

HAIVISION



Makito X1 Rugged

Video Encoder

VERSION 1.3

18 Jun 2025

User's Guide

www.haivision.com

Edition Notice

© 2015-2025 Haivision. All rights reserved.

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

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

Edition Notice	2
About Haivision	2
Trademarks	2
Disclaimer	2
Contents	3
About This Document	6
Conventions	6
Typographic Conventions and Elements	6
Action Alerts	6
Getting Service Support	7
Introduction	9
Product Overview	9
Physical Description	11
MX1 Rugged v2 (#S-MX1E-R-V2-SDI1)	11
MX1 Rugged v2 (28V DC)	11
MX1 Rugged (#S-MX1E-R-SDI1)	12
LED Status Indicator	13
Resetting the MX1 Rugged	14
Default Network Settings	15
Getting Started with the Web Interface	16
Accessing the Encoder	17
Security Steps	17
Default Encoder IP Address	18
Role-based Authorization	19
Signing In to the Web Interface	20
Exploring the Web Interface	23
Changing Your Password	25
Password Requirements	27
Signing Out	27
Managing the Encoder	28
Configuring Video Encoders	30
Video Encoders List View	30
Configuring Video Encoder Settings	32
Video Encoder Settings	35
Video Encoder Statistics	41
Configuring Audio Encoders	43
Audio Encoders List View	43
Configuring Audio Encoder Settings	44
Audio Encoder Settings	46
Audio Encoder Statistics	47
Configuring Metadata Capture	49
Metadata List View	50
Configuring HD-SDI Metadata Sources	52
Configuring Network Metadata Sources	56
Configuring Serial Metadata Sources	59
Metadata Settings	62
Metadata Statistics	68

CoT/UDP with SPI Message Filtering Based on UID	69
Configuring Streams.....	70
Streams List View.....	70
Setting Up Streams.....	73
Configuring Secure Reliable Transport (SRT).....	80
Stream Settings.....	87
Stream Statistics.....	96
Configuring Ad Insertion Sources.....	100
Ad Insertion Settings.....	102
Ad Insertion Statistics.....	103

System Administration 105

Viewing System Status Information.....	106
Status Settings.....	109
Rebooting the Encoder.....	110
Taking a System Snapshot.....	110
User Preferences.....	112
Saving and Loading Presets.....	113
Installing Firmware Updates	118
Configuring Network Settings.....	122
Network Settings.....	126
Configuring Date and Time	130
Date and Time Settings.....	134
Enabling and Disabling Network Services.....	135
Services Settings.....	138
Enabling ONVIF Support and Milestone Integration.....	140
Pairing the Encoder with Haivision EMS	143
Configuring RTSP	145
Managing Licenses.....	146
License File Errors.....	152
Managing the COM Port.....	153
COM Port Settings.....	154

Managing Users and Security 156

Managing User Accounts.....	157
Account Management.....	159
Account Settings	162
Managing Public Key Authentication	163
Managing Messages.....	164
Managing Banners.....	166
Managing Security Policies.....	169
Policy Settings	173
Managing Certificates	177
Generating a Certificate.....	177
Importing a Certificate	180
Viewing Certificate Details.....	182
Certificate Settings	183
Managing Audits	185
Audit Settings	186

Using SNMP to Configure A/V Services 188

SNMP Overview.....	189
Supported MIBs.....	189
SNMP Agent Components	191
snmpd.....	191
snmpd.conf.....	191
snmpd.local.conf	191
nmcfgr.....	192
SNMPv3	194
Examples.....	194
SNMP Utilities.....	195
SNMP Syntax for Setting Up Streams	196
Examples.....	197

CLI Command Reference	198
Accessing the CLI	198
Syntax Conventions	199
Command Summary and Access Control	201
Operation Commands	204
adinsertion	205
audenc	208
leds	213
metadata	215
passthrough	230
rtsp	234
session	235
stream	237
temperature	247
videnc	248
vidin	254
Administration Commands	256
account	257
audit	259
banner	261
certificate	263
config	266
date	269
dtconfig	270
emspair	271
ethercfg	274
haiversion	276
ipconfig	277
ipv6config	281
license	284
messages	286
nmcfg	288
package	293
passwd	295
policy	296
pubkey	301
reboot	302
routes	303
service	304
system_snapshot.sh	307
tzconfig	308
Technical Specifications	309
Video Input Interfaces	310
Video Encoding	310
Supported Video Encoding Input and Downscale Resolutions	311
Audio Encoding	313
Advanced Features	313
ISR Metadata	313
Network and Management Interfaces	314
IP Network Interfaces	314
Management Interfaces	314
Dimensions, Weight, Power	315
Appliance	315
OEM Board	315
Regulatory/Compliance Specifications	316
Accessing the REST API	317
Getting Help	319

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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



Tip

Indicates highlights, suggestions, or helpful hints.



Note

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



Important

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

 Caution

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

 Warning

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

Getting Service Support

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

This user's guide explains how to configure and manage the Makito X1 Rugged encoder to stream audio, video, and metadata to a compatible decoding device, using either the Web interface, the Command Line Interface (CLI), or an SNMP server.

For information on installing and connecting to the Makito X1 encoder, refer to the [\(1.3 2\) Makito X1 Rugged Encoder Installation Guide](#).

**Important**

Before using the encoder, please familiarize yourself with the [\(1.3 2\) Safety Guidelines](#) in the [Installation Guide](#) and [\(1.3 2\) Waste Electrical and Electronic Equipment \(WEEE\) Disposal](#) notice in the [\(1.3 2\) Preface](#) (available at <https://doc.haivision.com>).

**Note**

Unless otherwise specified, references to the "Makito X Series" or "Makito X" can be taken to include the Makito X, Makito X4, Makito X1, and Makito FX family of encoders and decoders.

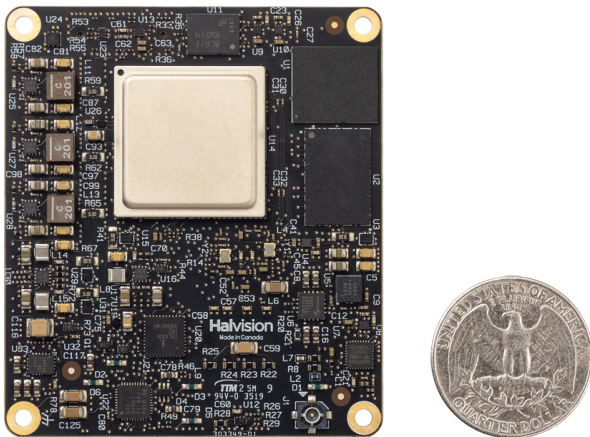
Introduction

This section provides an overview of the Makito X1 Encoder, along with a description of the main hardware components and key features.

Topics Discussed

- [Product Overview](#)
- [Physical Description](#)
- [Resetting the MX1 Rugged](#)

Product Overview



The Makito X1 Rugged is an ultra-compact H.265/HEVC and H.264/AVC low latency encoder for real-time streaming of MISB/JITC-compliant full motion video in demanding Intelligence, Surveillance and Reconnaissance (ISR) environments.

Makito X1 Rugged features include the following:

- **HEVC Encoding** - With dual encoding cores, the Makito X1 Rugged can encode HD 1080p60 or SD with H.265/HEVC and H.264/AVC compression simultaneously. On the first encoder (only), it offers independent control of scaling, cropping, and encoding parameters. It also supports Network Adaptive Encoding to provide quality streams even when network bandwidth is variable or unpredictable, for example, over constrained IP networks, line-of-sight (LOS) and satellite links.

- **Small Form Factor, Powerful Encoding** – The Makito X1 Rugged is a portable, SWaP- (Size, Weight, and Power)-optimized video encoder available as a hardened appliance or OEM board for advanced integrations.
 - The appliance is designed for deployment in portable man-wearable equipment or small platforms in harsh environments.
 - The OEM board is suited for deep integration within ISR sensor, datalink, or mission systems.
- **Ultra Low Latency for ISR and Situational Awareness** – The Makito X1 Rugged streams high-quality full-motion video at low encoding latencies suitable for the most demanding ISR applications. It ensures excellent picture quality at low bit rates to address the real-time requirements for air, ground, manned or unmanned platforms.
- **Compliant Encoding with KLV Metadata from Haivision** – The Makito X1 Rugged complies with MISB/STANAG specifications for encoding and KLV metadata. It supports selective filtering of KLV metadata parameters to ensure downstream interoperability with exploitation systems and cross-domain applications. It provides the flexibility to combine H.265/HEVC and H.264/AVC encoded video with synchronous or asynchronous KLV metadata and optimizes streaming bandwidth.

**Note**

For information on the OEM board, please refer to the *Makito X1 Integrator's Board Installation Guide* (available upon request at sales@haivision.com).

Physical Description



Note

This page includes information regarding both the original Makito X1 chassis and the Makito X1 chassis v2. The Network connector and DC IN/IO connector on v2 have been changed in order to meet higher vibration requirements.

Following is a description of the Makito X1 interfaces, connectors, and LED status indicators:

MX1 Rugged v2 (#S-MX1E-R-V2-SDI1)



MX1 Rugged v2 (28V DC)



MX1 Rugged (#S-MX1E-R-SDI1)



The Makito X1 comes equipped with the following interfaces:

- **DC In & I/O** connector combining:
 - Power (+5VDC, < 8 W, or 28V DC)
 - Analog audio inputs (Two (2) channels of analog audio -- 10K, 20K or 40K kOhms input impedance)
 - Serial (RS-232/422 Port - can be used for Management, Pass-thru or KLV or CoT metadata ingest)
- **CVBS/SDI** connector → 75 Ω BNC (either analog CVBS (Composite Video Baseband Signal) or SDI video signal with format auto-detected)
- **Network** connector → 10/100/1000 Base-T Gigabit Ethernet; cable also includes a Reset button

The BNC connector is used for Composite (CVBS), SD-SDI (Serial Digital Interface) and HD-SDI video input signals. It is also a 3G-SDI capable interface supporting 1080p 50/60 fps video @ 3Gbps. In addition, the BNC connector supports auto-detection of the HD resolution and embedded digital audio.

