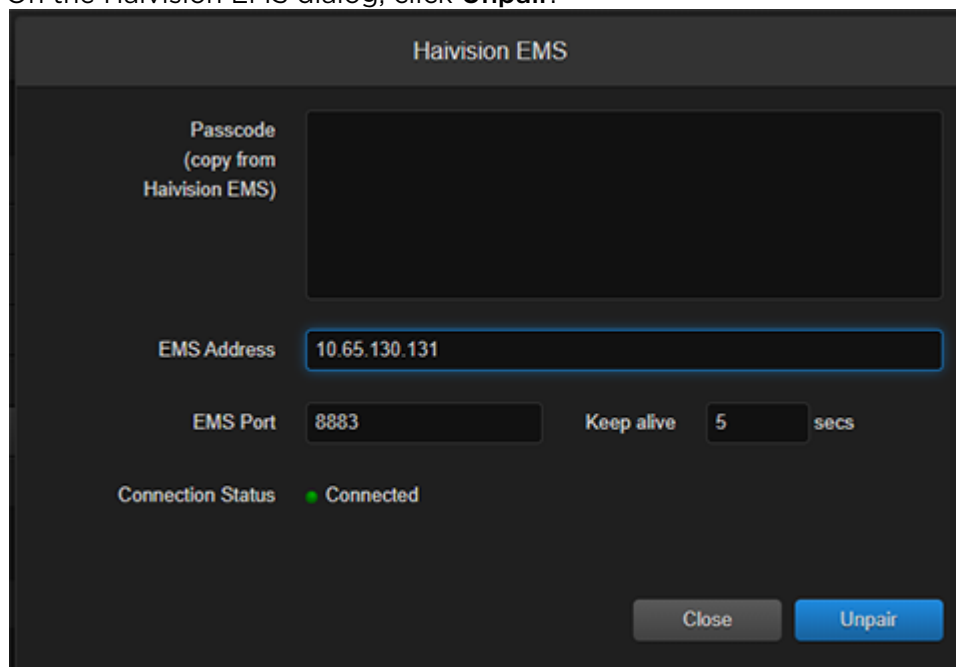
   The unpairing takes effect immediately.

Managing Licenses

- **License File Errors**

Feature licensing allows you to view the licensed capabilities of your Makito X4 as well as add new functionality to already deployed systems.

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 Series appliance.

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 and the associated features, including Audio/Video Inputs, Video, Audio, Metadata, and Stream capabilities.

Settings   Security

Status
Presets
Update
Network
Date and Time
Services
Licensing

Install

☐ All   Delete

Name

☐ HAI-031906060007-MX4-audenc+16.lic

License Features

Audio/Video Inputs

Number Of Baseband Inputs	4
Maximum Input Resolution	UHD

Video

Number Of Video Encoders	8
High Efficiency Video Coding (H.265)	On
MPEG-4 Advanced Video Coding (H.264)	On
Maximum Video Bit Depth	10
Maximum Video Color Subsampling	4:2:2

Audio

Number Of Audio Encoders	16
MPEG-2 AAC-LC ADTS	On
MPEG-4 AAC-LC LOAS/LATM	On

Metadata

Key-Length-Value Metadata (KLV)	On
Cursor-On-Target Metadata (CoT)	On

Stream

Secure Reliable Transport (SRT)	On
TS/RTP	On
TS/UDP	On

System

Maximum Upgradable Release	8.8
Expiration Date	2028-01-01

> **ⓘ Note**
>
> The System values show the version limit (Maximum Upgradable Release) and Expiration Date for the current license. The encoder will block installation of firmware versions that are above the Maximum Upgradable Release version. The unit will remain functional as long as it has not reached the Expiration Date. To obtain an updated license, please contact **Sales@haivision.com.**

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

| | Change | dub-mx4-cot.lic | ✕ | Upload |

| ☐ All | Delete |
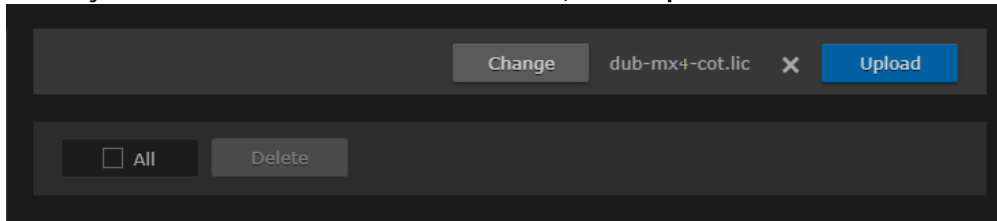
4. To apply your changes, click the **Reboot** button. The encoder will reboot and you will be returned to the Sign-in page.
5. To view an installed license file, click the file in the list. The license file opens in a separate window.

```
#----BEGIN LICENSED FEATURE---- metadata.lcf ----

[METADATA]
KLV.Descr=KLV) Key-Length-Value Metadata
KLV=On

#wlicopt metadata metadata 0n KLV

COT.Descr=CoT) Cursor-on-Target Metadata
COT=On

#wlicopt metadata metadata 0n CoT

#----END LICENSED FEATURE---- metadata.lcf ----
#----BEGIN LICENSING DATA---------------------
[LIC-SIGNATURE]
Version=2.0.1
CreatedOn=2019-03-19 11:42:11
CreatedBy=automation@haivision.com
Sequence=tst1553010131_metadata.lic

[LIC-DEVICES]
HAI-031906060007=Yes

#----END LICENSING DATA-----------------------

Verifying license file "HAI-031906060007-MX4-metadata+cot.lic"...
License verification successful.
```

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

> **ℹ 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 X4 Rugged 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.
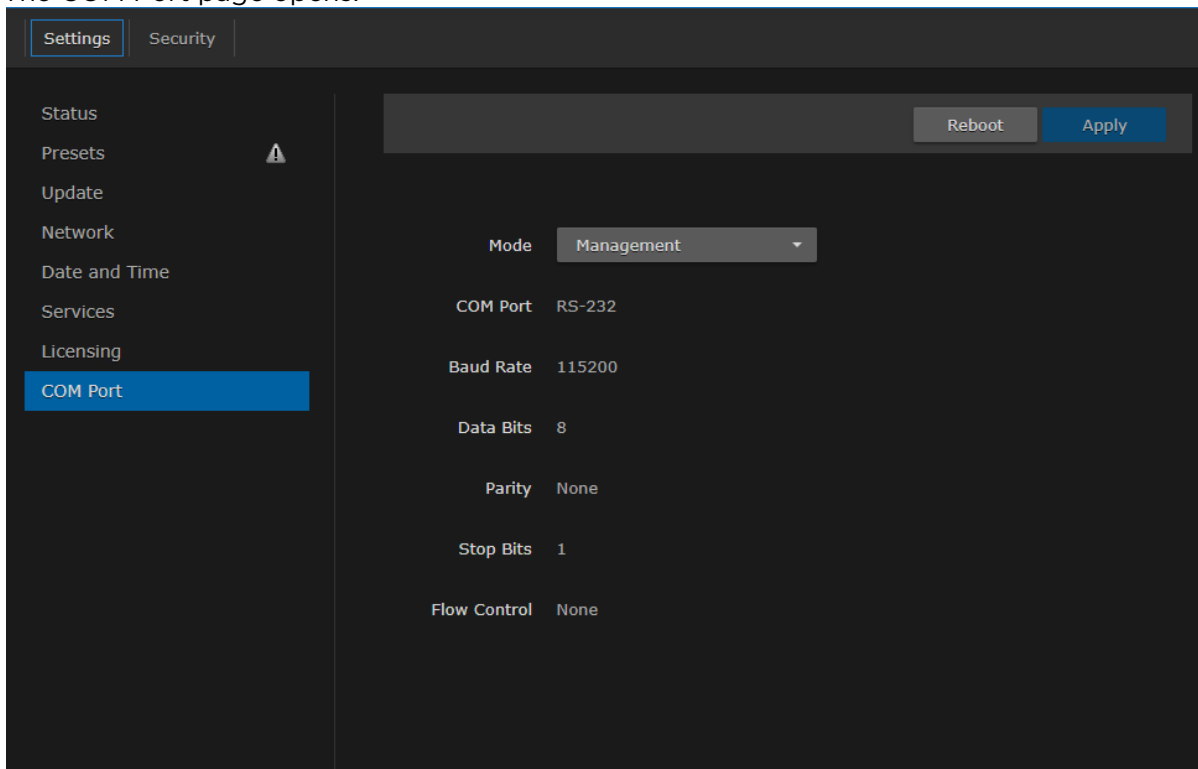
2. (If applicable) To capture metadata, select **Metadata** from the COM Port **Mode** drop-down list.
   OR
   To configure serial pass-through, select **Pass-Through** from the **Mode** drop-down list.
3. To apply your change, click **Apply**.
4. Click **Reboot**.

The changes will take effect after the reboot has completed.

Related Topics

- **COM Port Settings**
- **Installing the Makito X4 Rugged Encoder**

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 Users and Security

> ℹ️ **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 X4 (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 X4.

An account can be allocated to each user of the system so that the identity of the user can be uniquely determined. The Makito X4 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 X4 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.
   The Accounts List View opens, displaying the list of defined user accounts for the encoder.
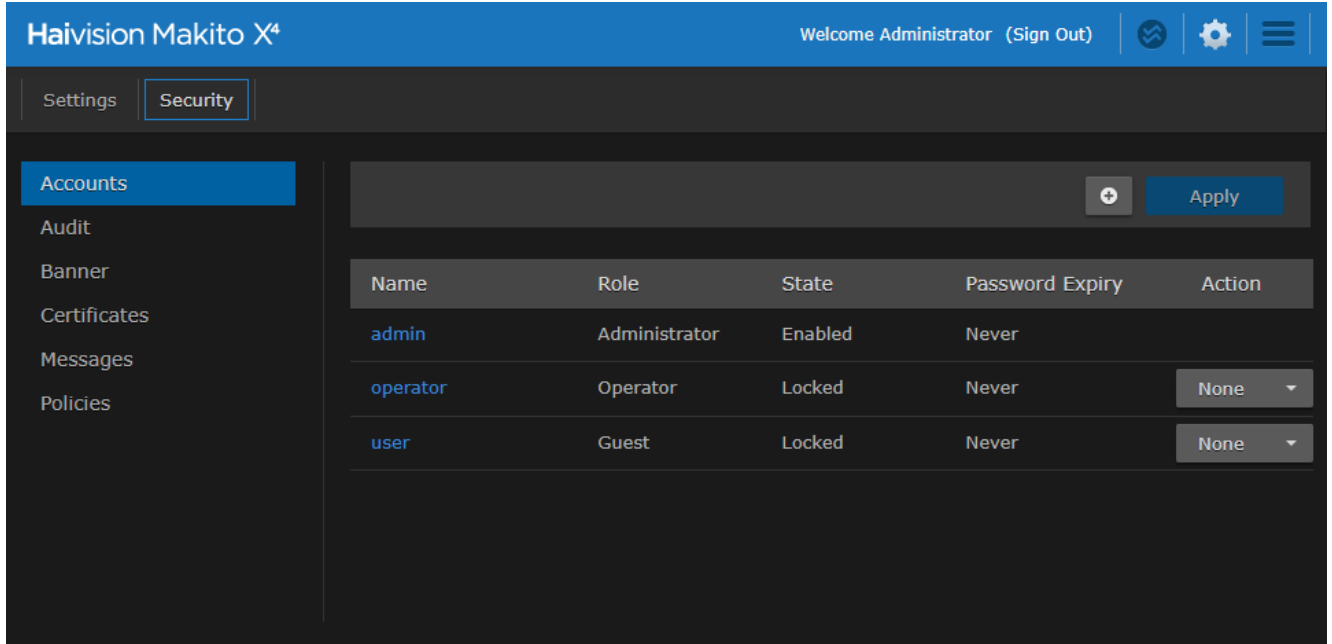
The Accounts List View displays the Name, Role, State (Enabled or Locked), and Password Expiry status for each account. It also provides an option to lock/unlock or delete an account.

2. To view or modify user account details, click the account link in the table to open the Account Settings page. For details, see Account Management.
3. To add a new account, click the ⊕ Add button. For details, see Account Management.
4. To lock or unlock an account, click the drop-down list under **Action** and select either:
   • Lock (if the current State is Enabled) or
   • Unlock (if the current State is Locked).
5. To delete an account, click the drop-down menu under **Action** and select Delete.
6. To apply your changes, click **Apply**. The changes will take effect immediately.

Account Management

> ✅ **Tip**
>
> It is recommended to set the Policies for your system before creating users.

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

To add a new account:

1. From the Accounts List View, click the ⊕ **Add** button.
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" in **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
Username	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
Current Password	n/a	(Your own account only) Type in your current password. ⚠ **Note** This is not required for other accounts since an administrator is frequently asked to change the password by users who have forgotten their passwords.
New Password	n/a	Type in the new password.
Confirm 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 **Add**. • 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**.
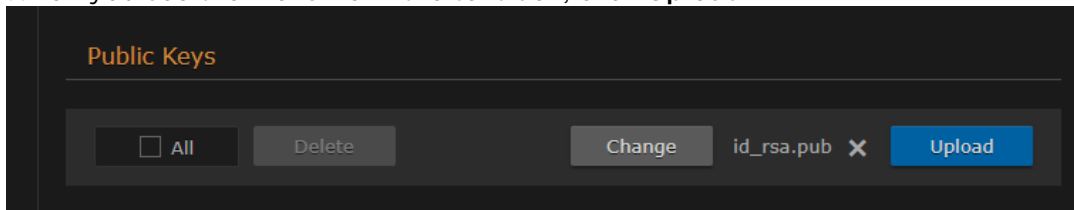
> ✅ **Tip**
>
> To select a different public key file, click **Change**. To remove the selection, click ✖.