LED Status Indicator

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

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).
	Orange fast blinking	Reset button is pressed for more than five seconds (Factory Reset enabled). After Orange fast blinking, the LED turns off, stays off for a while, and then starts Green slow blinking towards the end of the booting up.

Important

The LED status indicator can be shut off completely through the command line interface. In this case, there will be no indications of any kind from the LED. For details, see [leds](#).

Tip

For information on installing and connecting to the Makito X1 encoder, refer to the [\(1.3 2\) Makito X1 Rugged Encoder Installation Guide](#).

Related Topics

- [Install the Makito X1 Rugged Encoder](#)
- [Resetting the Encoder](#)

Resetting the MX1 Rugged

This section describes the steps to perform a hardware reset on the Makito X1. The Reset button (located on the Ethernet/Factory Reset cable) is used either to reset the system or to restore the factory default settings.

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



Note

After a factory reset, only the firmware revision, serial number, MAC address, and licenses are preserved. All other data is deleted (including saved presets, added user accounts, modified passwords, and encoding or decoding settings). All settings are returned to their factory preset conditions (including the IP address). Preset Auto-Save is enabled by default after a factory reset.



Important

Do *not* perform a factory reset during bootup. This may cause the unit to enter error mode (LED flashing orange) and fail to boot.

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

1. With the encoder on, press the button labeled **Reset** on the Ethernet/Factory Reset cable.
2. **System Reset:** Press the 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 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.



Important

The LED status indicator can be shut off completely through the command line interface. In this case, there will be no indications of any kind from the LED. For details, see [leds](#).



Caution

When performing a Factory Reset, do not remove or disconnect the power supply until the reset is complete.

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

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 connecting the appliance, refer to the [\(1.3 2\) Makito X1 Rugged Encoder Installation Guide](#).

Also, please familiarize yourself with the [\(1.3 2\) Safety Guidelines](#) in the [Installation Guide](#) and [\(1.3 2\) Waste Electrical and Electronic Equipment \(WEEE\) Disposal](#) notice in the [\(1.3 2\) Preface](#) (available at <https://doc.haivision.com>).

All Makito X1 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 X1 through its Ethernet LAN port.

Topics Discussed

- [Accessing the Encoder](#)
 - [Default Encoder IP Address](#)
 - [Role-based Authorization](#)
- [Signing In to the Web Interface](#)
- [Exploring the Web Interface](#)
- [Changing Your Password](#)
- [Signing Out](#)

Accessing the Encoder

Managing the Makito X1 from the Web interface requires a connection from the unit's LAN port to your network. You must then connect a computer with a Web browser to the network to access the Web interface.

To access the encoder configuration Web page:

1. From your computer, open a Web browser.

**Note**

The Makito X1 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 X1, see [CLI Command Reference](#).

For information on SNMP management of the Makito X1, 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).

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

**Note**

The Makito X1 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 MX1 Rugged](#)

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 <i>not</i> 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

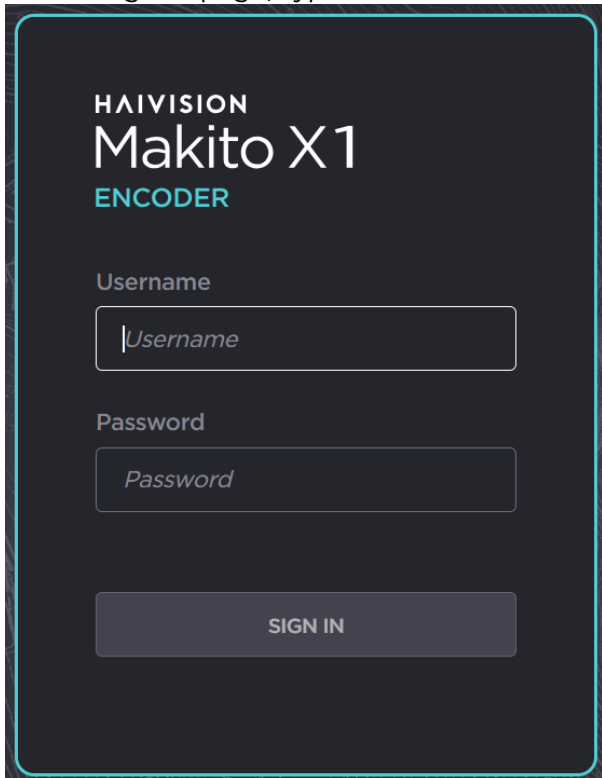
To sign in to the Makito X1 configuration Web page:

- 1. From your Web browser, type the encoder’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.



Note

The Makito X1 provides three pre-defined user accounts. For information, see [Role-based Authorization](#).

4. After the first login, the Help Us Improve pop-up appears, as below.

privacy policy.' At the bottom are two buttons: 'DECLINE' and 'ACCEPT'." data-bbox="121 615 647 867"/>

To help improve Haivision products by providing anonymous user analytics data, click **Accept**.

To decline this feature, click **Decline**.

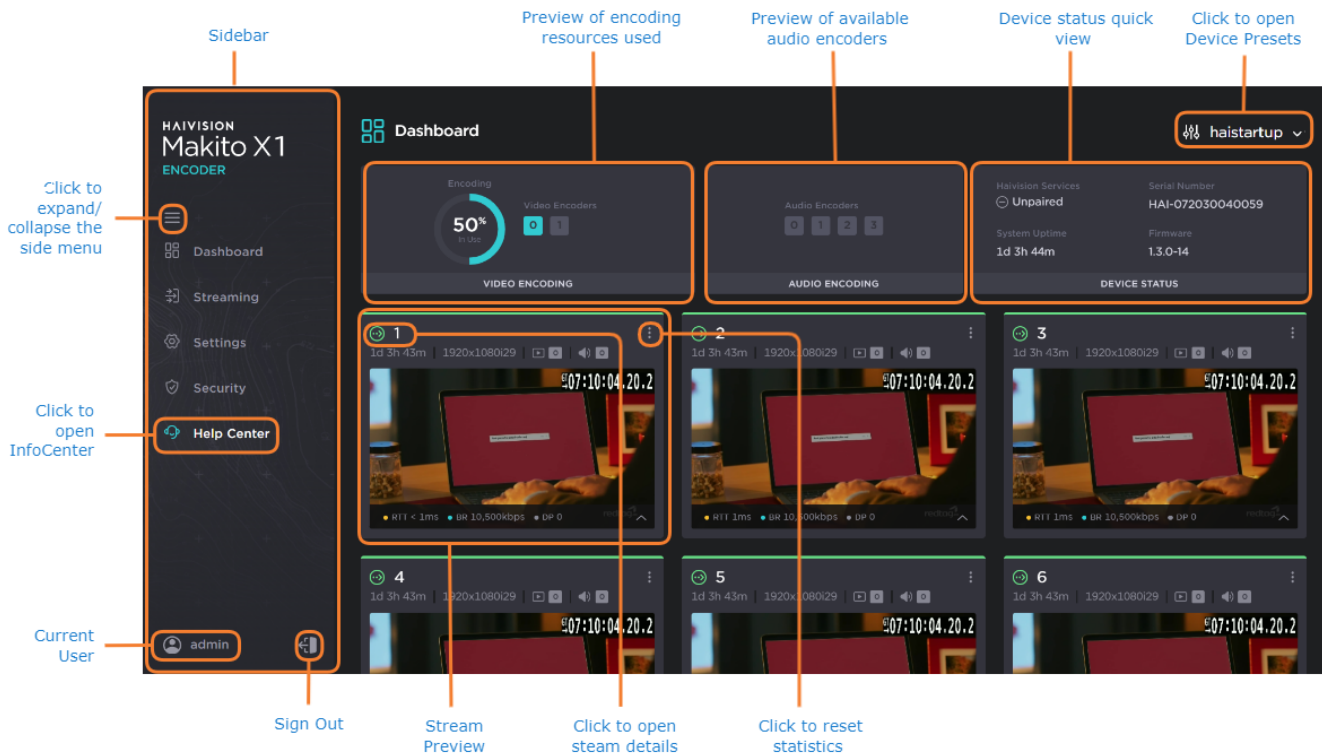
**Info**

You can enable or disable this feature any time by going to **Settings**>[Services](#).

Exploring the Web Interface

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

The Makito X1 Web interface opens to the Dashboard, as shown in the following example.



- Select **Streaming** from the sidebar to set up [Streams](#), [Video Encoders](#), [Audio Encoders](#), or [Metadata](#).
- Select **Settings** from the sidebar to:
 - View the [Status](#) settings and configure User Preferences
 - View or [Update](#) the Current Software
 - View or configure the [Network settings](#)
 - View or configure the [Date and Time](#)
 - View or configure [Services](#)
 - Manage [Licensing](#)
- Select **Security** from the sidebar to manage:
 - [Accounts](#)
 - [Messages](#)
 - [Banner](#) display
 - [Policies](#)
 - [Certificates](#)
 - [Audit](#) settings
- Select **Help Center** from the sidebar to access online Help. You will be re-directed to the **Haivision InfoCenter** website, which contains the Makito X1 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 Help for the Makito X1 Rugged Encoder will open in your Web browser.

Related Topics:

- [Managing the Encoder](#)
- [System Administration](#)
- [Managing Users and Security](#)

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.

Users assigned either **Operator** or **Guest** roles can change their passwords from the Accounts page, as described in this section. This is useful when logging into a Makito X1 Rugged Encoder on which the factory defaults have not been changed.



Note

Administrative users may change their passwords from the Accounts page. See [Managing User Accounts](#).

To change your password:

1. To navigate to the Accounts tab, click **Security** on the sidebar, and select the **Accounts** tab.

2. On the Operator or User's Account page, type your current password in the Current Password field.

The screenshot shows the 'Accounts' page in a dark-themed interface. At the top, there's a 'Username' field containing 'operator' and an 'APPLY' button. Below this is the 'PASSWORD' section, which includes a 'Role' dropdown menu set to 'Operator'. The password fields are 'Current Password', 'New Password', and 'Confirm Password', each with a toggle icon to show or hide the password. At the bottom is the 'PUBLIC KEYS' section with an 'ADD' button and a table with columns for 'NAME' and 'FINGERPRINT'.

3. Type the new password in the New Password field, and again in the Confirm 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 X1, be sure to sign out. To do so, click **Sign out**  from the sidebar.

Signing out prevents misuse and unauthorized access to the encoder.

Managing the Encoder

This section explains how to set up and manage video encoding and streaming, using the Web interface.

**Note**

For an overview of the Web interface, see [Getting Started with the Web Interface](#).

Topics Discussed

- [Configuring Video Encoders](#)
 - [Configuring Video Encoder Settings](#)
 - [Video Encoder Settings](#)
 - [Video Encoder Statistics](#)
- [Configuring Audio Encoders](#)
 - [Configuring Audio Encoder Settings](#)
 - [Audio Encoder Settings](#)
 - [Audio Encoder Statistics](#)
- [Configuring Metadata Capture](#)
 - [Configuring HD-SDI Metadata Sources](#)
 - [Configuring Network Metadata Sources](#)
 - [Configuring Serial Metadata Sources](#)
 - [Metadata Settings](#)
 - [Metadata Statistics](#)
 - [CoT/UDP with SPI Message Filtering Based on UID](#)
- [Configuring Streams](#)
 - [Setting Up Streams](#)
 - [Configuring Secure Reliable Transport \(SRT\)](#)
 - [Stream Settings](#)
 - [Stream Statistics](#)
- [Configuring Ad Insertion Sources](#)
 - [Ad Insertion Settings](#)
 - [Ad Insertion Statistics](#)

Configuring Video Encoders

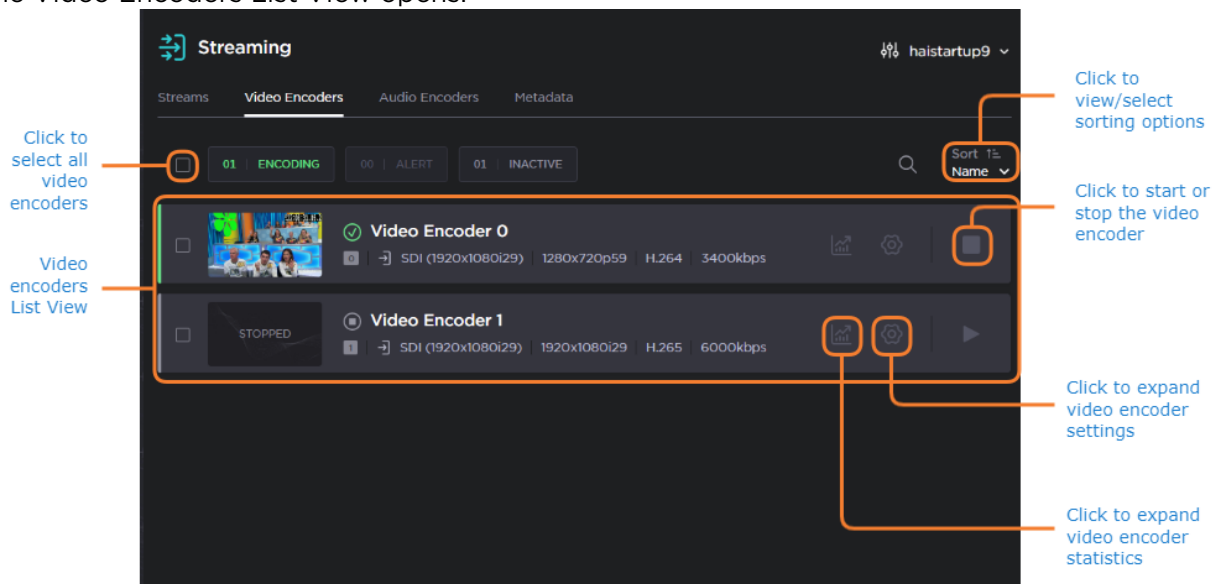
From the Video Encoders page, you can configure two video encoders to apply to streams. Each encoder can be configured independently and assigned to multiple outputs to support multi-bitrate streaming. You can start and stop each video encoder, as well as display statistics.

The Makito X1 supports concurrent AVC/H.264 and HEVC/H.265 video encoding.

Video Encoders List View

To open the Video Encoders List View:

1. Click Streaming from the sidebar, and select the **Video Encoders** tab.
The Video Encoders List View opens.



The Video Encoders List View displays the status, Name, Input format, Resolution, Codec (Algorithm), and Bitrate for each video encoder.

2. From here, you can perform the following tasks:
 - To view or modify the video encoder statistics, click the **Statistics** icon  on the video encoder panel.
 - To view or modify the video encoder Name, Input, and Detailed Settings, click the **Settings** icon  on the video encoder panel.
 - To change the video encoder status, click the **Start/Stop** icon  (as applicable) on the video encoder panel.
 - To change the status for multiple video encoders, check the check-boxes on each video encoder panel and click the **Start** or **Stop** buttons (as applicable) that appear above the list.
3. To apply your changes, click **Apply**.

Topics Discussed

- [Configuring Video Encoder Settings](#)
- [Video Encoder Settings](#)
- [Video Encoder Statistics](#)

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. For supported video encoding resolutions, see [Supported Video Encoding Input and Downscale Resolutions](#).

To configure the Video Encoding Settings:

1. From the Video Encoders List View, click the **Settings** icon  on the encoder panel.
The Video Encoder Detail View opens, displaying the settings for the selected video encoder.

Streaming

haistartup

Streams
Video Encoders
Audio Encoders
Metadata

☐
01 | **ENCODING**

☐
00 | ALERT

☐
01 | INACTIVE

Sort
Name

☐

Video Encoder 0

ID

BNC-1 (1280x720p59) | 1280x720p59 | H.265 | 6000kbps

Name

Video Encoder 0

CANCEL

APPLY

INPUT

Input

BNC-1

☐ FIR Filter
☐ Square Division

Input Format

1280x720p59

SETTINGS

Codec Algorithm

HEVC/H.265

Resolution

Automatic

☐ Closed Captioning

Encoding Profile

Main

Frame Rate

Automatic

Timecode Source

None

Chroma Subsampling

4:2:0 8-bit

Framing

IP

Aspect Ratio

Automatic

Rate Control

CBR

☐ Intra Refresh

Bitrate*

6000

GOP Size*

120

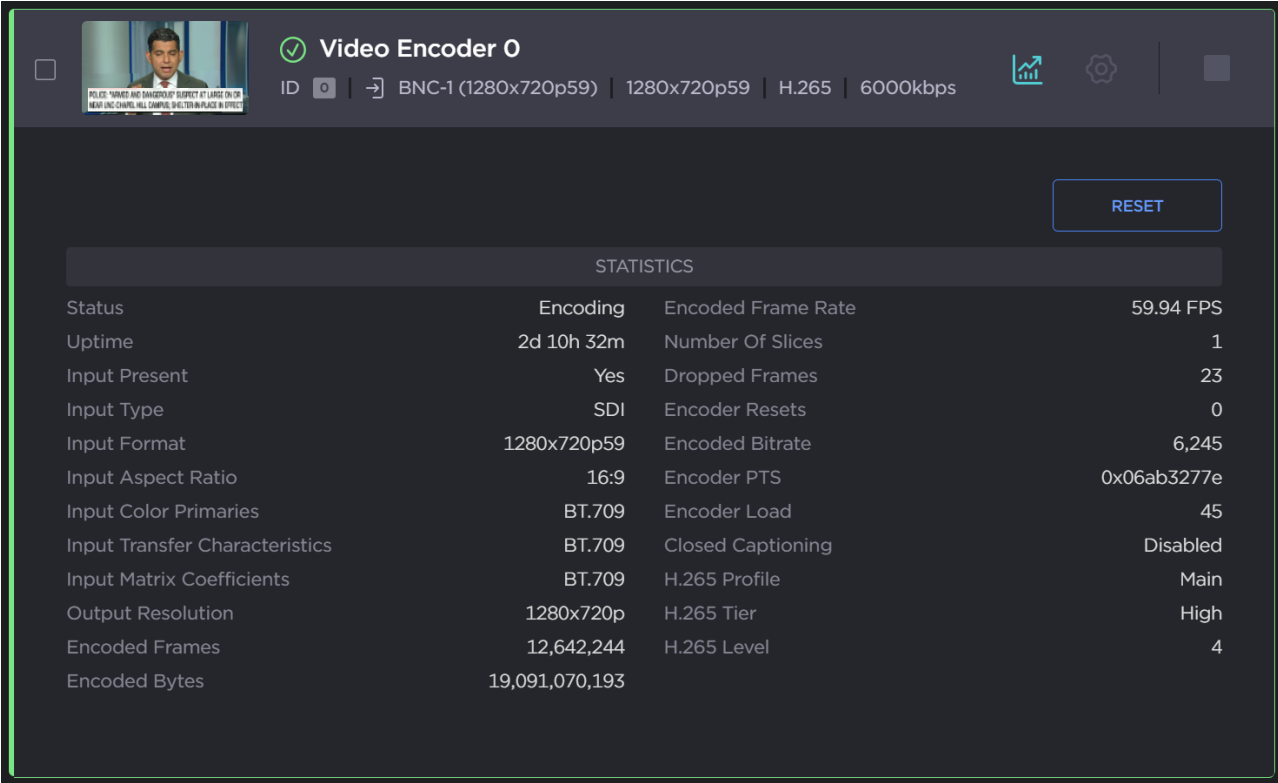
☐ Partial Image Skip

Slices

1

- Select or enter the new value(s) in the appropriate field(s). See [Video Encoder Settings](#).

- 3. Click the **Settings** icon  again to retract the video encoder settings.
- 4. To start or stop the encoder, click the **Start/Stop**  /  icons (as applicable).
- 5. To view the statistics for the encoder, click the **Statistics** icon . For details, see [Video Encoder Statistics](#).



- 6. To reset the video encoder statistics, click **Reset**.
- 7. Click the **Statistics** icon  again to retract the video encoder statistics panel.
- 8. To apply your changes, click **Apply**.