The file is then added to the Public Keys list of along with the fingerprint for the key (e.g., for identification purposes).
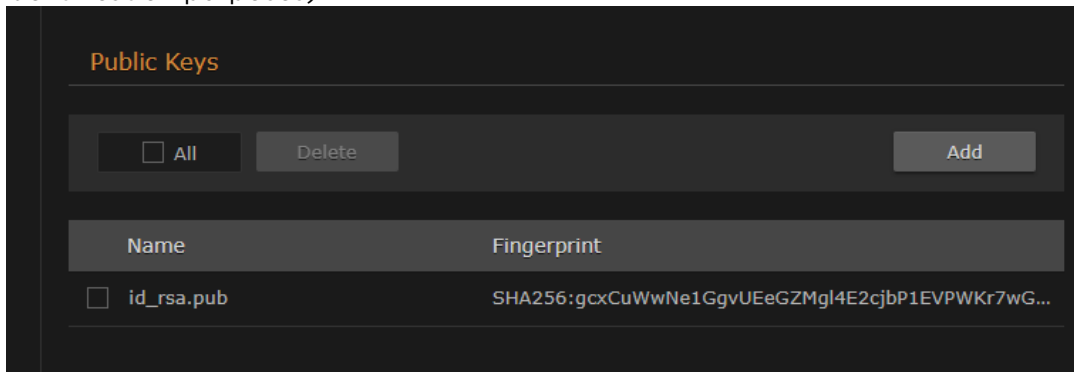
> ⚠️ **Note**
>
> You can now access the CLI interface from your SSH client without providing your account password. You may have to provide a password to decrypt your private key but this is done by your SSH client. If you no longer use password-based authentication to access your account, it is recommended to set a very long password.

> ✅ **Note**
>
> To delete one or more previously uploaded public key files from the list, check the checkbox next to one or more filenames (or check **All**) and click **Delete**.

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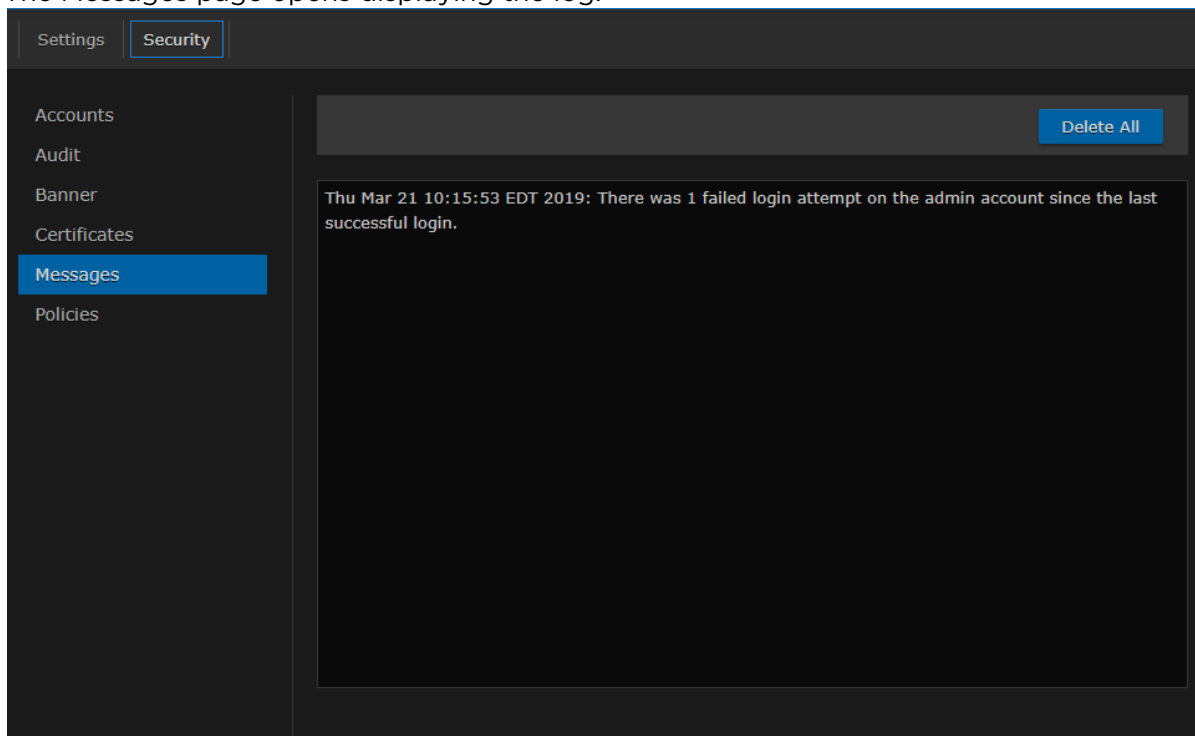
2. To delete the messages, click **Delete All**. The messages will be deleted immediately.

Managing Banners

From the Banner page, administrators can upload a text file for the Advisory and Consent Banner. 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 banner is a single text file with a maximum file size of 4KB.

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. To display the Advisory Notice and Consent Banner upon user sign-in, check the checkbox.

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

> ✅ **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.
> To delete the current banner, click **Delete**. The banner will be deleted immediately.

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. To display the Advisory Notice and Consent Banner upon user sign-in, check the checkbox.

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

From the Policies page, administrators can set policies for passwords, session timeout, and cryptographic strength for Makito X4 user accounts. These policies will apply to all user accounts; therefore, it is recommended to set the policies before beginning to create accounts.
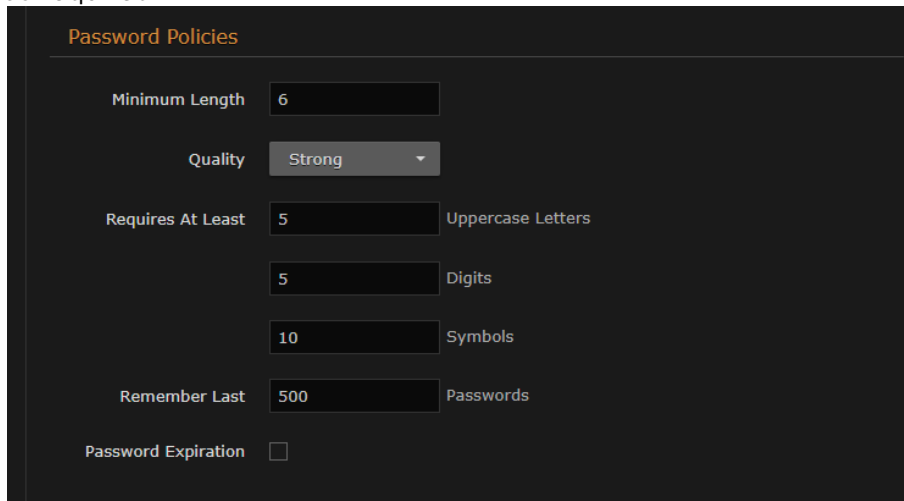
To view and manage the Security policies for the encoder:

1. On the Administration page, click **Security** on the navigation bar and **Policies** on the sidebar. The Policies page opens.
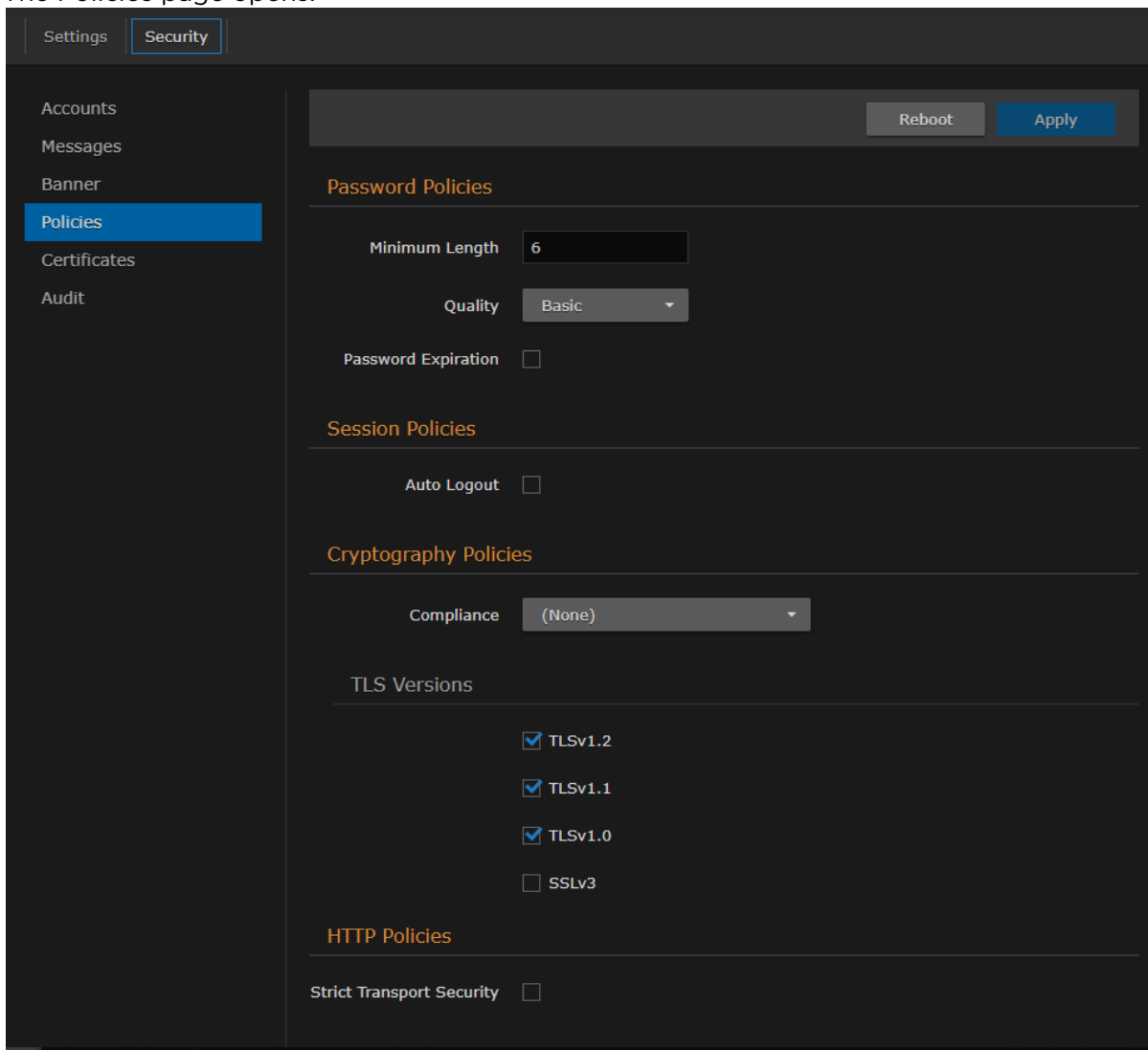
2. Select or enter the new value(s) in the appropriate field(s). For details, see **Policy Settings**.

3. To specify additional password quality criteria, select "Strong" for the Quality and adjust the values as required.

4. 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.

> **!** **Important**
>
> Makito X self-signed TLS certificates are generated with a validity period of less than 825 days.

Generating a Certificate

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

1. On the Administration page, click **Security** on the navigation bar and **Certificates** on the sidebar. The Certificates page opens.
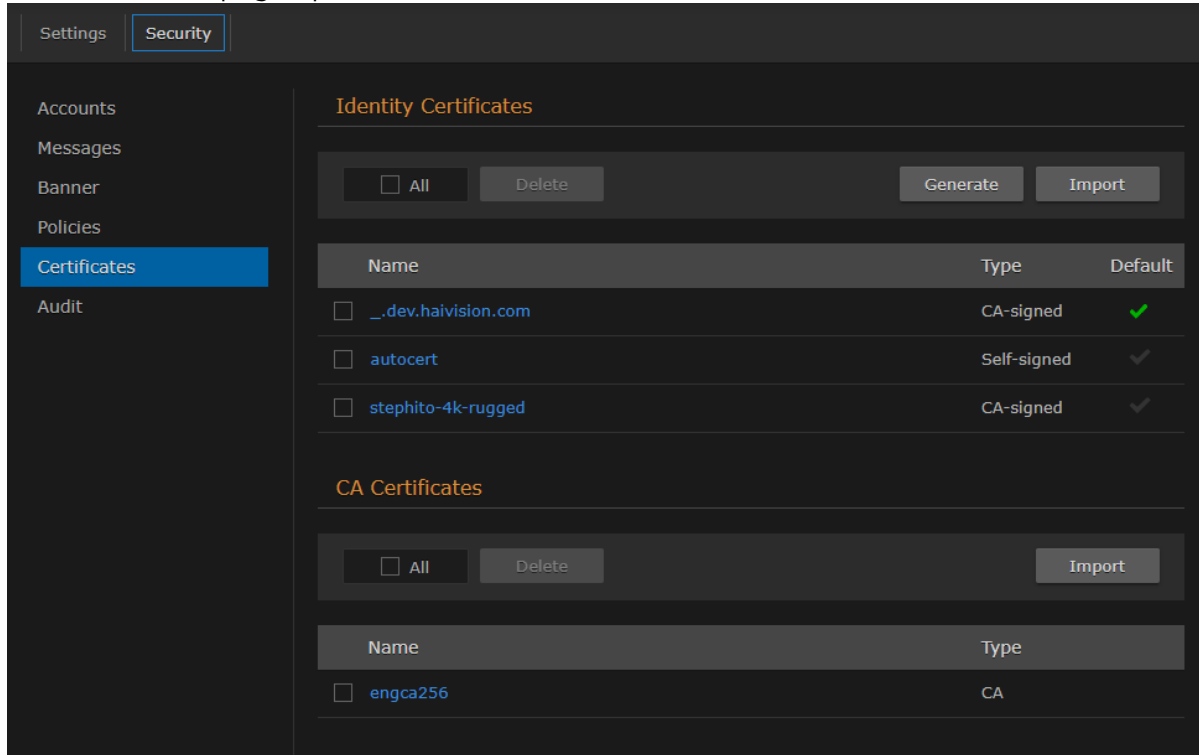
   The default Identity Certificate is indicated with a blue check.
2. Under Identify Certificates, click **Generate**.
3. (Optional) Type a name for the certificate in the Generate Certificate dialog.

4. Select either Self-signed or Certificate Signing Request from the drop-down list. For more information, see "Sign" in "Certificate Settings" (link below).
5. For the subject, type in information about the device that the Identity Certificate represents. For more information, see "Subject" in "Certificate Settings".
6. Click **Generate**.
   If 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".**
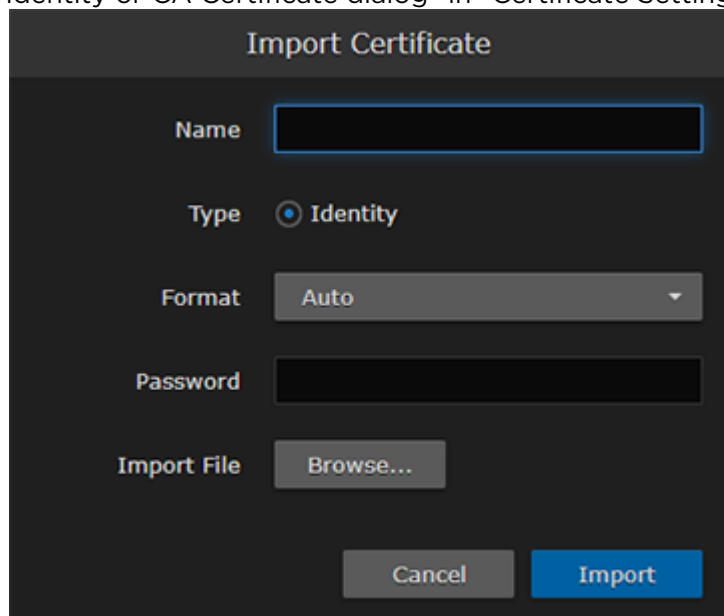
Related Topics:

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

Importing a Certificate

To import an Identity Certificate:

1. On the Certificates page, click **Import** in the Identity Certificates section.
2. On the Import Certificate dialog, type in the Name and complete the remaining fields. See "Import Identity or CA Certificate dialog" in "Certificate Settings" (link below).
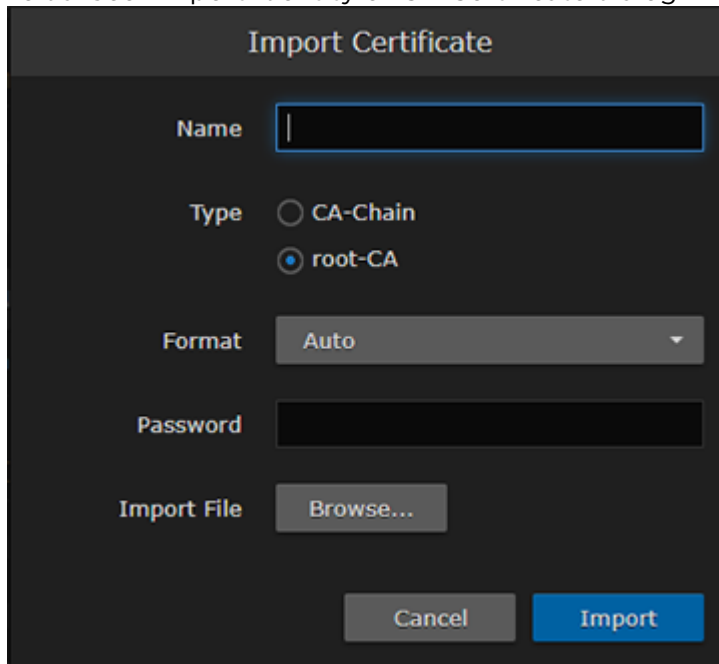
3. Click **Import**.

To import a CA Identity:

1. On the Certificates page, click **Import** in the CA Certificates section.

2. On the Import Certificate dialog, type in the Name, select the Type, and complete the remaining fields. See "Import Identity or CA Certificate dialog" in "Certificate Settings" (link below).

3. Click **Import**.

Related Topics:

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

Viewing Certificate Details

To view the details of a certificate file:

1. On the 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: 84:DE:EC:DE:EC:93:4B:8D:CE:5A:42:FC:90:83:E9:F5
    SHA1: A9:B8:80:A7:22:0B:81:B0:BB:D3:B4:C4:33:16:06:8E:F1:19:62:68
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fa:45:9c:0d:12:9a:0f:32
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=gpm4e.haivision.com
        Validity
            Not Before: Feb 25 17:38:01 2019 GMT
            Not After : Feb 24 17:38:01 2029 GMT
        Subject: CN=gpm4e.haivision.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9c:0f:03:ba:ed:f3:63:8a:b9:e6:96:34:76:38:
                    ba:3a:6e:c5:82:8c:7f:29:3b:30:e8:67:c7:56:83:
                    db:15:63:4a:13:97:f8:ec:94:17:88:27:b9:be:dc:
                    e4:7d:1c:02:bb:10:10:5e:39:dd:3b:38:fe:06:3e:
                    fa:a8:60:6a:7f:ae:ea:5a:b8:bd:a0:3d:48:5e:ec:
                    42:df:a3:7f:db:c7:e7:f5:c5:ef:d6:47:bd:fb:e2:
                    e3:7e:25:73:84:66:3b:34:52:b9:4a:46:a9:a3:54:
                    7c:7e:72:59:7e:7d:fe:98:f8:bc:0f:61:25:2f:56:
                    6d:70:87:34:e9:34:00:7a:88:be:e4:b2:df:60:53:
                    24:ff:84:c0:4e:80:80:23:5a:b0:66:dc:e4:cc:69:
                    0e:48:30:8b:d3:98:02:55:26:ca:ee:68:b9:78:6f:
                    70:54:28:b3:22:e4:ba:49:2b:8e:d7:f6:c4:c6:99:
                    34:57:a3:0b:4a:92:d0:7c:4b:bc:27:d1:77:76:fd:
                    db:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:3D:78:9B:C5:28:0B:4B:C9:FD:30:77:FB:16:50:36:5C:20:C7:A9
            X509v3 Authority Key Identifier:
                keyid:57:3D:78:9B:C5:28:0B:4B:C9:FD:30:77:FB:16:50:36:5C:20:C7:A9

            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Alternative Name:
                DNS:gpm4e.haivision.com, DNS:gpm4e, IP Address:10.65.11.176
    Signature Algorithm: sha256WithRSAEncryption
        56:78:9a:62:d2:a7:b7:7d:bd:40:8b:b1:60:ea:49:3a:e6:74:
        a2:30:fe:4e:1b:e8:8a:55:59:5c:15:7b:ad:97:d2:44:e9:d6:
        90:e0:5f:8c:bf:75:fb:b9:6b:3d:b0:21:d8:6a:4e:f0:ce:58:
        5a:29:fc:2f:f7:5e:fa:4e:50:00:9d:31:4f:28:2f:f9:bf:46:
        3f:0b:8c:9e:a5:3e:61:e7:da:3e:84:73:a0:3d:61:32:94:18:
        78:df:1b:6c:bc:03:c7:03:b2:f5:2b:44:36:37:49:b9:05:2b:
        2f:ca:17:ee:4d:2e:2b:ce:71:19:ad:e7:e4:30:76:5e:0b:f3:
        c6:ec:f5:1b:10:be:fc:55:7c:99:98:54:1f:76:97:a9:23:a7:
        53:d8:48:5f:8a:3b:55:d8:97:e4:fa:51:7c:e3:0b:90:7d:46:
        e3:a1:bc:97:fb:e7:72:a9:5a:85:fa:39:46:03:d9:f1:4f:e6:
        b2:a7:89:08:73:3d:54:74:b4:c9:57:80:9e:98:34:5e:8f:23:
        7b:33:e5:1e:b0:60:1f:a1:aa:81:3f:a5:ed:e5:7c:e1:9e:1d:
        7d:48:ff:ee:5f:5c:d1:23:fd:81:cc:4d:6d:75:a7:38:d6:7e:
        22:98:e6:d2:af:8b:ac:30:ba:3d:23:dc:ef:65:33:6d:28:8c:
        03:d8:30:d8
-----BEGIN CERTIFICATE-----
MIIDPDCCAiSgAwIBAgIJAPpFnA0Smg8yMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME2dwbTR1LmhhaXZpc21vbi5jb20wHhcNMTkwMjI1MTczODAxWhcNMjkwMjI0
```

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	n/a	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.
Type		Select the type of the imported certificate:
	Identity (Identity Certificates)	• **Identity:** If you are importing an identity certificate.
	root-CA (CA Certificates)	• **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.
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 **Browse** 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.
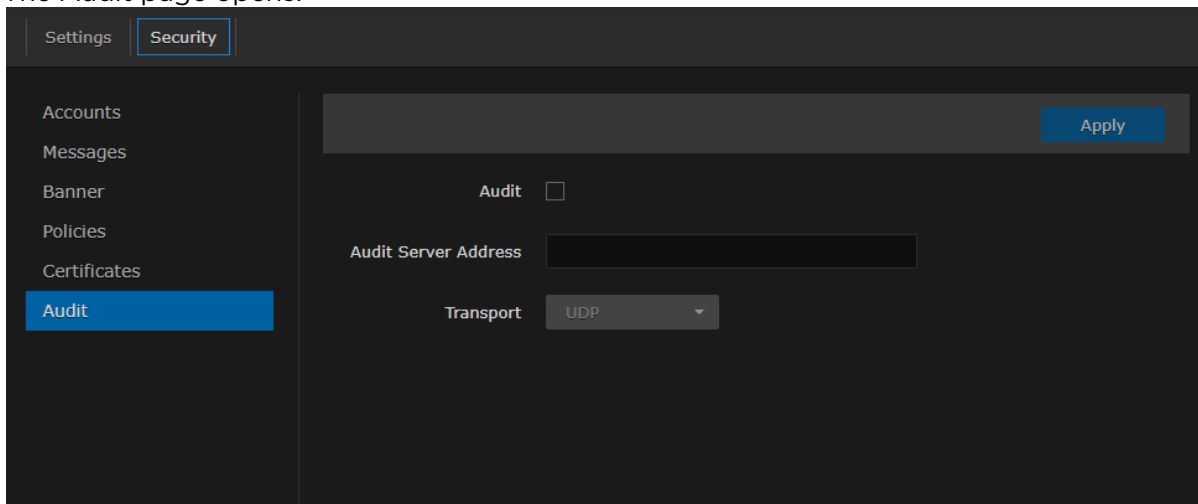
2. Check the **Audit** checkbox to start logging to the audit server.
3. Type the audit server address and port in the Audit Server Address field. See "Audit Settings" (link below) for more details.
   The server address must be the Common Name or one of the Subject Alternative Names in the server's 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.
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".
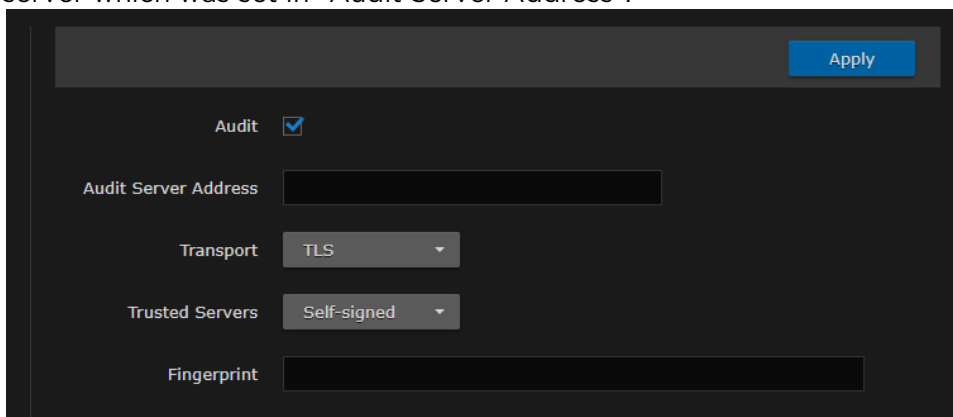
7. To apply your changes, click **Apply**.

Related Topics

- **Managing Certificates**

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.
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.

Using SNMP to Configure A/V Services

> **ℹ 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 X4.

> **✅ 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 Makito X devices 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 Series uses Net-SNMP Version 5.7.3 and support SNMP v1, v2c, and v3.

The Makito X Series 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 X4 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-only

• HAI-MAKITO-X4-ENC-CAPS.txt	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X4 (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-X4-DEC-CAPS.txt	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X4 (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.

> ℹ️ **Note**
>
> You can also download the MIBs directly from your Makito X4 under: `/usr/share/snmp/mibs/HAI-*.txt`

SNMP Agent Components

This section presents key components used to set up SNMP management on the Makito X4.

- **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 Series 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 SeriesX 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, ad insertion, 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` , `estroy`). 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 Series 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 RS-232 (Makito X4 Rugged only). This alphabetical command reference lists and describes the available Command Line Interface (CLI) commands to configure and manage the Makito X4 encoder.

Accessing the CLI

To access the encoder CLI:

1. Open a telnet session to the encoder (for the default encoder IP address, see Default Encoder IP Address).
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 X4 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, audio/video encoding, H.264 and HEVC streaming. 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 X4, 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 X4 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.
session	Yes	Yes	"get" only	Manage SAP multicast advertising sessions.
stream	Yes	Yes	"get" only	Create and manage audio/video streams.
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.

Administration Commands

Command	Role			Description
	Admin	Operator	Guest	
Network and Management				
config	Yes	Yes	"list" only	Manage configurations on the Makito X4.
date	Yes	Yes	Yes	Display the current date.
dtconfig	Yes	—	—	Set the date and time on the encoder.
emspair	Yes	—	—	Pair and unpair the Makito X with/from a Haivision EMS (Element Management System).
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 X4.
ipconfig	Yes	—	—	View and set the parameters that specify the networking context for the Makito X4, 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 X4.
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.
reboot	Yes	—	—	Halt and restart the Makito X4.
service	Yes	—	—	Enable and disable network services, including HTTP, SNMP, SSH, and Telnet.
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.
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.
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 X4, 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. As of Makito X4 v1.5, Makito X1 v1.2, and Makito FX v1.0 you can specify a range or a comma-separated list of IDs for the operation, as shown in the examples that follow.

The number of encoders varies with the hardware platform:

Makito X4	encoder ID is a number between 0 and 31.
Makito X4 Single Channel	encoder ID is a number between 0 and 3.
Makito X1	encoder ID is a number between 0 and 3.
Makito FX	encoder ID is a number between 0 and 3.

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	Mutes encoding of the audio input (i.e., causes the encoder to encode silence instead of the selected audio input.) ✅ **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.

Action	Description
get	Displays encoder audio status information. You can specify configuration, statistics, or all audio information. ✅ **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	SDI1CH1+2	The Audio Input for the encoder. The available inputs for Makito X4 devices: • Analog (Makito X4 Rugged only) • SDI1CH1+2, SDI1CH3+4, SDI1CH5+6, SDI1CH7+8, SDI1CH9+10, SDI1CH11+12, SDI1CH13+14, SDI1CH15+16 • SDI2CH1+2, SDI2CH3+4, SDI2CH5+6, SDI2CH7+8, SDI2CH9+10, SDI2CH11+12, SDI2CH13+14, SDI2CH15+16 • SDI3CH1+2, SDI3CH3+4, SDI3CH5+6, SDI3CH7+8, SDI3CH9+10, SDI3CH11+12, SDI3CH13+14, SDI3CH15+16 • SDI4CH1+2, SDI4CH3+4, SDI4CH5+6, SDI4CH7+8, SDI4CH9+10, SDI4CH11+12, SDI4CH13+14, SDI4CH15+16
	SDI1CH1+2	The available inputs for Makito X1 devices: • Analog, SDI1CH1+2, SDI1CH3+4, SDI1CH5+6, SDI1CH7+8, SDI1CH9+10, SDI1CH11+12, SDI1CH13+14, SDI1CH15+16
	HDMICh1+2	The available inputs for Makito FX devices: • HDMI1Ch1+2 • SDI1Ch1+2, SDI1Ch3+4, SDI1Ch5+6, SDI1Ch7+8, SDI1Ch9+10, SDI1Ch11+12, SDI1Ch13+14, SDI1Ch15+16
language	n/a	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.

Parameter	Default	Description/Values
level	6	(Makito X1 and Makito X4 Rugged, Analog Input only) Adjusts the maximum analog Audio Input signal level (0 dBfs): • Makito X4 Rugged: from 0 to +6dBU • Makito X1: from -6 to 0dBU
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.
sample rate	48 kHz	The number of audio samples per second taken from the incoming signal. • 48 kHz (SDI audio is always sampled at 48 kHz) • 16 kHz (Analog Input, Makito X1 and Makito X4 Rugged only) ⚠ **Note** See `bitrate` (below) since the allowed bitrate ranges for 16 kHz sample rate are different than what was previously available for 48 kHz.
bitrate	128 kbps	The Audio Bitrate for the encoder. 4..576 ⚠ **Note** The available bitrate range depends on the current `mode` and `sample rate`. As of v1.4, the Makito X4 allows lower audio encoding bitrates (intended for very limited bandwidth streaming situations), as well as higher quality audio encoding at higher bitrates. 48 KHz sample rate: • For mono, the bitrate range is 12 to 288 kbps. • For stereo, the bitrate range is 14 to 576 kbps. 16 KHz sample rate: (analog only): • For mono, the bitrate range is 4 to 96 kbps. • For stereo, the bitrate range is 5 to 192 kbps.

Examples