Related Topics

- [Video Encoder Settings](#)
- [videnc](#) (CLI Command)

Video Encoder Settings

The following tables list the Video Encoder controls and settings:

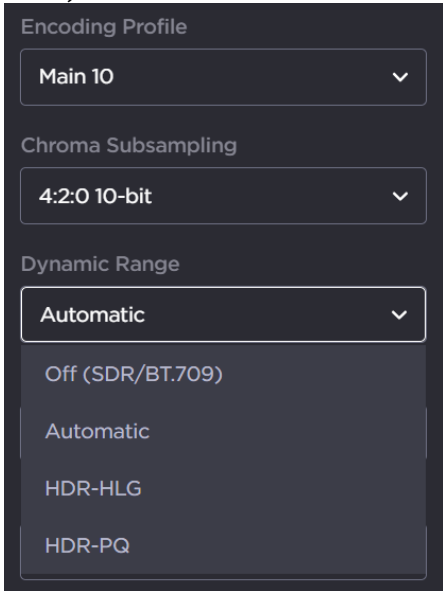
Input

Video Encoder Setting	Default	Description/Values
Input		The Video Input port for the encoder (Read-only since the Makito X1 provides one BNC input).

Video Encoder Setting	Default	Description/Values
	BNC-1	BNC-1
FIR Filter	Disabled	Check this checkbox to enable Input Image Filtering for the input interface. This parameter filters the video input and removes noise in order to optimize the compression of the image and to enhance the overall quality of the coded video stream.  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.
Input Format	n/a	This is the input signal auto-detected from the video source. It includes the number of pixels per line, whether the video is interlaced or progressively scanned (indicated by i or p), and the number of frames per second.  Note If the signal cannot be detected (or is outside the supported range), the Input Format will be Unknown.

Encoder Parameters

Video Encoder Setting	Default	Description/Values
Codec Algorithm	HEVC	Select the codec algorithm for the encoder: - AVC/H.264 - HEVC/H.265
Encoding Profile	Main	Select the application profile class for the encoder:
		(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

Video Encoder Setting	Default	Description/Values
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)
Dynamic Range		(10-bit Chroma Subsampling must be selected) Select to configure the encoder to detect the inbound High Dynamic Range (HDR) transfer function signaling and forward that information within the encoded stream. - Off (SDR/BT.709) - Automatic: the encoder detects HDR transfer function from the source - HDR-HLG: HDR content is based on the Hybrid Log Gamma (HLG, BT.2100) transfer function - HDR-PQ: HDR content is based on the Perceptual Quantizer (PQ, SMPTE ST 2084/ BT.2100) transfer function 
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 When set to Auto, the Max Bitrate is the same as the configured Bitrate below.
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. Partial Image Skip is useful for ISR customers who have multiple streams being decoded by various decoders with limited network bandwidth resources. In order to ensure that all the streams stay within their bandwidth budgets, they use CBR implementations of video encoders to constrain their output streams to adhere to specified bandwidth limits.  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.  Note Manually selecting a coded picture resolution will increase the video encoder latency by one (1) frame period.
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  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)  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 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 by the Intra Refresh Rate parameter. Intra-refresh minimizes latency, smooths the video bitrate, and minimizes GOP pulsing artifacts.  Tip Intra-refresh requires that decoders that do not support random access points be started first.
GOP Size	120	(Intra-Refresh must be disabled) Enter the Group of Pictures size for the encoded video. 1..1000
slices	1	Configures the encoder to use multiple slices per frame instead of the normal 1 slice per frame encoder configuration. Encoding latency is improved since encoded slices can be transmitted on the network without having to wait for the whole frame to be encoded. 1..11  Note Latency improvements are only seen on decoders that do not buffer entire video frames before decoding and can actually decode and output slices. Multiple slices cannot be used in conjunction with Partial Image Skip or Framing containing B-frames (IBP, IBBBBP).
Closed Captioning	Disabled	(Optional) Check this checkbox to enable Closed Captioning on the output Stream.

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

Related Topics

- [Video Encoding](#) (in [Technical Specifications](#))

Video Encoder Statistics

The following table lists the Video Encoder statistics (some only available when Status is Encoding):

Video Encoder Statistic	Description/Values
Status	The current operating status of the encoder, either: • Encoding • Resetting • Await Framing • Failed • Stopped
Up Time	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	(only available when Status is Encoding) The video input for the encoder: For example, SDI, ST 2110, or Composite (Makito X4 Rugged Encoder only).
Input Format	The input signal detected from the video source.
Input Aspect Ratio	The aspect ratio of the video source.
Input Color Primaries	(SDI or SQD Personalities only) Indicates the chromaticity coordinates of the source primaries as specified in terms of the CIE 1931 definition of x and y. e.g., BT.709, BT.601(625), BT.601(525), BT.2100
Input Transfer Characteristics	(SDI or SQD Personalities only) Indicates the reference opto-electronic transfer function (OETF) of the source picture, or indicates the inverse of the reference electro-optical transfer function (EOTF) of an output linear optical intensity. e.g., BT.709, BT.601, BT.2100(PQ), BT.2100(HLG)
Input Matrix Coefficients	(SDI or SQD Personalities only) Describes the matrix coefficients used in deriving luma and chroma signals from the green, blue, and red. e.g., BT.709 BT.601, BT.2100(NCL Y'CbCr)
Output Resolution	The stream output resolution.
Encoded Frames	Number of encoded frames.
Encoded Bytes	Number of encoded bytes.
Encoded Frame Rate	The video frame rate per second.
Number of Slices	The number of slices per frame being generated by the encoder. The range is 1 (default) up to 11.
Dropped Frames	Number of dropped frames.
Encoder Resets	Number of encoder resets.
Encoded Bitrate	The video bitrate used for the encoder (in kbps).

Video Encoder Statistic	Description/Values
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 (%).
Scaler Load	Percentage of FPGA scaler capability being used by a given encoder.
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	(CC must be enabled) Number of extracted Caption Service Descriptor Bytes.  Tip CSDs define signaling and announcement of caption services.
Timecode Source	(Timecoding must be enabled) The selected 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.
H.264 or H.265 Profile	The application profile class for the encoder, either: - H.264: Main, High, or Baseline or - H.265: Main, Main-10, Main-4.2.2 10.
H.265 Tier	The application tier for the encoder, as defined by the HEVC standard, either Main or High. The Main tier is a lower tier than the High and was designed for most applications. The High tier was designed for very demanding applications (in terms of their maximum bit rate).
H.264 or H.265 Level	The required level of decoder performance to be able to process the video incoming stream: e.g., 3, 3.2, 4, or 4.2
Reset	Click to reset the Video Encoder statistics.

Related Topics:

- [Video Encoder Settings](#)

Configuring Audio Encoders

From the Audio Encoder page, you can configure up to four 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.



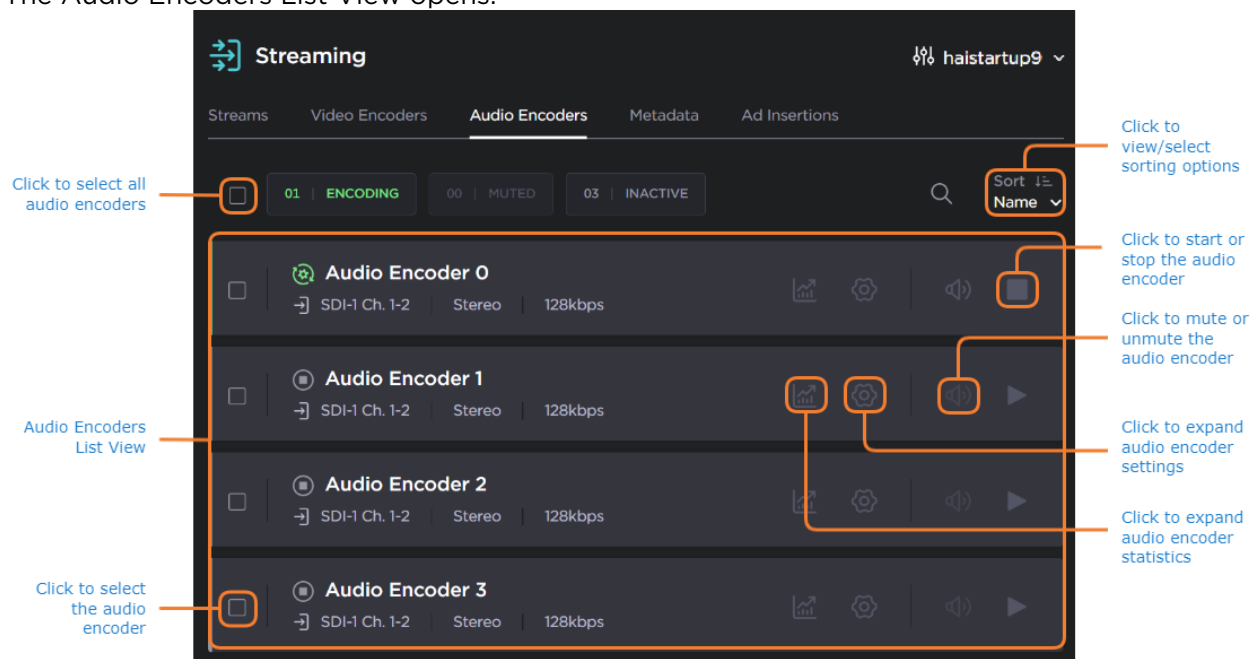
Note

The Makito X1 is capable of encoding up to eight channels of audio in channel pair groups.

Audio Encoders List View

To open the Audio Encoders List View:

1. Click **Streaming** on the sidebar, and select the **Audio Encoders** tab.
The Audio Encoders List View opens.



2. The Audio Encoders List View displays the Status, Name, Input, Channel Mode, Language, and Bitrate for each audio encoder.
3. From here, you can perform the following tasks:
 - To view details or modify the audio settings for an encoder, click the **Settings** icon  in the audio encoder panel to open the Audio Encoder Detail View.
 - To view the Audio Encoder statistics, click the **Statistics** icon  in the audio encoder panel. From here, click the **Reset** button to reset the statistics.