```
# audenc 0,2,3 start
```

Starts audio encoders 0, 2 and 3. You will receive the following confirmation:
```
3 audio encoders started successfully.
```

```
# audenc 0-3 stop
```

Stops audio encoders 0, 1, 2 and 3.
```
4 audio encoders stopped successfully.
```

```
# audenc 0,2,4-6 stop
```

Stops audio encoders 0, 2, 4, 5 and 6
```
5 audio encoders stopped successfully.
```

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

Sets the Audio Input to SDI1CH1+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 Language     : (None)
    Audio Bitrate      : 128 kbps
    Audio Samplerate   : 48 KHz
    Audio Mode         : Stereo
    Audio Algorithm    : MPEG2-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
```

```
# audenc 0 get stats
```

Returns audio configuration information for a Rugged encoder configured for Analog Input, such as:

```
Encoder ID            : 0
Name                  : "Audio Encoder 0"
Configuration:
  Audio Input         : Analog
  Audio Language      : (None)
  Audio Bitrate       : 5 kbps
  Audio Samplerate    : 16 kHz
  Audio Mode          : Stereo
  Audio Algorithm     : MPEG2-ADTS
  Audio Input Level   : 6 dBu
```

Related Topics

- **Configuring Audio Encoders**
- **Audio Encoder Settings**

leds

The `leds` command may be used to help locate a Makito X4 device by initiating blinking of the Status LEDs on the Makito X4 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.

The blinking duration can be set from 1 to 60 minutes. If no duration is set, blinking will last for 15 minutes and can be cancelled at any time using `leds stop`.

Synopsis

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

Actions

Action	Description
start	Initiates blinking of the Status LEDs on the Makito X4 face-plate.
stop	Cancels blinking of the Status LEDs on the Makito X4 face-plate.
get	Displays LED status information for the Makito X4.

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 LEDs, provides the following confirmation:
```
LEDs set to blink for 2 minutes.
```

```
# leds get
```

Displays current LED status:
```
LED States:
  Status        : Green
  4K Status     : Off
  Error         : Off
  SDI-1 Status  : Off
  SDI-2 Status  : Green
  SDI-3 Status  : Green
  SDI-4 Status  : Green
```

```
# leds stop
```

Cancels blinking of the LEDs.
```
LEDs no longer blinking.
```

Related Topics

- **Viewing System Status Information**

metadata

The `metadata` command is used to manage metadata sources. This command configures the Makito X4 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 X4 supports three metadata input types: either from the COM1 serial port (Makito X4 Rugged only), the HD-SDI interface, or a user-definable UDP network port.

Multiple metadata sources can be multiplexed into the same Transport Stream. To do so, you must specify the metadata source elementary stream (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
enable_passthrough_on_serial_port
```

> ⚠️ **Note**
>
> `enable_metadata_on_serial_port` will configure the serial port for metadata input. The serial port will no longer be available for console IO (management) or pass-through. `enable_console_on_serial_port` will configure the serial port for console IO (management). `enable_passthrough_on_serial_port` will configure the serial port for pass-through.

Actions

Action	Description
start	Starts the metadata source.
stop	Stops the metadata source.
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	Displays information on the metadata source. You can specify configuration, statistics, or all metadata information. ✅ **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	(Makito X4/Makito X1 Rugged Encoders only) Enables metadata capture from the serial port.
enable_console_on_serial_port	(Makito X4/Makito X1 Rugged Encoders only) 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

Parameter	Default	Description/Values
`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 (Makito X4 only) • bnc3 (Makito X4 only) • bnc4 (Makito X4 only)
`decimation`	1	(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)		

Parameter	Default	Description/Values
`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.
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 (Makito X4/Makito X1 Rugged Encoders only) and UDP Source-specific parameters		
`format`	KLV	Selects the data format for the metadata. • KLV • CoT

Parameter	Default	Description/Values
`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.
`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 (Makito X4/Makito X1 Rugged Encoders only)		
`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 (Makito X4 Rugged only), (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

- **CoT Relaying**

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 X4 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

- **Mission ID/Security Data Set 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.

Examples

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

- **UAS KLV Tag Filtering**

passthrough

On a Makito X Series encoder with serial ports (such as the Makito X with SDI, the Makito X1 Rugged, or the the Makito X4 Rugged), 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	Displays passthrough information. You can specify configuration, statistics, or all information. ✅ **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
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

Parameter	Default	Description/Values
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 Xon/Xoff is a protocol for controlling the flow of data between devices on an asynchronous serial connection. ✅ **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)	Specifies the amount of time in seconds a TCP connection will be kept open when no data is being received from the remote client. The timeout can be up to 10 minutes (0..600 seconds). The idle timeout is important when you have more than one remote end point controlling the serial port: if a remote application is left running with the TCP connection active, no one else will be able to control the COM port. ✅ **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**

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	A unique number or name assigned to the stream. The ID of the existing stream to be advertised via SAP. ✅ **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.

Parameter	Default	Description/Values
copyright	n/a	(Optional) Enter the copyright information for the session.
[id]	n/a	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)**

stream

The `stream` command is used to create and manage Makito X4 audio/video streams.

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.

Synopsis

```
stream create addr=ipaddr port=udpport [id=number] [name=text]

  [encapsulation=ts-rtp | ts-udp | 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]]
  [shaping=yes,no [ceiling=percentage] [idlecells=yes,no]
  [delayaudio=yes,no]] [interface=auto,eth0,eth1] [databitrate-auto,valueinkbps]
  [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)
 direct-rtp: RFC3984 [rtcp=on,off]
 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]
    [resource="resid"] [user="username"] [publishid="string"]
    [redundancy=none, active-active, active-backup] [secaddr=ip addr] [secport=udpport]
    [secsourceport=udpport]
    [secinterface=auto,eth0,eth1]
```

```
Parameters available for all ts-based streams:
 [videopid=pid] [audiopid=pid[,pid,pid]] [datapid=pid]
 [pcrpid=pid] [pmtpid=pid]
 [program=num] [tsid=id]
```

```
Possible methods 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
```

```
stream id/name start
stream id/name stop
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.
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
`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	ℹ️ **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 `63` characters
`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
`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.
`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`
`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 MPEG-TS stream (UDP or RTP), and video encoder `0` for 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 (MPEG-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.

`datasrc`	n/a	(Optional) The metadata source. `id/name` (`0=serial, 1-4=SDI;` all others are `UDP`) ℹ️ **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`
`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. ℹ️ **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`
`idlecells`	no	(Optional, shaping must be `yes`) When enabled, Idle TS cells will be inserted into a MPEG-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`
`interface`	auto	(Dual NICs must be available) Assigns the stream to either eth0 or eth1, or auto. (When set to "auto", eth0 takes precedence as long as the address is resolvable; otherwise the output switches to eth1.)
`databitrate`	auto	(CBR or CVBR streams with Metadata sources) Enables you to set the Metadata value used in the calculation that compares the output stream bitrate to the Total TX Bandwidth value. • `auto:` The system tries to measure the bitrate of metadata sources and adjust the stream bitrate accordingly (especially useful for traffic shaped streams) • Enter a value in kbps between 0 and 10,000.
`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
ts-rtp and ts-udp streams		
`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`	O	(Optional) Transport Stream ID. Identifies the transport stream in the Program Association table (PAT) of the TS stream. 0-65535
`fec`	no	Enables Forward Error Correction (FEC). `yes,no` FEC settings include: [rows=10] [columns=10] [level=A,B] [alignment=yes,no]
SRT (see Configuring Secure Reliable Transport (SRT)) ***encapsulation must be*** `ts-srt`		
`mode`	caller	Specifies the SRT Connection Mode: • caller • listener • rendezvous
`sourcepo rt`	auto	(SRT connection mode must be caller) Specifies the UDP source port for the SRT stream.
`encrypti on`	none	Enables AES encryption and specifies the key length, either: none, AES-128, or AES-256
`passphra se`	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	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%	Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-50%
`adaptive`	no	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.
`resource`	n/a	(Stream Publishing ID) Identifies the name of the resource and facilitates selection should the listener party be able to serve multiple resources. See **Configuring SRT Access Control**.
`user`	n/a	(Stream Publishing ID) Identifies the User Name, or authorization name, that is expected to control which password should be used for the connection. The application should interpret it to distinguish which user should be used by the listener party to set up the password.
`publishi d`	n/a	(Stream Publishing ID) Enter using custom format. For more information, see **Configuring SRT Access Control**.

`redundancy`	none	Configures the stream to use redundant transport paths: • none • active-active: Stream packets are sent on both defined network paths, and both links continually transmit. The listener uses the first received stream packets and ignores the duplicate packets received from the other network paths. This mode maintains low latency at the expense of network bandwidth. See **Using Path Redundancy with SRT Streaming**. • active-backup: The interfaces are bonded for redundancy (or fault tolerance mode). Only one interface works at a time and the other one works only if the first one fails.
`secaddr`	n/a	The destination IP address for the redundant stream.
`secport`	n/a	The destination UDP port for the redundant stream.
`secsourceport`	n/a	The UDP source port for the redundant stream.
`secinterface`	n/a	(Dual NICs must be available) The interface for the redundant stream, either auto, eth0 or eth1.