- To change the status for an audio encoder input, click the the **Mute/Unmute** icon / or the **Start/Stop** icon  /  (as applicable).
 - To change the status for multiple audio encoder inputs, click the checkboxes on each audio encoder panel you wish to modify and click the **Start**, **Stop**, **Mute**, or **Unmute** buttons (as applicable) that appear above the List View.
 - Change the Audio Encoders sort order by clicking the **Sort** dropdown menu.
4. To apply your changes, click **Apply**.

Topics Discussed

- [Configuring Audio Encoder Settings](#)
- [Audio Encoder Settings](#)
- [Audio Encoder Statistics](#)

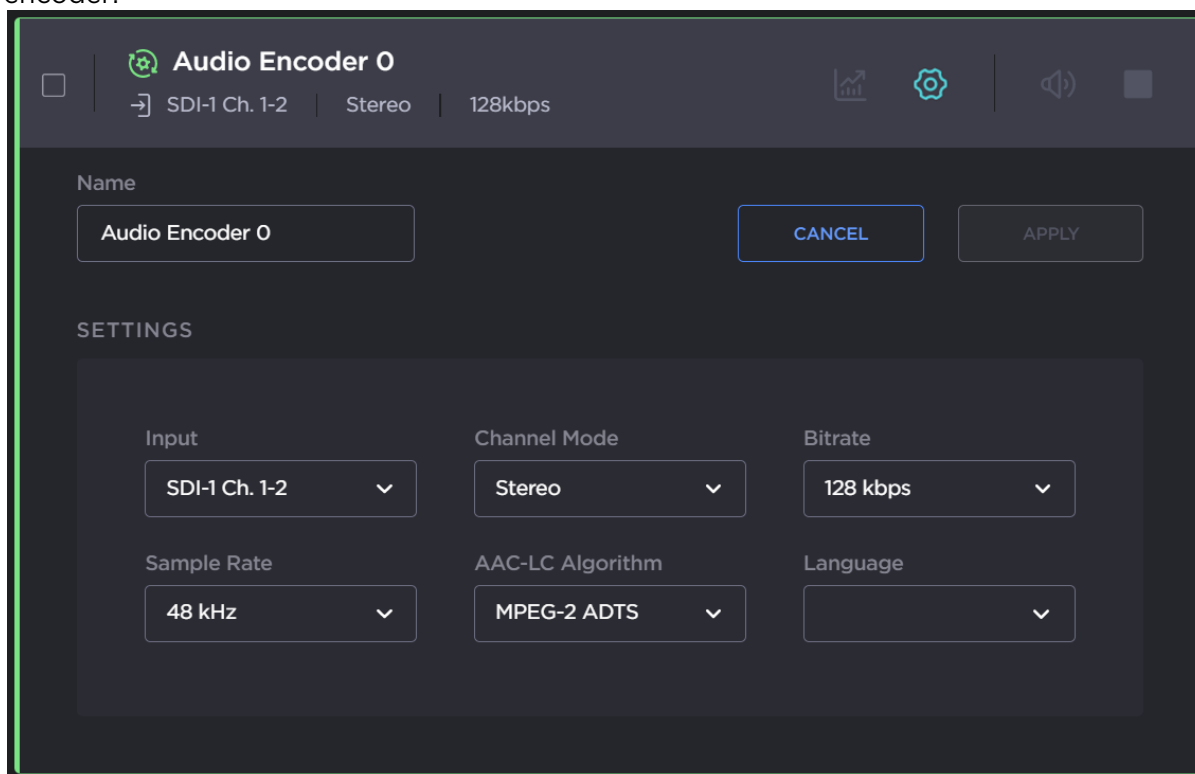
Configuring Audio Encoder Settings

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 the **Settings** icon  in the audio encoder panel you wish to modify.
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 the **Start/Stop** icon  (as applicable).
4. To mute the audio (when active), click the **Mute** icon .



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 the **Statistics** icon . For details, see [Audio Encoder Statistics](#).
6. To apply your changes, click **Apply**.
7. To retract the Audio Encoder Detail View, click the **Settings** icon  again.

Related Topics:

- [Audio Encoder Settings](#)
- [audenc](#) (CLI Command)

Audio Encoder Settings

The following tables list the Audio Encoder controls and settings:

Input Parameters

Audio Setting	Default	Description/Values
Input	SDI1 (1-2)	Select the Audio Input for the encoder. - Analog - SDI1 (1-2) . . (15-16)

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:  Note As of v1.1.1, the Makito X1 allows lower audio encoding bitrates (intended for very limited bandwidth streaming situations), as well as higher quality audio encoding at higher bitrates. The allowed bitrate ranges for 16 kHz sample rate are different than what was previously available for 48 kHz. 48 KHz sample rate: - Mono: 12 to 288 kbps - Stereo: 14 to 576 kbps
		16 KHz sample rate (analog only): - Mono: 4 to 96 kbps - Stereo: 5 to 192 kbps
Sample Rate (kHz)	48 kHz	The number of audio samples per second taken from the incoming signal. 48 kHz 16 kHz (Analog audio input 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.

Audio Setting	Default	Description/Values
0 dBFS Audio Level (dBu)	0 dBu	(Analog Input only) Adjusts the maximum analog Audio Input signal level (0 dBfs) from -6 to 0 dBu.  Note This is useful in applications such as broadcast and streaming to allow higher audio headroom.
Language	n/a	To specify the language of the input, start typing letters and select the language from the list.
Statistics	n/a	Click the Statistics icon  to view statistics for the encoder. See Audio Encoder Statistics .
Mute	n/a	Click the Mute/Unmute icon  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 the Stop icon  to stop an active encoder. Click the Start icon  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
Status	The current operating status of the encoder, indicated by the status icon, either: •  - Encoding •  - Muted •  - 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.

Audio Encoder Statistic	Description/Values
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 Encoding) 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 X1 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 X1 supports the following metadata input types:

Input Type	Description
SDI	The Makito X1 extracts KLV metadata packets from the HD-SDI interface as per MISB RP 0605.2. See Configuring HD-SDI Metadata Sources .
Network	The Makito X1 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	The Makito X1 Rugged extracts either KLV or CoT metadata packets from the COM1 serial port. See Configuring Serial Metadata Sources .

The Makito X1 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 X1 supports insertion of multiple metadata sources into the same KLV Elementary Stream.

The Makito X1 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.

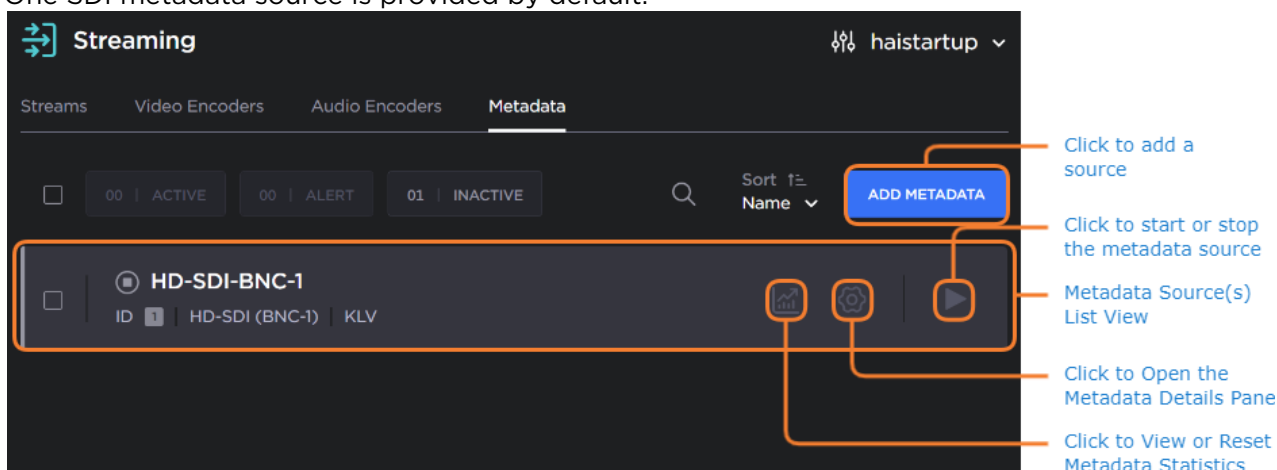
CoT/UDP and CoT/Serial metadata sources can also be re-transmitted to other IP destinations for follow-up analysis by third party systems. For more information, see [Configuring CoT Retransmission](#).

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

Metadata List View

To open the Metadata List View:

1. Click **Streaming** on the sidebar and select the **Metadata** tab.
The Metadata List View opens, displaying the list of defined Metadata sources for the encoder. One SDI metadata source is provided by default.



The Metadata List View displays the Status, source Name, ID number, Type, and Format for each source.

2. From here, you can perform the following tasks:
 - To view or modify source details, click the **Settings** icon to expand the the Metadata Detail View.
 - To view or reset the source statistics, click the **Statistics** icon .
 - To add a Network or HD-SDI source, click the **Add Metadata** button.
 - To change the status for a source, click the **Start/Stop** icon (as applicable).
 - To delete a source click the checkbox on the source panel and then click **Delete**.
3. To apply your changes, click **Apply**.

Topics Discussed

- [Configuring HD-SDI Metadata Sources](#)
- [Configuring Network Metadata Sources](#)
- [Configuring Serial Metadata Sources](#)
- [Metadata Settings](#)
- [Metadata Statistics](#)
- [CoT/UDP with SPI Message Filtering Based on UID](#)

Configuring HD-SDI Metadata Sources

The Makito X1 auto-detects the hardware setup of the encoder and automatically creates the source(s) if SDI video is connected.

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



Note

Only progressive scan formats are supported (i.e., 1280x720p and 1920x1080p). The Makito X1 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 **Settings** icon  on the metadata panel. The HD-SDI Source Detail View opens.

HD-SDI-BNC-1

ID 1 | HD-SDI (BNC-1) | KLV

Name

HD-SDI-BNC-1

CANCEL

APPLY

SOURCE

HD-SDI Input

BNC-1

DECIMATION

Decimation

None

UAS KLV TAG FILTERING

UAS KLV Tag Filtering

UAS KLV SECURITY TAG FILTERING

UAS KLV Security Tag Filtering

MISSION ID INSERTION

Mission ID

SECURITY DATA SET INSERTION

Security Data Set Insertion

or

2. To create an additional HD-SDI source, from the Metadata List View, click the **Add Metadata** button.
3. On the Add Metadata Source dialog, type in a unique name for the metadata source, and select HD-SDI from the the Metadata Type drop-down list.

4. Select the HD-SDI Input from the drop-down list.

Decimation:

5. To configure frame-decimation to reduce the bandwidth used by the metadata service, select either a decimation factor (**By Factor**) or reference encoder (**With 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. Toggle UAS KLV Tag Filtering on to filter MISB 0601 metadata tags to eliminate unwanted KLV information, see [Filtering UAS KLV Metadata Tags](#).

Mission ID/Security Data Set Insertion:

8. To configure a mission ID or security data set, see [Configuring KLV Metadata Insertion](#).
9. To apply your changes and start the Metadata stream, click **Apply**, or, if creating an additional source, click **Add Metadata**.
10. To start or stop the stream, click the **Start/Stop** icon (as applicable).
11. To view Metadata statistics, click the **Statistics** icon . For details, see [Metadata Statistics](#).
12. To return to the List View, click the **Settings** icon again.

Related Topics

- [Metadata Settings](#)
- [metadata](#) (CLI Command)

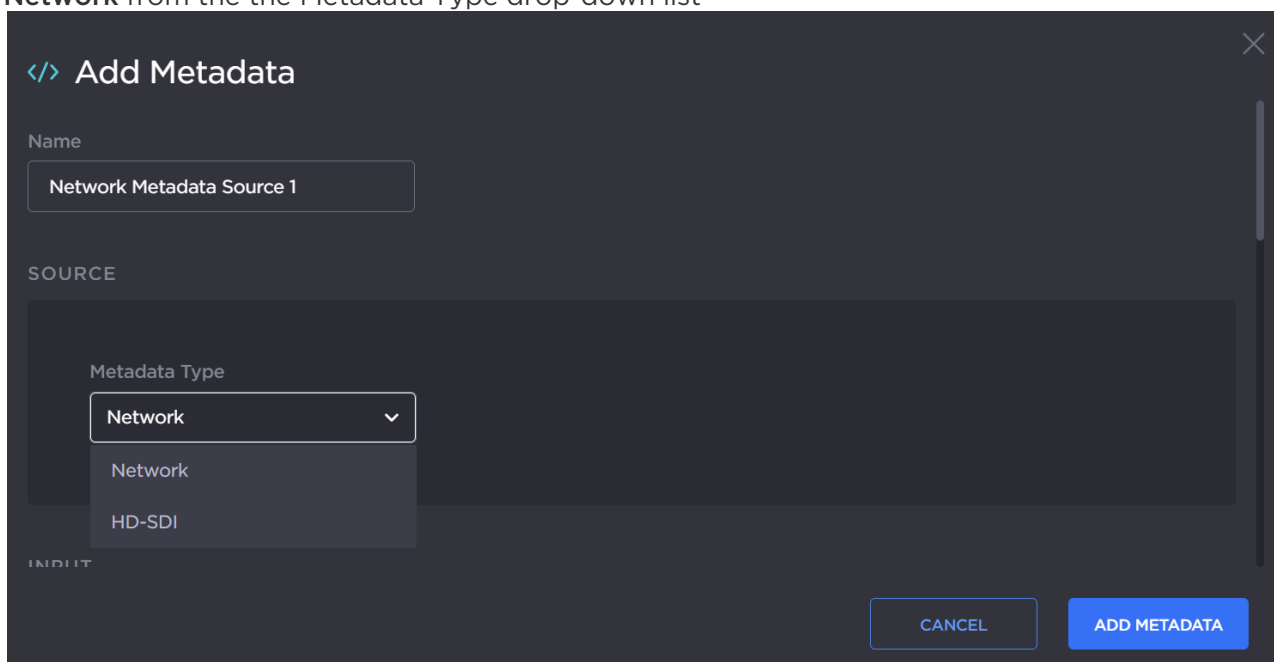
Configuring Network Metadata Sources

You can configure the Makito X1 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 X1 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 Metadata** button.
2. On the Add Metadata panel, type in a unique name for the metadata source, and select **Network** from the the Metadata Type drop-down list



3. Configure the remaining Input, Network, Mission ID Insertion and Security Data Set Insertion sections.

INPUT

Data Format

KLV

NETWORK

IP Address

Any

Port

MISSION ID INSERTION

Mission ID

SECURITY DATA SET INSERTION

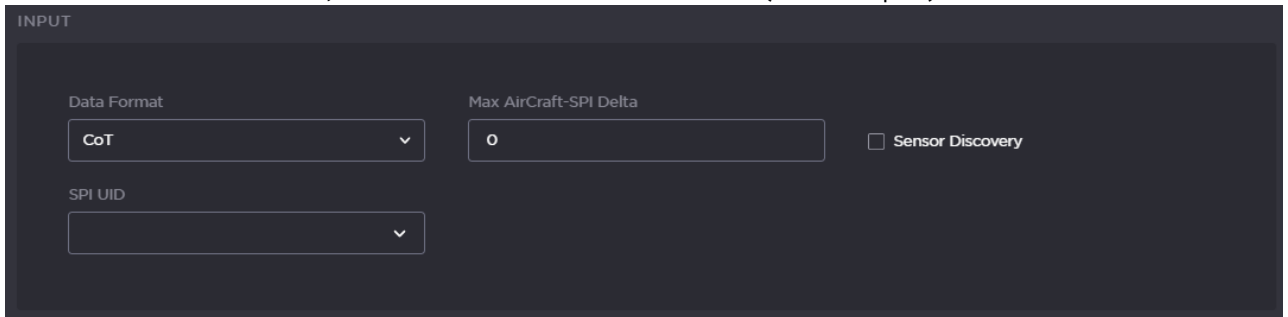
Security Data Set Insertion

CANCEL

ADD METADATA

Input and Serial Settings

- If CoT has been installed, select CoT for the Data Format (under Input).



- Select or enter the remaining value(s). For details on the Metadata fields, see [Metadata Settings](#).

CoT Relaying

- (Optional) To set up CoT re-transmission, see [Configuring CoT Retransmission](#).
- Mission ID/Security Data Set Insertion**
- (Optional) To configure a mission ID or security data to replace or insert, see [Configuring KLV Metadata Insertion](#).
- To apply your changes and start the Metadata stream, click **Add Metadata**.
- To start or stop the stream, click the **Start/Stop** icon  /  (as applicable).
- To view Metadata statistics, click the **Statistics** icon . For details, see [Metadata Statistics](#).
- To return to the List View, click the **Settings** icon  again.

Related Topics

- [Metadata Settings](#)
- [metadata](#) (CLI Command)

Configuring Serial Metadata Sources

**Note**

The Makito X1 automatically creates the Serial metadata source if the COM Port Mode is set to Metadata. See [Managing the COM Port](#).

You can configure the Makito X1 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 **Settings** icon  on the Serial metadata source (i.e., the first source in the list).

2. On the Serial Source Detail View, type in the Name for the source.

☐

(None)

ID

Serial

CoT

Max AirCraft-SPI Delta 0 ms

Name

CANCEL

APPLY

INPUT

Data Format

CoT

Max AirCraft-SPI Delta

0

☐ Sensor Discovery

SPI UID

COM PORT

Standard

RS-232

Baud Rate

115200

Data Bits

8

Parity

None

Stop Bits

1

Flow Control

None

COT RELAYING

CoT Relaying

MISSION ID INSERTION

Mission ID

SECURITY DATA SET INSERTION

Security Data Set Insertion

Input and COM Port 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 [Configuring CoT Retransmission](#).

Mission ID/Security Data Set Insertion

- 6. (Optional) To configure a mission ID or security data to replace or insert, see [Configuring KLV Metadata Insertion](#).
- 7. To apply your changes and start the Metadata stream, click **Apply**.
- 8. To start or stop the stream, click the **Start/Stop** icon  /  (as applicable)
- 9. To view Metadata statistics, click the **Statistics** icon . For details, see [Metadata Statistics](#).
- 10. To retract the Metadata Source Detail View, click the **Settings** icon  again.

Related Topics:

- [Metadata Settings](#)
- [Metadata Statistics](#)
- [metadata](#) (CLI Command)

Metadata Settings

Expand the sections below to view the encoder Metadata controls and settings:

HD-SDI Sources

HD-SDI Sources

Metadata Setting	Default	Description/Values
Source		
Name	n/a	Enter a unique name for the source.
HD-SDI Input	BNC-1	(From the List View, read-only) The Input port for the metadata source. • BNC-1
Decimation		

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: <code>1/2..1/60</code>  Note <code>1/2</code> 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 Filtering UAS KLV Metadata Tags)		
UAS KLV Tag Filtering	off	Specifies a list of tag numbers/labels from the UAS Datalink Local Set that are allowed to be streamed. Tags not included in this list will be discarded. Select either: - None - Minimum Set: the set of metadata objects as define in MISB 0902. - All: the set of metadata objects as define in MISB 0601.
UAS KLV Security Tag Filtering	off	Specifies a list of tag numbers/labels from the Security Local Data set inside the UAS that are allowed to be streamed. Tags not included will be discarded. Select either: - None - Minimum Set: the set of metadata objects as define in MISB 0902. - All: the set of metadata objects as define in MISB 0102.  Tip #48 must be included under UAS KLV Tag Filtering.
KLV Insertion (See Configuring KLV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLV input only) When set to On, enables reclassification of received UAS KLV messages. <code>on,off</code>
Security Classification	unclassified	Specifies the classification of the security data set. Select either: <code>unclassified, restricted, confidential, secret, topsecret</code>
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.