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
```

Creates and starts a streaming session.

```
# 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 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 encoder stream #1, for example:

```
Stream                    : 1
Name                      : "SRT1"
Configuration:
  Encapsulation           : TS-SRT
  Mode                    : Caller
  Redundancy              : (None)
  Interface               : Auto
  Address                 : 192.0.2.235
  UDP Port                : 1234
  Contents                : Video ("Video Encoder 0":0),
                            Audio ("Audio Encoder 0":0)
  Video PID               : 33 (0x21)
  Audio PID               : 36 (0x24)
  PCR PID                 : 33 (0x21)
  PMT PID                 : 32 (0x20)
  Transport Stream ID     : 1
  Program Number          : 1
  MTU                     : 1500
  TOS                     : 0xB8
  TTL                     : 18
  Bandwidth               : 6,510 kbps
  Traffic Shaping         : Off
  AES Encryption          : Off
  Network Adaptive        : No
  Max Traffic Overhead    : 25% (10,923 kbps)
  Added Latency           : 250 ms
  Persistent              : Yes
Statistics :
  State                   : STREAMING
  Up Time                 : 3d1h16m8s
  Source Port             : 43825
  Sent Packets            : 1,040,512
  Sent Bytes              : 1,252,450,560
  Bitrate                 : 198 kbps
  SRT v1.4.2:
    Peer Version          : 1.3.2
    Reconnections         : 1
    AES Encryption        : Off
    Resent Packets        : 6
    Resent Bytes          : 8,160
    Dropped Packets       : 0
    Dropped Bytes         : 0
    Received ACKs         : 41,084,318
    Received NAKs         : 6
    Max Bandwidth         : 12,659 kbps
    Path Max Bandwidth    : 345,085 kbps
    RTT                   : < 1 ms
    Local Buffer Level    : 14 ms
    Latency               : 250 ms
```

```
# stream 2 get stats
```

Returns status information for Stream #2, such as:

```
Stream ID                : 2
Name                     : (None)
Statistics:
  State                  : STREAMING
  Up Time                : 5d16h33m26s
  Source Port            : 39419
  Sent Packets           : 317,298,860
  Sent Bytes             : 402,565,886,576
  Bitrate                : 6,006 kbps
  SRT v1.4.2:
    Peer Version         : 1.3.2
    Reconnections        : 1
    AES Encryption       : Off
    Resent Packets       : 2
    Resent Bytes         : 2,720
    Dropped Packets      : 0
    Dropped Bytes        : 0
    Received ACKs        : 40,252,057
    Received NAKs        : 2
    Max Bandwidth        : 11,234 kbps
    Path Max Bandwidth   : 346,473 kbps
    RTT                  : < 1 ms
    Local Buffer Level   : 12 ms
    Latency              : 250 ms
```

```
# stream 1 del
```

Deletes Stream #1.

> ℹ️ **Note**
>
> To configure the ceiling percentage for CBR streams with metadata, see **Bandwidth Overhead for CBR Streams with Metadata**.

Related Topics

- **Configuring Streaming Outputs**
- **Output Settings**

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 - 7) or all.

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
algorithm	H265	The codec algorithm for the encoder: (See AVC and HEVC Encoding) • H264 (AVC) • H265 (HEVC)
input	BNC-1	The Video Input port for the encoder: • BNC-1 • BNC-2 • BNC-3 • BNC-4

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**).
`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. ℹ️ **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: `32–120000`
`resizemode`	Scale	(`resolution` cannot be set to Auto and must be less than the Input Format detected) Select whether to scale or crop the input to the desired resolution. See "Resizing" in **Video Encoder Settings**.
`gopsize`	120	The Group of Pictures size for the encoded video. Range: `1–1000` ℹ️ **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 (i.e., video compression mode) 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 • `IBBP` : I, BB (two B frames in sequence) and P frames (highest delay; highest quality) • `IBBBP:` I, BBB (three B frames in sequence) and P frames • `IBBBBP:` I, BBBBB (four B frames in sequence) and P frames (highest delay; highest quality) > ℹ️ **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.
`profile`		Select the application profile class for the encoder: • For H.264: Baseline, Main, High, High10, High422 • For H.265: Main, Main10, Main422-10
`skipframes`	Off	(`ratecontrolmode` must be CBR) Select whether to allow the encoder to skip part of the image in order to respect the bitrate limit. See "Partial Image Skip" in **Video Encoder Settings**.
`picrate`	Auto	The video frame rate per second: • `Auto` : Encodes at the same frame rate as the input • Range: 1-60
`intrarefresh`	Off	This parameter enables Intra-refresh video encoding support in order to minimize latency, smooth the video bitrate, and minimize GOP pulsing artifacts.
`closedcaption`	Off	This parameter enables Closed Captioning on the encoder stream. `Off, On`
`chromasubsampling`		Select the Chroma Subsampling for the encoder: • 420-8bit • 420-10bit (Encoding Profile must be Main 10 or Main 4:2:2 10) • 422-8bit (Encoding Profile must be Main 10 or Main 4:2:2 10) • 422-10bit (Encoding Profile must be Main 10 or Main 4:2:2 10)

Parameter	Default	Description/Values
`ratecontrolmode`	CBR	Select the Rate Control for the encoder: • CBR (Constant Bitrate): Includes Traffic Shaping, Idle Cells and Delayed Audio • CVBR (Capped Variable Bitrate, VBR): Includes Traffic Shaping only
`maxbitrate`		(Rate Control must be VBR) Enter the maximum video bitrate for the encoder: `0..120000` (`0` is Auto configure) ℹ **Note** `maxbitrate` should be greater than or equal to `bitrate`.
`ptsoffset`	50 ms.	Offset video timestamps by this value in ms. Range: `-1000..1000`
`resolution`	Auto	Specifies the stream output resolution (i.e., 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) • 2160p, 3840x2160p • 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

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                    : "Video Encoder 0"

Configuration:
  Video Input           : BNC-1
  Video Format          : Auto-Detect
  Aspect Ratio          : Auto-Detect
  Video Codec Algorithm : H.265
  Video Encoding Profile : Main
  Video Bitrate         : 6000 kbps
  Video GOP Size        : 120
  Encoded Picture Rate  : Input/Auto
  Output Resolution     : Input/Auto
  Time Code             : None
  Closed Captioning     : Off
  Video Resize Mode     : Scale
  Video GOP Structure   : IP
  Video GOP Mode        : Normal
  Chroma Subsampling    : 4:2:0 8-bit
  RateControl Mode      : VBR
  Video MaxBitrate      : Auto
```

```
# videnc 0 get stats
```

Returns encoder statistics:

```
Encoder ID              : 0
  Name                  : "Video Encoder 0"
  Statistics :
  State                 : WORKING
  Uptime                : 21h8m28s
  Input Present         : Yes
  Input Type            : SDI
  Input Format          : 1920x1080p59
  Output Resolution     : 1920x1080p
  Input Aspect Ratio    : 16:9
  Encoded Slices        : 1
  Encoded Frames        : 2,148,020
  Encoded Bytes         : 2,326,715,604
  Encoded Frame Rate    : 59.94
  Encoded Bitrate       : 5,994 kbps
  Encoder PTS           : 0x1708c8ce8
  Encoder Load          : 14%
  Closed Captioning     : Disabled
  H.264 Profile         : Main
  H.264 Tier            : Main
  H.265 Level           : 4.1
  Entropy Coding        : CABAC
```

Related Topics

- **Configuring Video Encoders**
- **Video Encoder Settings**

vidin

The `vidin` command is used to view and manage video input parameters. ID is used to select the video input: either 0 for BNC-1, 1 for BNC-2, 2 for BNC-3, 3 for BNC-4, or all.

Synopsis

```
vidin ID set
vidin ID get
vidin ID clear
```

Actions

Action	Description
set	Configures video input parameters. A series of one or more `parameter=value` pairs can be specified at once. See **Parameters** below.
get	Displays information on the video input.
clear	Clears the video input's statistics.
help	Displays usage information for the `vidin` command.

Parameters

Parameter	Default	Description/Values
filter	Off	This parameter enables Input Image Filtering for the input interface in order to optimize the compression of the image and to enhance the overall quality of the coded video stream.

Related Topics

- **Configuring Video Encoders**
- **Video Encoder Settings**

Administration Commands

account

The `account` command is used to create, delete, and modify user accounts for Makito X Series devices.

> ⚠ **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 device, including account name, role, state, password expiry status, and public key(s).
list	Lists the account information for the user or the Makito X device 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 "Changing Your Password" (link below).
pubkey add|remove keyfile	Adds or removes a public key to the user account. See "Managing Public Key Authentication" (link below) for more information.
pubkey list	Lists any public key files that have been uploaded for this account.
lock	Locks the user account (if Enabled).

Action	Description
unlock	Unlocks the user account (if Locked).
delete	Deletes the user account.

Parameters

Parameter	Default	Description/Values
role	Administrator	Use with the `account create` command to specify the role for the user account, either: • Administrator • Operator • Guest For details on roles, see "Role-based Authorization" (link below).

Examples

```
# account all list

Returns the list of all accounts, for example:
name               role             state      pwd expiry     pubk
------------------ ---------------- ---------- -------------- ----
admin              Administrator    Enabled    never          Yes
jdube              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**
- **Account Setting**
- **Changing Your Password**
- **Managing Public Key Authentication**
- **Role-based Authorization**

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.

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`

Parameter	Default	Description/Values
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**
- **Audit Settings**

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 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 *
*************************************************************************
```

Related Topics

- **Managing Banners**

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

Examples

```
# certificate all get
```

Returns the certificate information for the Makito X4.

```
Certificate Name     : autocert (default)
Type                 : id
Signature            : Self-signed
Subject              : test.haivision.com
Issuer               : test.haivision.com
Expiration           : Feb 13 18:54:26 2029 GMT
Fingerprint          : md5:70:AC:75:C5:B4:5E:C8:51:1C:13:CA:9E:E2:CB:EF:E3
X509v3 Subject Alternative Names:
   DNS               : test.haivision.com
   IP Address        : 10.65.11.148


Certificate Name     : cert1
Type                 : id
Signature            : Self-signed
Subject              : MX4-test
Issuer               : MX4-test
Expiration           : Aug 3 18:31:37 2022 GMT
Fingerprint          : md5:45:5B:7E:C2:BF:D6:6E:9F:32:B9:7F:BE:73:E1:3F:DC
X509v3 Subject Alternative Names:
   DNS               : MX4-test
   IP Address        : 10.65.135.35


Certificate Name     : cert2
Type                 : id
Signature            : Request not signed
Subject              : QA-test
Issuer               : Request not signed
Expiration           : No expiration date is set before certificate is signed.
Fingerprint          : md5:75:85:8d:ec:82:61:6d:11:be:fe:28:45:d6:2d:68:00
```

Related Topics

- **Managing Certificates**

config

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

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**

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 202303271100
```
Sets the encoder clock to Wednesday March 27 11:00:00 EDT 2023

Related Topics

- **date**
- **tzconfig**
- **Configuring Date and Time**

emspair

The `emspair` command is used to pair and unpair a Makito X Series device with/from a Haivision EMS (Element Management System). This allows the Haivision EMS to discover, manage and monitor the Makito X Series. Administrators of multiple Makito X Series devices can use Haivision EMS to manage activities such as rebooting and upgrading the software and monitoring the status of devices for large installed bases. The EMS server managing may be in one facility while the devices being managed are in another facility.

Device unpairing is achieved by running the `emspair unpair` command. The current EMS agent state can be queried with the `emspair status` command.

- If the device is in `UNPAIRED` state, the `unpair` command has no effect.
- If device is in `PAIRED`, `CONNECTING` or `CONNECTED` states, the `unpair` command will attempt to communicate the intention to the EMS server immediately (if `CONNECTED`) or upon next successful connection. The EMS server will then proceed with removing the device registration and instructing the device to erase local pairing information.
- If the `-f` (force) flag is specified, the device will immediately inform the EMS server that it wishes to unpair if it is in `CONNECTED` state. The device will proceed to disconnect and erase all local pairing information regardless of server response or current state.

> ⚠️ **Note**
>
> A Makito X Series device can only talk to a single EMS at a time.
> After a factory reset, the EMS service is disabled, and the Makito X Series device loses all of its locally stored pairing information and must be re-paired with an EMS server afterwards.