Network Sources

Network Sources

Metadata Setting	Default	Description/Values
Metadata Source Name		
Name	n/a	Enter a unique name for the source.
Input		
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 only) Specifies the maximum delta between SPI and Aircraft message timestamps for them to be considered a valid pair that can be converted to KLV. 0..1000 ms  Note Only available if CoT has been installed.
Sensor Discovery	Disabled	(CoT input only) Check this checkbox to enable discovery of SPI UUIDs that will be shown in the SPI UUID field below and can then be potentially used as the SPI UUID for SPI message filtering.
SPI UUID	n/a	(CoT input only) Double-click the text box to display the list of the SPI messages detected by the Makito X and select a string for the UUID filter.
Network		
IP Address	n/a	(Optional) The address is only required for reception of multicast metadata. In this case, you need to provide the multicast IP address to which the data is being sent. You can also specify the address if you only want to accept KLV messages coming from a specific sender.
Port	n/a	(Required) Specifies the local UDP port on the Makito X that is receiving the packets.
CoT Relaying (See Configuring CoT Retransmission)		
CoT Relaying	off	When set to On, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP. See Configuring CoT Retransmission for details of adding a relay host.
+Relay (IP Address/Port)	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.
KLTV Insertion (See Configuring KLTV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLTV input only) When set to On, enables reclassification of received UAS KLTV 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.

Serial Sources (Rugged Encoder only)

Serial Sources

Metadata Setting	Default	Description/Values
Metadata Source Name		
Name	n/a	Enter a unique name for the source.
Input Settings		
Data Format	KLTV	Select the data format for the metadata: - KLTV (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 X and select a string for the UID filter.
COM Port		
Standard	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 Configuring CoT Retransmission)		
CoT Relaying	off	When set to On, the system will retransmit received CoT/UDP or CoT/Serial metadata to up to 8 other hosts over UDP. See Configuring CoT Retransmission for details of adding a relay host.
+Relay (IP Address/Port)	n/a	Use to specify the IP address and UDP port for each relayed packets. You can optionally specify the TTL and ToS.
TTL	64	(Time-to Live for stream packets) Specifies the number of router hops that IP packets from this stream are allowed to traverse before being discarded. Range = 1..255
ToS	0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = 0..255 (decimal) or 0x00..0xFF (hex)  Important A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474.  Note The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.

KLV Insertion (See Configuring KLV Metadata Insertion)		
Mission ID Insertion	n/a	Enter a string of up to 127 characters.
Security Data Set Insertion	off	(KLV input only) When set to On, enables reclassification of received UAS KLV messages. <code>on,off</code>
Security Classification	unclassified	Specifies the classification of the security data set. Select either: <code>unclassified, restricted, confidential, secret, topsecret</code>
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 metadata stream, either: • Working • Disabled • 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)

Configuring Streams

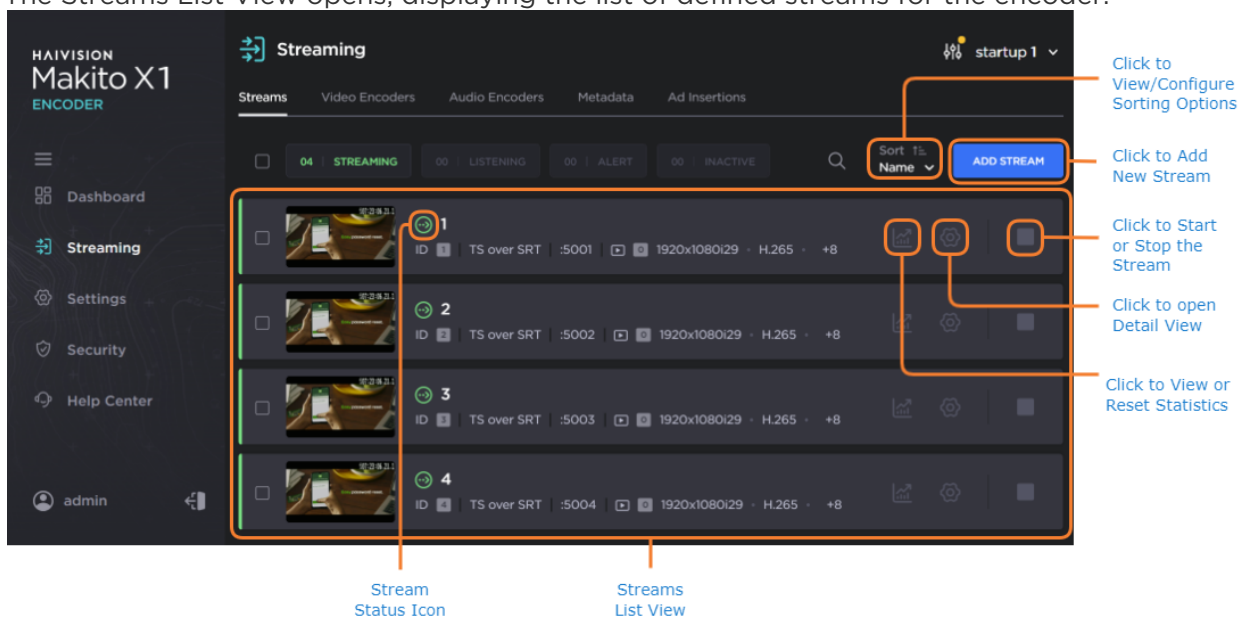
From the Streams page, you can create multiple output streams using the defined video encoders, audio encoders, and metadata (if applicable). Each output stream is configured independently. For details see:

- [Configuring Video Encoders](#)
- [Configuring Audio Encoders](#)
- [Configuring Metadata Capture](#)

Streams List View

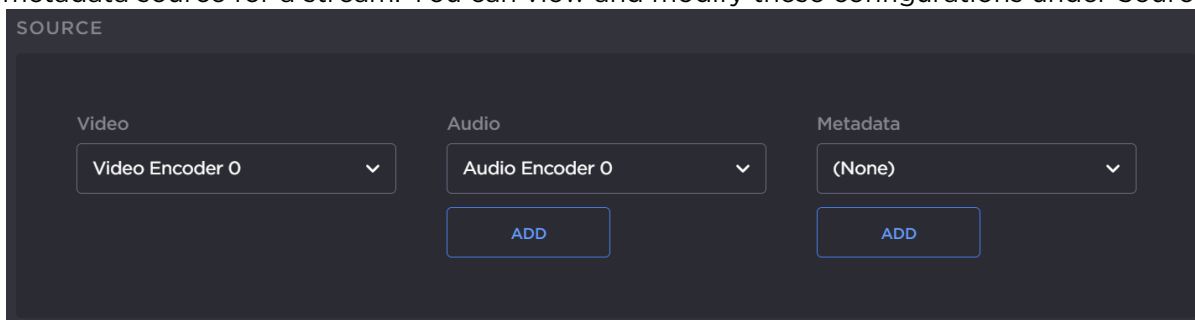
To open the Streams List View:

1. Click **Streaming** on the sidebar, and select the **Streams** tab.
The Streams List View opens, displaying the list of defined streams for the encoder.



2. The Streams List View displays the Status, Stream Name, Protocol, Destination (IP Address and Port), and Selected Content (Video/Audio Encoders and Metadata source) for each stream.
3. From here, you can perform the following tasks:
 - To create a stream, click the **Add Stream** button.
 - To view details or modify the settings for a stream, click the **Settings** icon  in the Stream panel to expand the Stream Detail View. From here you can view or modify the:
 - Source settings
 - Streaming Parameters
 - Destination
 - Link Parameters
 - SAP

- From the Stream Detail View, you can also view the video encoder, audio encoder, or metadata source for a stream. You can view and modify these configurations under Source.



- The Stream State is color coded, and the Stream Status is indicated by the Status icon. The possible Stream Statuses are:

Status	Color	State	Icon	Description
ACTIVE	Green	STREAMING		The stream is active and running.
STOPPED	Gray	STOPPED		The stream is stopped.
LISTENING	Blue	LISTENING		The stream is listening for a connection.
ALERT	Amber	CONNECTING		The stream is in the process of connecting.
		SECURING		Acquiring keys for protected content.
		RESOLVING		DNS resolution of the host name to IP address is in progress.
		SCRAMBLED		The stream is scrambled, i.e. the encoder is unable to decrypt the encrypted stream.
	Red	FAILED		An error has occurred, and caused the stream to fail.

- To change the status for an existing stream, click the check box to the far left of the Stream Panel and select either **Start**, **Stop** (as applicable), or **Delete**. Alternatively, click the **Start/Stop** icon to start or stop the stream.
- To view the stream statistics, click on the **Statistics** icon in the Stream Panel. From here, you can:
 - Click **Reset** to reset the stream statistics
 - (SRT streams only) Click **Detailed Statistics** to view the detailed stream statistics page
 - Click the **Sort** dropdown to sort the streams by Ascending or Descending order, and/or by ID, Name, Destination IP, Protocol, or Status.
 - To apply your changes, click **Apply**.
- Click the **Sort** dropdown to sort the streams by Ascending or Descending order, and/or by ID, Name, Destination IP, Protocol, or Status.

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

Topics Discussed

- [Setting Up Streams](#)
 - [Setting Up a Second Stream](#)
 - [Session Announcement Protocol \(SAP\)](#)
- [Configuring Secure Reliable Transport \(SRT\)](#)
 - [Configuring SRT Path Redundancy](#)
 - [Configuring SRT Access Control](#)
- [Stream Settings](#)
- [Stream Statistics](#)

Setting Up Streams

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 Streams List View, click the **Settings** icon  on an existing stream panel, or click the **Add Stream** button to add a new stream.

The Stream Detail View, or Add Stream panel (as below), opens.