Synopsis

```
emspair <operation> [args]


emspair pair [-c <passcode>] [-h <host>] [-p <port>] [-k <seconds>] [-r <seconds>]
emspair unpair -f
emspair status
```

Actions

Action/ Operation	Option/ Argument	Description
pair	-c <passcode> -h <host> -p <port> -k <seconds> -r <seconds>	Pairs the Makito X Series device with an EMS server: Passcode to use for pairing operation Overrides server host address Overrides server host port Override keepalive period Override reconnect delay period
unpair	-f	Unpairs the Makito X Series device from the EMS server: Forces unpairing

Action/ Operation	Option/ Argument	Description
status		Queries agent status

Examples

```
# emspair pair -c CIqn9+kFUncKDDEwLjY1LjExLjE4NxCzRVJkCkBmZTBlMD
A1ZGYyNzM3MmI4MmY0Njc1ODUzZGQ3MDhhZDk4MWE2NGJjNDEyODliNDNlMDAxYzJjNTJmMmZhODZhEi
A4N2YyM2ZkNi1kNGEyLWExNGYtNzNhZi0yMjliNmRiZA==


Pairing configuration:
----------------------
Expires: Sun Jul 28 16:55:38 2019


Server: 10.65.11.187:8883
---------------------
* Starting operation...
* Waiting for completion...
* Operation completed successfully!
Status Report:
---------------------
Last State: PAIRED
Server: 10.65.11.187:8883
Device ID: 26637ed0-7a22-ab4f-71bf-baf4dc59
Enabled: Yes
Waiting To Unpair: No
```

```
# emspair unpair
* Starting operation...
* Waiting for completion...
* Operation completed successfully!
Status Report:
--------------------
Last State: UNPAIRED
Server: (None)
Device ID:
Enabled: Yes
Waiting To Unpair: No
```

```
#  emspair status
* Starting operation...
* Waiting for completion...
Status Report:
--------------------
Last State: PAIRED
Server: 10.66.131.132:8883
Device ID: 37a1de75-4aac-bf4f-70bf-ee7f66dc
Enabled: Yes
Waiting To Unpair: No
```

```
#   emspair status
* Starting operation...
* Waiting for completion...
Status Report:
---------------------
Last State: CONNECTED
Server: 10.65.11.187:8883
Device ID: bcda955f-15f2-b14f-67af-497000ca
Enabled: Yes
Waiting To Unpair: No
```

```
# emspair status
* Starting operation...
* Waiting for completion...


Status Report:
---------------------
Last State       : CONNECTED
Server           : 10.65.130.149:8883
Device ID        : 24adb057-a3b2-cc4f-4abf-933cd63a
Enabled          : Yes
Waiting To Unpair: No
Keepalive        : 3 sec


Reconnect Delay 5 sec
```

Related Topics

- **Pairing the Decoder with Haivision EMS**

ethercfg

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

When a Makito X Series device 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.
```

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 Makito X Series devices. Status information can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

It also displays the Firmware Build ID and Build Time as well as the serial number for the unit.

> ✅ **Tip**
>
> The MAC Address is shown on the Network page (Web Interface) and in the System Snapshot.

Synopsis

```
haiversion
```

Actions

N/A

Parameters

N/A

Example

```
# haiversion

Displays information about the hardware and software components.
Card Type              : "Makito X4 SDI Encoder"
Part Number            : B-MX4E-SDI4
Serial Number          : HAI-031809050009
MAC Address            : 5c:77:57:00:b3:dc
Firmware Version       : 1.0.0-42
Firmware Date          : "Apr 12 2019"
Firmware Time          : "15:28:39"
Hardware Version       : C
Hardware Compatibility : -002G
CPLD Version           : 4 (Official, Internal flash)
Boot Version           : "U-Boot 2020.06 (Feb 26 2020 - 10:41:13)-Makito4K"
```

Related Topics

- **Viewing System Status Information**

ipconfig

The `ipconfig` command is used to view and set the parameters that specify the IP (IPv4) networking context for Makito X Series devices, 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.

When DHCP is enabled, you can configure the `DHCP Vendor Class ID` (option 60), which is set by default, for example, "Haivision Makito X4 Encoder" or "Haivision Makito X4 Decoder". This allows IT departments to identify Makito X Series devices on their networks.

Also, if there is a slow DHCP server at the client's site, you may find it useful to adjust the `DHCP Client Retries` and `Timeout` options to obtain a DHCP address. These options were added to circumvent issues caused by the unit's booting before having obtained a valid DHCP address.

> ⚠ **Note**
>
> Enabling the Multicast DNS (mDNS) protocol allows mDNS applications such as the Safari Web browser to automatically find the encoder. In Safari, navigate to Bookmarks and then select Bonjour to see the Makito X Series device listed.

> 🛑 **Warning**
>
> If you are connecting to the Makito X Series 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 [iface]
ipconfig configure [iface]
ipconfig renew
ipconfig release
ipconfig disable [iface]
```

Actions

Action	Description
display	Displays the current IP configuration for the specified network interface. See **Parameters** below for interface.
configure	Configures IP settings for the specified network interface. See **Parameters** below for interface.
renew	Renews the DHCP address lease.
release	Releases the current DHCP address lease.

Action	Description
disable	Disables IPv4 functionality for the specified network interface. See **Parameters** below for interface. Use to configure the device to use IPv6 network only. ⚠️ **Note** You cannot disable IPv4 if IPv6 is already disabled.

Parameters

Parameter	Default	Description/Values
iface	eth0	Allows for multiple network interfaces. Select the interface to view and configure. Either eth0 or eth1.

Examples

```
# ipconfig display
```

Returns current IP settings for the 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

> ✅ **Tip**
>
> For descriptions of the parameters that follow, see Network Settings.

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

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-hevc:~$ 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 device.

> ⚠ **Note**
>
> Multiple licenses may be installed on the same device at the same time.

Synopsis

```
license list
license info <feature.lic/all> [-w]
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`.
info	Displays options information for license file(s). -w Display warnings (*W)
view	Displays the content of the specified license file.
install	Installs the specified (uploaded) license. ⚠ **Note** 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):
  HAI-031907070046.lic
```

```
# license view HAI-031907070046.lic
```

Displays the contents of the specified license.

```
# license verify HAI-031907070046.lic
```

Verifies the specified license:
```
Verifying license /usr/share/haivision/licenses/HAI-031907070046.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.

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

> ⚠ **Note**
>
> The `messages` command can only be used by 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-install 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**

nmcfg

The `nmcfg` (Network Management Configuration) command is used by system administrators or GUI/ Web interface applications in the configuration of SNMP for certain Makito X series devices. The `nmcfg` s cript 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).

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.

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	Defines the access permissions for the community or the user. ⓘ **Info** 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. Both IPv4 and IPv6 are enabled.

```
# nmcfg
snmp agent
-------------- ----------------
status running
transport udp:161
         udp6:161

system parameter       value
-------------------- -----------------------------------------
engineid             0x80001f88035c775700b3dc
contact              <undefined>
location             <undefined>

model perm/group       level  user/community      af   source
----- --------------- ------ -------------------- ---- ---------------
v2c   rw              noauth admin                ipv4 localhost
v2c   rw              noauth admin                ipv4 localnet
v2c   rw              noauth admin                ipv6 ::1
v2c   rw              noauth admin                ipv6 fe80::/10
v2c   ro              noauth public               ipv4 localnet
v2c   ro              noauth public               ipv6 fe80::/10

# nmcfg system define contact "myname <myname@example.org>"
Starting SNMP Service

# nmcfg system define location "Media Lab"
Starting SNMP Service

# nmcfg community permit admin rw 198.51.100.122
Starting SNMP Service
```

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. Both IPv4 and IPv6 are enabled.

```
# nmcfg
snmp agent
-------------- ----------------
status          running
transport       udp:161
                udp6:161

system parameter        value
-------------------- -----------------------------------------
engineid             0x80001f88035c775700b3dc
contact              <undefined>
location             <undefined>

model perm/group        level  user/community     af   source
----- ---------------- ------ ------------------ ---- ---------------
v2c   rw               noauth admin              ipv4 localhost
v2c   rw               noauth admin              ipv4 localnet
v2c   rw               noauth admin              ipv6 ::1
v2c   rw               noauth admin              ipv6 fe80::/10
v2c   ro               noauth public             ipv4 localnet
v2c   ro               noauth public             ipv6 fe80::/10

# 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
Starting SNMP Service

# nmcfg
snmp agent
-------------- ----------------
status          running
transport       udp:161
                udp6:161
```

```
system parameter       value
---------------------- ------------------------------------------
engineid               0x80001f88035c775700b3dc
contact                joe net <jnet@example.org>
location               Media Lab

model perm/group       level  user/community       af   source
----- ---------------- ------ -------------------- ---- ---------------
usm   guest            auth   guest                -    -
usm   administrator    priv   joenet               -    -
usm   operator         priv   johnsmith            -    -


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. 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.

Related Topics

- **messages** (CLI command)

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 (link below).
>
> Passwords can be up to 80 characters long. See "Password Requirements" under "Changing Your Password" (link below) for the supported character set. Password policies set by the administrator may enforce the selection of strong passwords.

Synopsis

```
passwd
```

Actions

N/A

Parameters

N/A

Examples

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

Related Topics

- **account**
- **Changing Your Password**
- **Role-based Authorization**
- **Managing User Accounts**

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.

> ℹ️ **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 https set hsts=no
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.
https set	Enables HTTP Strict Transport Security (HSTS). When enabled, HSTS forces web browsers to only contact the Web interface over HTTPS, instead of using HTTP.
pname/all get	Displays the policy information for either the policy (i.e., password, session, or crypto) or the Makito X4.

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(Deprecated): All management cryptography follows the guidelines of NIST Special Publication 800-52 Rev 1. • SP800-52r2 ℹ **Note** Either selection reinforces security for all management functions of the device in terms of cryptography. This setting takes effect upon the next reboot.
sslv3	See Note	ℹ **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
https	No	ℹ **Note** When preparing a Makito X4 device for hardening, you need to enable the HSTS policy.
password		
quality	Basic	Specifies the required password strength, either: • Basic • Strong
minlen	6	Specifies the minimum password length. Range: 6–40
minuppers	See Note	ℹ **Note** Default is N/A if quality=Basic, 0 if quality=Strong.

Parameter	Default	Description/Values
mindigits	See Note	**ℹ Note** Default is N/A if quality=Basic, 0 if quality=Strong.
minsymbols	See Note	**ℹ 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 Makito X4, and prevents users from changing their password to any password used within the specified history count. Range: 5 –400
session		
autologout	No	Enables or disables auto-logou: Yes, No
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 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 Makito X4 such as:
```
Crypto:
  Compliance  : NDPP11
  SSLv3       : Disallowed
  TLSv1.0     : Yes
  TLSv1.1     : Yes
  TLSv1.2     : Yes
HTTPS:
  HSTS        : Yes
Password:
  Quality     : Strong
  MinLen      : 10
  MinUppers   : 1
  MinDigits   : 0
  MinSymbols  : 1
  Remember    : 5
  Expiry      : Yes
  Lifetime    : 30 days
Session:
  Autologout  : Yes
  IdleTimeout : 20 minutes
```

Related Topics

- **Managing Security Policies**
- **Policy Settings**

pubkey

The pubkey command is used to manage your account's authorized SSH public keys. You must first get the public key of your SSH client. Note that this only applies to SSH CLI access to Makito X devices.

> ⚠ **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 Makito X.
remove	Removes the specified public key file from the Makito X.
list	Lists the public key files currently loaded on the Makito X.

Examples

```
# pubkey add makito.pub
```
Uploads the public key file makito.pub to the Makito X.

```
# 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**
- **Managing Public Key Authentication**

reboot

The reboot command is used to turn off and restart Makito X devices. Any unsaved configurations will be lost. The unit will restart with the saved startup configuration.

> ⚠ **Note**
>
> The reboot command can only be used by an administrator.

Synopsis

```
reboot
```

Example

```
# reboot
```

Reboots the Makito X.

> ⚠ **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**

service

For security purposes, you may need to stop one or more network services from accessing the Makito X device. The `service` command is used to enable and disable the following network services: all, or (depending on the platform) EMS, HTTP, ONVIF, (serial) PASSTHROUGH, RTSP, SAP (decoder only), SNMP, SSH, TALKBACK, TELNET, and VF.

> ⚠️ **Caution**
>
> Take care not to disable *all* network services; you must at least keep `http` (Web interface), `telnet` , or `ssh` active. Otherwise you will lose access control to the unit, and the only way to re-enable these services is by a Factory Reset.

Synopsis

```
service svcname action
```

where (depending on the platform):
svcname can be: all, ems, http, onvif, passthrough, rtsp, sap, 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 all status
```

Displays information about all services (ex: Makito X Decoder), such as:

```
ems service is currently enabled
ems service is enabled at system startup
http service is currently enabled
http service is enabled at system startup
sap service is currently disabled
sap service is disabled at system startup
snmp service is currently enabled
snmp service is enabled at system startup
ssh service is currently enabled
ssh service is enabled at system startup
talkback service is currently disabled
talkback service is disabled at system startup
telnet service is currently enabled
telnet service is enabled at system startup
```

```
# service
```

Displays usage information for the service command (ex: Makito X1 Rugged Encoder).

```
Usage: service svcname action
svcname can be: all, ems, http, onvif, passthrough, rtsp, snmp, ssh, telnet


action can be:
start   activates the service right away and configures the unit so that
        the service will be started automatically when the unit is rebooted.


stop    de-activates the service right away 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 and startup status of the service.
```

```
# service telnet stop
```

Stops telnet connection to the Makito X.

```
# service telnet restart
```

Re-starts telnet connections to the Makito X.

Related Topics

- **Enabling and Disabling Network Services**
- **Services Settings**

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**

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 X4 encoder.

Topics in This Chapter

- **Audio/Video Interface Specifications**
- **Video Encoding**
- **Audio Encoding**
- **Advanced Features**
- **ISR Metadata (Optional)**
- **Network and Management Interfaces**
- **Chassis Options**
- **Power Connector Pinouts (Single- and Dual-Height Chassis)**
- **Regulatory/Compliance**
- **Closed Captioning**

Audio/Video Interface Specifications

Video Interfaces   Audio Interfaces

Makito X4 Video Interfaces (Quad BNC Inputs)		
SD-SDI	SMPTE 259M-C	270 Mbps Interface, 720 x 480i video format (29.97/30 Hz) 720 x 576i (25 Hz)
ED-SDI	SMPTE 334	720 x 480p video format (29.97/30/59.94/60 Hz) 720 x 576p (25/50 Hz)
HD-SDI	SMPTE 292M	1,485 Gbps interface
	SMPTE 274M	1920 x 1080 video format 1920x1080i (23.98/24/25/29.97/30 Hz) 1920x1080p (23.98/24/25/29.97/30 Hz)
	SMPTE 296M	1280 x 720 video format 1280x720p (50/59.94/60 Hz)
3G-SDI	SMPTE 424M (Level A Only)	3 Gbps interface
	SMPTE 425M	1080p60 video format 1920x1080p (50/59.94/60 Hz)
6G-SDI	SMPTE 2081 (1 input only)	Up to 3840 x 2160p (25/29.97/30 Hz)
12G-SDI	SMPTE 2082 (1 input only)	Up to 3840 x 2160p (50/59.94/60 Hz)
Impedance		
SDI	75 Ohms	

Video Interfaces   **Audio Interfaces**

Makito X4 Audio Interfaces (16-bit PCM Audio)		
Up to 32 channels of embedded audio per blade, in (stereo) 16 channel pairs. The channel pair sources are: sdi1ch1&2, sdi1ch3&4, sdi1ch5&6 ... sdi1ch15&16 sdi2ch1&2, sdi2ch3&4, sdi2ch5&6 ... sdi2ch15&16 sdi3ch1&2, sdi3ch3&4, sdi3ch5&6 ... sdi3ch15&16 sdi4ch1&2, sdi4ch3&4, sdi4ch5&6 ... sdi4ch15&16		
Note When in mono mode, each audio encoder can only encode one left or right channel. In this case, only 16 mono channels can be encoded.		
Digital Embedded Audio		
SD-SDI	SMPTE-272M	Formatting AES/EBU Audio and Auxiliary Data into Digital Video Ancillary Data Space

| HD/3G-SDI | SMPTE 299M | Formatting 24-Bit Digital Audio Format for SMPTE Bit-Serial Interfaces |

Video Encoding

Makito X4 Video Encoding – H.264 AVC/H.265 HEVC (MPEG-4 Part 10)	
SD/ED/HD/3G-SDI Input Resolutions	3840x2160p 60/59.94/50/30/29.97/25 Hz 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 720x480/576i 60/59.94/50 Hz (interlaced shown in fields per second) ℹ **Note** For supported video encoding resolutions, see Supported Video Encoding Input and Downscale Resolutions.
H.264/AVC VIDEO ENCODING	• MPEG-4 AVC part 10 / ISO/IEC 14496-10 • Baseline, Main, and High Profiles • Up to Level 5.2 (1080p60) and lower intermediate levels • I, IP, IBP, IBBP, IBBBP and IBBBBP Framing • 8-bit or 10-bit pixel depth • Chroma sub-sampling 4:2:0 or 4:2:2 • Bitrates SD/HD from 32 kbps to 30 Mbps ❗ **Important** The Makito X4 accepts interlaced SDI video (1080i, 576i, 480i) and can encode and output 1080i, 576i, and 480i HEVC streams. However, in H.264/AVC, it can only encode and output progressive (non-interlaced) content. The Makito X4 cannot encode and stream 1080i/576i/480i in H.264.
H.265/HEVC VIDEO ENCODING	• ISO/IEC 23008-2 • I, IP, IBP, IBBP, IBBBP and IBBBBP Framing • Main Profile Up to Level 5.1 • 8-bit or 10-bit pixel depth • Chroma sub-sampling 4:2:0 or 4:2:2 • Bitrates SD/HD from 32 kbps to 30 Mbps
Rate Control	Capped variable bit rate (CVBR) Constant bit rate (CBR)
Encoding Latency	Less than 60ms (H.264 encoder at 720p60, 6Mbps) Less than 50ms (HEVC encoder at 720p60, 6 Mbps) ℹ **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, High, High10 and High422 Profiles • Up to Level 5.2 and lower Intermediate Levels • Configurable Group of Picture (GOP) size • Configurable frame rate

Makito X4 Video Encoding – H.264 AVC/H.265 HEVC (MPEG-4 Part 10)	
Compression Standards (HEVC)	• H.265/HEVC • ISO/IEC 23008-2 • Main, Main10 and Main422-10 Profiles • Up to Level 5.1 (1080p60 @ 15 Mbps) • Up to Level 5.2 and lower Intermediate Levels • Configurable Group of Picture (GOP) size • Configurable frame rate • Deblocking filter
Macro-block processing limitation	The aggregate pixel processing power for all video encoding engines cannot exceed either: • 4 x 1920x1080p60 or • 1 x 3840x2160p60 or • 497,664,000 pixels per second
Video Encoding Limits	• Up to 3840x2160p60

Supported Video Encoding Input and Downscale Resolutions

Encoded Output Resolutions		Input Resolutions and Frame Rates																						
		3840x2160p							1920x1080p						1920x1080i		1280x720p						720x480i	720x576i
Name	Resolution	60/59.97	50	30	29.97	25	24	23.98	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	25
UHDp	3840x2160p	1	1	1	2	2	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
HD 1080p	1920x1080p	2	2	4	4	4	4	4	4	8	4	8	8	8	4	4	-	-	-	-	-	-	-	-
HD 1080i	1920x1080i	-	-	-	-	-	-	-	-	-	-	-	-	-	8	8	-	-	-	-	-	-	-	-
3/4 HD 1080p	1440x1080p	2	2	4	4	4	4	4	5	8	5	8	8	8	4	4	-	-	-	-	-	-	-	-
3/4 HD 1080i	1440x1080i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1/2 HD 1080p	960x1080p	2	2	4	4	4	4	4	8	8	8	8	8	8	4	4	-	-	-	-	-	-	-	-
1/2 HD 1080i	960x1080i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
HD 720	1280x720p	2	2	4	4	4	4	4	8	8	8	8	8	8	4	4	8	8	8	8	8	8	-	-
3/4 HD 720	960x720p	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8	8	8	8	8	8	-	-
1/2 HD 720	640x720p	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8	8	8	8	8	8	-	-
SD 480p	720x480p	2	2	4	4	4	4	4	8	8	-	-	8	8	4	-	8	8	-	-	8	8	4	-
SD 480i	720x480i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-
SD 576p	720x576p	-	2	-	-	4	4	4	-	-	8	8	8	-	-	4	-	-	8	8	8	-	-	4
SD 576i	720x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8
4CIFp	704x576p	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
4CIFi	704x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

3/4 D1 NTSCp	540x480p	2	-	4	4	-	4	4	8	8	-	-	8	8	4	-	8	8	-	-	8	8	4	-
3/4 D1 NTSCi	540x480i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3/4 D1 PAL	540x576p	-	2	-	-	4	-	-	-	-	8	8	8	-	-	-	-	8	8	8	-	-	4	
3/4 D1 PAL	540x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
70% VGA	448x336p	2	2	4	4	4	4	4	8	8	8	8	8	8	4	4	8	8	8	8	8	8	4	4
Half-D1 NTSC	352x480i/p	2	2	4	4	4	4	4	8	8	-	-	8	8	-	-	8	8	-	-	8	8	-	-
Half-D1 PAL	352x576i/p	-	-	-	-	-	-	-	-	-	8	8	8	-	-	-	-	8	8	8	8	-	-	
CIF	352x288i/p	2	2	4	4	4	4	4	8	8	8	8	8	8	-	-	8	8	8	8	8	8	-	-

Legend:

8	Up to 8 encoding cores/instances supported
4	Up to 4 encoding cores/instances supported
2	Up to 2 encoding cores/instances supported
1	Only a single encoding core/instance supported

Resolutions marked "-" are not supported.

Audio Encoding

Audio Encoding – MPEG AAC [1]	
Audio Channels	Up to 32 embedded audio channels in channel pair groups per blade (SDI)
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
Compression Standards	MPEG-2 AAC-LC ISO/IEC 13818-7 MPEG-4 AAC-LC ISO/IEC 14496-3

Advanced Features

Advanced Features
Multi-bitrate (MBR) Encoding
HD/SD De-interlacing
Built-in Downscaling
EIA-608-B/SDI and EIA-708-B/SDI Closed Captioning
Forward Error Correction (FEC) using PRO-MPEG FEC for TS over RTP streams
AES Encryption 128-bit or 256-bit with Furnace systems or SRT
Aspect ratio configuration
AFD (Active Format Description) for SDI

ISR Metadata (Optional)

Metadata Inputs   Metadata Processing/Output Metadata

Metadata Inputs

- CoT to KLV Conversion
- KLV or CoT over IP/UDP
- KLV Capture and Streaming over SD-SDI/HD-SDI/3G-SDI (SMPTE 336)
- KLV or CoT Capture and Streaming over Serial (Makito X4 Rugged only, RS-232 or RS-422)
- SMPTE 336M Compliant
- MISB 0601.11 Compliant
- MISB 0604.2 Compliant, supporting:
  - Synchronous and Asynchronous formats
  - High precision Time Code insertion

Metadata Inputs   **Metadata Processing/Output Metadata**

Metadata Processing/Output Metadata

- CoT relay to another IP device
- KLV over SDI Metadata Rate Decimation
- KLV Metadata Processing (SMPTE 336, MISB 0601, 0102 and 0605 support)
    - MISB 0601 UAS and MISB 0102 Security KLV Tag Filtering
    - Mission ID Insertion and Security Data Set Insertion
- Time Code Support (SMPTE 12M)
- Closed Captioning (SMPTE 334-1/2)
- STANAG 4609 Stream Compliant

Network and Management Interfaces

IP Network Interfaces   Management Interfaces

IP Network Interfaces

Standard:	• Single Ethernet 10/100/1000 • Base-T, auto-detect, Half/Full-duplex • Unicast streaming IPv4/IPv6 • Multicast streaming (IGMPv3, Internet Group Management Protocol & IPv6) • Multiple unicast streaming • 10G SFP Port (future use)
H.264 Streaming Protocols:	• MPEG Transport Stream • Secure Reliable Transport (SRT) • TS over SRT, UDP or RTP
HEVC Streaming Protocols:	• MPEG Transport Stream • Secure Reliable Transport (SRT) • TS over SRT, UDP or RTP

IP Network Interfaces   **Management Interfaces**

Management Interfaces

Physical Interface:	• IP/Ethernet (IPv4 and IPv6)
Management Protocols:	• HTTPS (Web browser) • Command line over SSH, Telnet • SFTP/TFTP/SCP Client/Server • SNMP v3

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-MX4E-SDI4)	
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	12 VDC Nominal, 18W (each blade) ℹ️ **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)

Compatible with Haivision MB6X and MB21X multi-blade chassis.

Related Topics

- [Power Connector Pinouts (Single- and Dual-Height Chassis)](#)

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.)

MB6X - 6-Blade Chassis (#F-MB6X-RAC, #F-MB6X-MED, #F-MB6X-DC)	
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
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

MB21X - 21-Blade Chassis (#F-MB21X-R)[1]	
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
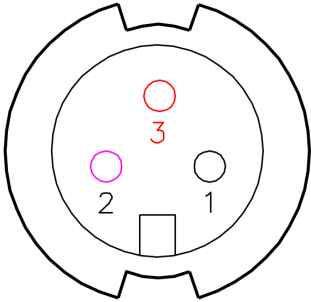
Rugged Appliance

Makito X4 Rugged Encoder (#S-MX4E-R-SDI4-ISR)	
Dimensions	66mm H x 146.2mm W x 185.7mm D (2.675" H x 5.755" W x 7.31" D)
Weight	1.93 kg (4.25 1bs.)
Power	28 VDC Nominal, 25W (MIL-STD-704F and MIL-STD-1275E compliant)
Temperature	Operating: -40°C to 71°C (-40°F to 160°F) Non-operating: -45°C to 85°C (-49°F to 185°F)
Relative Humidity	0-100% condensing
IP rating	IP67 ⚠ **Caution** The IP67 rating only applies when the connectors are mated. Otherwise the usage of dust cap connectors (provided by Haivision, shown in the following figures) is required.
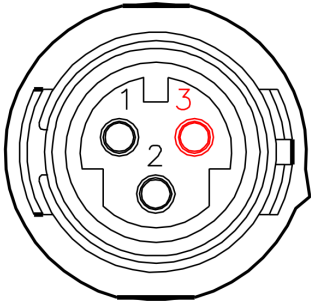
Power Connector Pinouts (Single- and Dual-Height Chassis)

The power connectors for the Single-Height and Dual-Height Chassis have the following pinouts:

Single-Height - Power Connector

Pin #	Description (Conxall P/N 16282-3SG-318)	
1	Reserved / Not Connected	
2	Ground	
3	VCC=+12VDC	

Dual-Height - Power Connector

Pin #	Description (Hirose P/N HR30-6R-3P(71))	
1	Reserved / Not Connected	
2	Ground	
3	12VDC (+V)	

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 X4 encoder supports the capture of EIA-608 and EIA-708 closed captions from the HD/SD-SDI video input and transports it within the video elementary stream of the MPEG-2 Transport Stream.

The EIA-608 and EIA-708 captions are encapsulated in a Caption Description Packet (CDP), as described in SMPTE-334-2, within the VANC as mentioned in SMPTE 334-1. The Caption information is multiplexed and transported as per ATSC A/72 Part 1:2008 (ATSC A/53 Part 4:2007) in a CC SEI NAL. The CDP consists 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.

The CDP also includes the Caption Service Descriptor (CSD) (as defined in ATSC A/65). The caption services stored in the CSD are announced in the MPEG-2 TS Program Map table (PMT).

The following block diagram shows the workflow for video and CC data into the encoder.
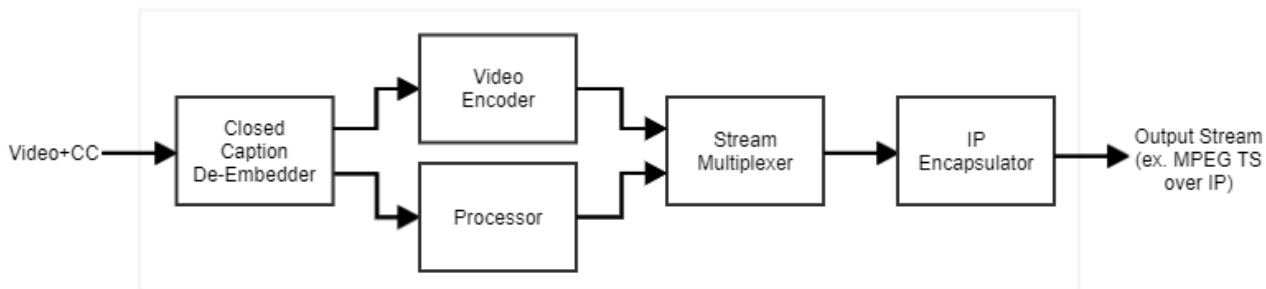
With the support of EIA-708, ATSC A/72 mandates a dedicated link bitrate of 9600 bits/sec (1200 bytes/sec or 20 bytes per frame for a p60 SDI signal). Of the 9600 bits/sec, 960 bits/sec are reserved for EIA-608 captions. 8640 bits/s are dedicated to 708-CC. This is a dedicated channel, so it has to be filled with filler data if no captioning information is present.

> ℹ **Note**
>
> Analog EIA-608 Line 21 Closed Captioning is only supported on the Makito X4 Rugged encoder (Composite input). See Makito X4 Rugged Closed Captioning

Makito X4 Rugged Closed Captioning

The Makito X4 Rugged 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 following figure). The Makito X4 Rugged encoder supports transport of all these services. [Note that Closed Captioning as specified by EIA-608-B does not exist over PAL.]
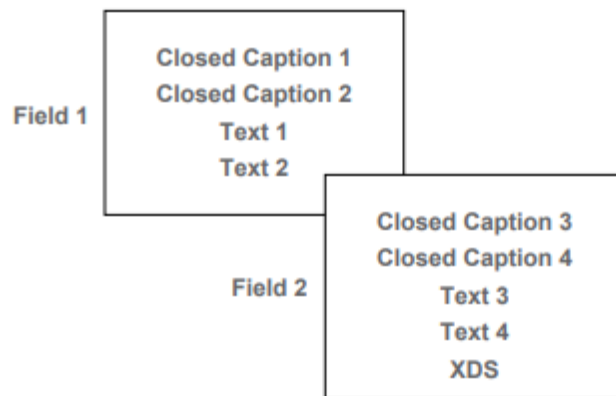
Line 21 of each field can contain up to 2 bytes of information, which can be used by any of the above services (not simultaneously but rather successively). With NTSC video at 30fps, the maximum EIA-608-B mandated throughput represents:

```
2 bytes x 2 Fields x 30fps x 8 bit/byte = 960 bps
```

Open Source Software Credits

This appendix lists the Open Source software packages currently deployed on the Makito X4 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	Included in X4 version
Linux kernel	5.4.0	Linux Kernel	GPL v2, June 1991	1.0
Linux-PAM	1.3.0	Linux Pluggable Authentication Module	Permissive free software license or GPLv2; 1996-2005; Morgan, Levine, Kukuk, Tricaud & Mraz	1.0
attr	2.4.47	Extended filesystem attributes	GPL v2, June 1991	1.0
bash	4.3.47	Bourne Again Shell - Posix.2 Shell	GPL v3, June 2007	1.0
beecrypt	4.2.1	Cryptography library	GPL v2, June 1991	1.0
busybox	1.24.1	Common Unix utilities	GPL v2, June 1991	1.0
chkconfig	1.3.30c	Service run level configuration	GPL v2, June 1991	1.0
chrony	3.3.2	Alternate Network Time Protocol (NTP)	GPL v2, June 1991	1.0
coreutils	8.25	Basic shell, file and text manipulation	GPL v3, June 2007	1.0
cracklib	2.8.18	Password resilience library	LGPL v2.1, June 1999	1.0
cron	3.0pl1	Time base job scheduler	Permissive free software license; 1988, 1990, 1993 Paul Vixie	1.0
debianutils	4.5.1	Misc. utilities	Small General Public License, February 1988, G. Maol, C. Adams, L. Knoll, R. Carr	1.0
dhcp	4.4.1	DHCP client	Mozilla Public License v2.0, 1995-2003, 2004-2018 Internet Software Consoltium (ISC), ISC inc.	1.0
dos2unix	7.4.0	Text file conversion	BSD styled license, 1994-1995 B Lin, 1998 J Wuebben C Wurll, 2009-2018 E Waterlander	1.0
dpkg	1.16.0	Debian Package Manager	GPL v2, June 1991	1.0
ethtool	4.19	Network interface configurator	GPL v2, June 1991	1.0
ffmpeg	4.3.0	Multimedia framework (Decoder only)	LGPL v2.1, June 1999	1.0
gawk	4.1.3	GNU AWK - Pattern scanning and processing	GPL v3, June 2007	1.0

Package	Version	Description	License	Included in X4 version
gdb	7.11.1	GNU Debugger	GPL v2, June 1991	1.0
ifupdown	0.8.19	Network Interface configurator	GPL v2, June 1991	1.0
iperf	2.0.5	Internet bandwidth measurement tool	Copyright (c) 1999-2007, The Board of Trustees of the University of Illinois	1.0
iperf3	3.1	Internet bandwidth measurement tool	Permissive free software license - 2014-2016 University of California	1.0
iproute2	4.16	Linux TCP/IP traffic control	GPL v2, June 1991	1.0
jpeg	8b	JPEG Software Tools	Permissive free software license - 2010 Independent JPEG group	1.0
lftp	4.8.3	File Transfer Program	GPLv3, June 2007	1.0
libcap	2.25	Library for setting/ getting Posix capabilities	Permissive free software license or GPLv2	1.0
libevent	2.1.8	Event notification library	3-clause ("modified") BSD License	1.0
libpcap	1.9.0	User-level packet capture	BSD	1.0
lighttpd	1.4.41	Lightweight open-source Web server	Permissive free software license, Jan Kneshcke, 2004	1.0
mDNSResponder	320.10.80	Multicast DNS Responder (Bonjour component)	Apache 2.0 Three-Clause BSD National ICT Australia Limited (NICTA) Public Software	1.0
ncurses	5.5	Text-base UI library	Permissive free software license	1.0
net-snmp	5.7.3	Simple Network Management Protocol	Multiple BSD Licenses	1.0
net-tools	1.60	Network tools	GPL v2, June 1991	1.0
netkit-ftp	0.17	File Transfer Protocol	Regents of the University of California	1.0
netkit-telnet	0.17	Telnet	Regents of the University of California	1.0
ntp	4.8.2-p10	Network Time Protocol	Permissive free software license, University of Delaware	1.0
openresolv	3.9.0	DNS management framework	2-clause BSD license, present since v1.0 but inactive (not used) https://www.freebsd.org/copyright/freebsd-license.html	1.0
openssh	7.3p1	Open SSH	Multiple BSD style licenses	1.0
openssl	1.0.2r	Open Secure Socket Layer	Dual OpenSSL / SSLeahy	1.0
pcre	8.39	Perl Compatible Regular Expression Library	BSD License	1.0

Package	Version	Description	License	Included in X4 version
popt	1.16	Command Line Parsing Library	BSD License	1.0
procps	3.2.8	Process reporting utilities	GPL v2, June 1991	1.0
readline	6.1	Command Line Editing Library	GPL v3, June 2007	1.0
rpm	4.4.2.3	RPM Package Manager	Dual GPL v2 - June 1991 and LGPL v2 - June 1991	1.0
sed	4.2.2	Stream Editor	GPL v3, June 2007	1.0
shadow	4.6	Shadow Passwords	Permissive free software license	1.0
sudo	1.9.5p2	Privilege modification	Permissive software license, Copyright (c) 1994-1996, 1998-2021, T. Miller et al.	1.0
sysstat	10.0.0	Performance monitoring	GPL v2, June 1991	1.0
tcpdump	4.9.1	Network monitoring and data acquisition	Permissive free software license	1.0
tftp-hpa	0.43	TFTP server	Permissive free software license	1.0
u-boot	2018.1	U-Boot boot loader	GPL v2, June 1991	1.0
UDT	`4.11`	UDP-based Data Transfer	Permissive free software license. See Third Party License Information	1.0
zlib	1.2.11	Compression library	Permissive free software license, Jean-Loup Gailly	1.0

Haivision is grateful to the following organizations for making available their Open Source software packages:

Package	Version	Description	License	Included in X4 version
`Linux kernel`	4.14.0	Linux Kernel	GPL v2, June 1991	1.0
`Linux-PAM`	1.3.0	Linux Pluggable Authentication Module	Permissive free software license or GPLv2; 1996-2005; Morgan, Levine, Kukuk, Tricaud & Mraz	1.0
attr	2.4.47	Extended filesystem attributes	GPL v2, June 1991	1.0
`bash`	4.3.30	Bourne Again Shell - Posix.2 Shell	GPL v3, June 2007	1.0
`beecrypt`	4.2.1	Cryptography library	GPL v2, June 1991	1.0

Package	Version	Description	License	Included in X4 version
busybox	1.24.1	Common Unix utilities	GPL v2, June 1991	1.0
chkconfig	1.3.30c	Service run level configuration	GPL v2, June 1991	1.0
chrony	3.3.2	Alternate Network Time Protocol (NTP)	GPL v2, June 1991	1.0
coreutils	8.25	Basic shell, file and text manipulation	GPL v3, June 2007	1.0
cracklib	2.8.18	Password resilience library	LGPL v2.1, June 1999	1.0
cron	3.0p11	Time base job scheduler	Permissive free software license; 1988, 1990, 1993 Paul Vixie	1.0
debianutils	4.5.1	Misc. utilities	Small General Public License, February 1988, G. Maol, C. Adams, L. Knoll, R. Carr	1.0
dhcp	4.4.1	DHCP client	Mozilla Public License v2.0, 1995-2003, 2004-2018 Internet Software Consoltium (ISC), ISC inc.	1.0
dos2unix	7.4	Text file conversion	BSD styled license, 1994-1995 B Lin, 1998 J Wuebben C Wurll, 2009-2018 E Waterlander	1.0
dpkg	1.16.0	Debian Package Manager	GPL v2, June 1991	1.0
ethtool	4.19	Network interface configurator	GPL v2, June 1991	1.0
gawk	4.1.3	GNU AWK - Pattern scanning and processing	GPL v3, June 2007	1.0
gdb	7.11	GNU Debugger	GPL v2, June 1991	1.0
ifupdown	0.8.19	Network Interface configurator	GPL v2, June 1991	1.0
iperf	2.0.5	Internet bandwidth measurement tool	Copyright (c) 1999-2007, The Board of Trustees of the University of Illinois	1.0
iperf3	3.1	Internet bandwidth measurement tool	Permissive free software license - 2014-2016 University of California	1.0
iproute2	4.16	Linux TCP/IP traffic control	GPL v2, June 1991	1.0
jpeg	8b	JPEG Software Tools	Permissive free software license - 2010 Independent JPEG group	1.0
lftp	4.8.3	File Transfer Program	GPLv3, June 2007	1.0

Package	Version	Description	License	Included in X4 version
`libcap`	2.25	Library for setting/getting Posix capabilities	Permissive free software license or GPLv2	1.0
`libevent`	2.1.8	Event notification library	3-clause ("modified") BSD License	1.0
`libpcap`	1.9.0	User-level packet capture	BSD	1.0
`lighttpd`	1.4.41	Lightweight open-source Web server	Permissive free software license, Jan Kneshcke, 2004	1.0
`mDNSResponder`	320.10.80	Multicast DNS Responder (Bonjour component)	Apache 2.0 Three-Clause BSD National ICT Australia Limited (NICTA) Public Software	1.0
`ncurses`	5.5	Text-base UI library	Permissive free software license	1.0
`net-snmp`	5.7.3	Simple Network Management Protocol	Multiple BSD Licenses	1.0
`net-tools`	1.60	Network tools	GPL v2, June 1991	1.0
`netkit-ftp`	0.17	File Transfer Protocol	Regents of the University of California	1.0
`netkit-telnet`	0.17	Telnet	Regents of the University of California	1.0
`ntp`	4.8.2-p10	Network Time Protocol	Permissive free software license, University of Delaware	1.0
`openssh`	7.3p1	Open SSH	Multiple BSD style licenses	1.0
`openssl`	1.0.2r	Open Secure Socket Layer	Dual OpenSSL / SSLeahy	1.0
`pcre`	8.39	Perl Compatible Regular Expression Library	BSD License	1.0
`popt`	1.16	Command Line Parsing Library	BSD License	1.0
`procps`	3.2.8	Process reporting utilities	GPL v2, June 1991	1.0
`readline`	6.1	Command Line Editing Library	GPL v3, June 2007	1.0
`rpm`	4.4.2.3	RPM Package Manager	Dual GPL v2 - June 1991 and LGPL v2 - June 1991	1.0
`sed`	4.2.2	Stream Editor	GPL v3, June 2007	1.0

Package	Version	Description	License	Included in X4 version
shadow	4.6	Shadow Passwords	Permissive free software license	1.0
sudo	1.8.28	Privilege modification	Permissive free software license - Free Software Foundation	1.0
sysstat	10.0.0	Performance monitoring	GPL v2, June 1991	1.0
tcpdump	4.9.1	Network monitoring and data acquisition	Permissive free software license	1.0
tftp-hpa	0.43	TFTP server	Permissive free software license	1.0
u-boot	2018.1	U-Boot boot loader	GPL v2, June 1991	1.0
UDT	4.11	UDP-based Data Transfer	Permissive free software license. See "Third Party License Information" (link below)	1.0
zlib	1.2.11	Compression library	Permissive free software license, Jean-Loup Gailly	1.0

Related Topics

- **Third Party License Information**

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