Add Stream

Name

SOURCE

Video

Video Encoder 0

Audio

Audio Encoder 0

Metadata

(None)

ADD

ADD

STREAMING PARAMETERS

Protocol

TS over UDP

TS Settings

DESTINATION

Address

Port

Valid values (1 - 65535)

LINK PARAMETERS

Timing & Shaping

VBR

MTU

1496

ToS

0x80

TTL

64

SAP

Transmit SAP

CANCEL

ADD STREAM

- Enter the stream name and select the sources (Video, Audio, and Metadata, if applicable). See [Stream Settings](#).
- To configure multi-track audio, click the **Add** button under the Audio field and select the next Audio Encoder to add to the stream.
To remove one or more Audio Encoder from the stream, click the **Remove** icon  next to the

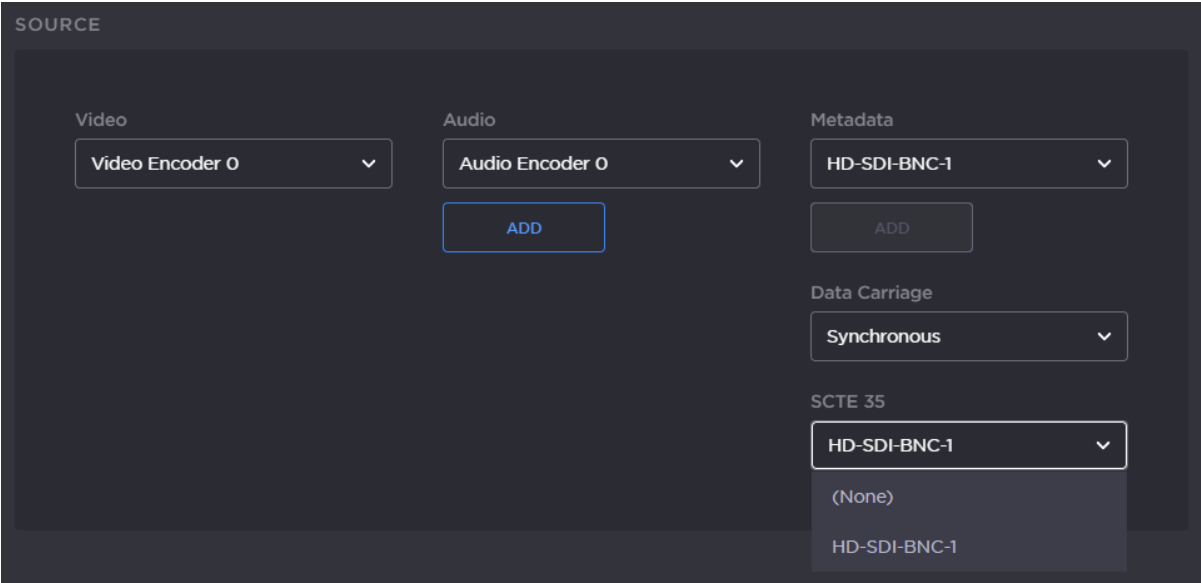
Audio Encoder field(s).

The screenshot shows the 'SOURCE' configuration panel. It has three main sections: Video, Audio, and Metadata. The Video section has a dropdown menu set to 'Video Encoder 0'. The Audio section has two dropdown menus; the first is set to 'Audio Encoder 0' and the second is set to 'Audio Encoder 1'. A dropdown menu is open for the second Audio Encoder, showing options: '(None)', 'Audio Encoder 0', 'Audio Encoder 1', 'Audio Encoder 2', and 'Audio Encoder 3'. The Metadata section has a dropdown menu set to '(None)' and an 'ADD' button below it. The bottom of the panel is labeled 'STREAMING PARAMETERS'.

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

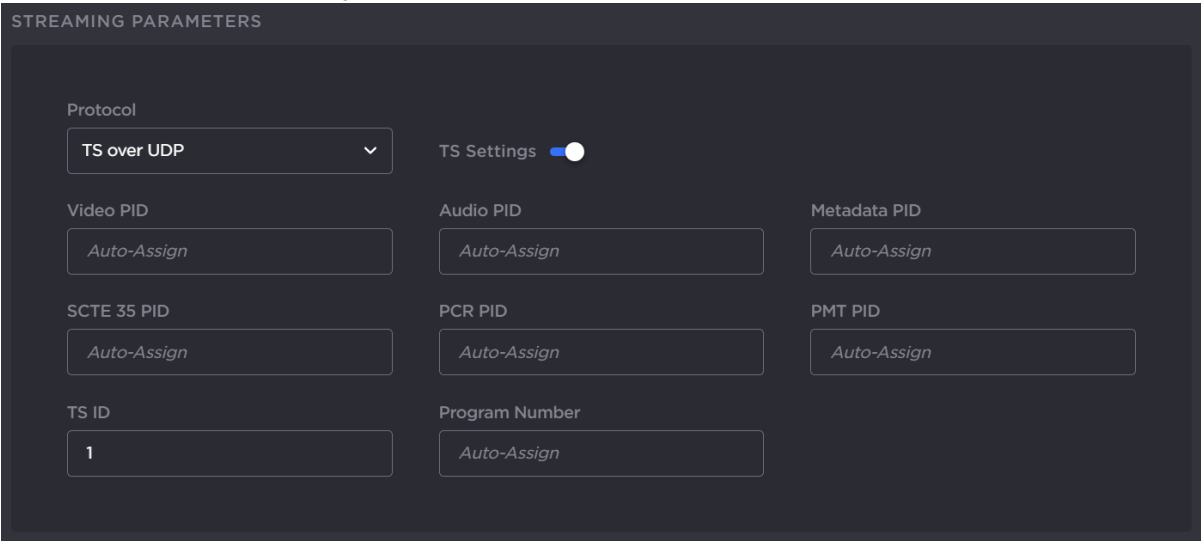
The screenshot shows the 'SOURCE' configuration panel. It has three main sections: Video, Audio, and Metadata. The Video section has a dropdown menu set to 'Video Encoder 0'. The Audio section has a dropdown menu set to 'Audio Encoder 0' and an 'ADD' button below it. The Metadata section has a dropdown menu set to 'HD-SDI-BNC-1' and an 'ADD' button below it. Below the Metadata section is a 'Data Carriage' section with a dropdown menu set to 'Synchronous'. A dropdown menu is open for the Data Carriage section, showing options: 'Synchronous', 'Asynchronous', and 'Async with Sync AU'. The bottom of the panel is labeled 'STREAMING PARAMETERS'.

- To stream metadata from multiple sources, click the **Add** button below the Metadata field and select the next metadata source to add to the stream.
- To enable ad insertion, select the available SDI input from the **SCTE 35** drop-down menu, as in the following example:



For information on setting up ad insertion sources, see [Configuring Ad Insertion Sources](#) and [adinsertion](#).

- 7. Under Streaming Parameters, select the Protocol from the dropdown menu.
- 8. To configure the Transport Stream settings (for TS over UDP, RTP, or SRT), toggle **TS Settings** on and enter the necessary values.



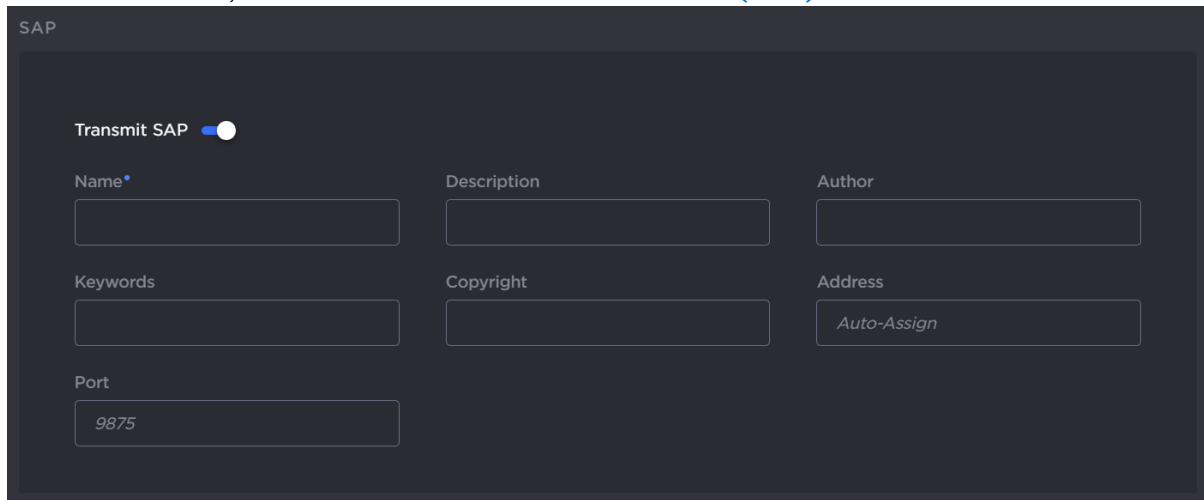
- 9. Enter the values for the Destination and Link Parameters.

Important

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

- 10. To configure a stream using the SRT (Secure Reliable Transport) streaming protocol, select TS over SRT for the Protocol and then complete the additional fields under Destination and SRT Access Control. See [Configuring Secure Reliable Transport \(SRT\)](#).

11. To configure SAP network announcements, toggle **Transmit SAP** on and fill in the SAP fields. For details, see [Session Announcement Protocol \(SAP\)](#).



The screenshot shows a dark-themed configuration window titled 'SAP'. At the top left, there is a toggle switch labeled 'Transmit SAP' which is currently turned on (blue). Below this, there are several input fields arranged in a grid:

- Name**: A text input field with a red asterisk indicating it is required.
- Description**: A text input field.
- Author**: A text input field.
- Keywords**: A text input field.
- Copyright**: A text input field.
- Address**: A text input field with a button labeled 'Auto-Assign' inside it.
- Port**: A text input field containing the value '9875'.

12. To start or stop streaming, click the **Start/Stop** icon  (as applicable).
13. To view streaming statistics, click the **Statistics** icon . For details, see [Stream Statistics](#).
14. Click **Apply** to apply your changes, or click **Add Stream** to begin the new stream and start streaming.
15. To return to List View, click the **Settings** icon  again.

Related Topics

- [Output Settings](#)
- [stream](#) (CLI Command)

Setting Up a Second Stream

To create a second stream:

1. On the Streams List View, click the **Add Stream** button.
2. Follow the steps in [Setting Up Streams](#) to configure the second session, with the two following exceptions:
 - a. 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 1 (to capture input from SDI Input 2, as shown in the following example).

- b. Under Destination, use a different Port number, for example, **2400**.
3. Click **Add Stream** again 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

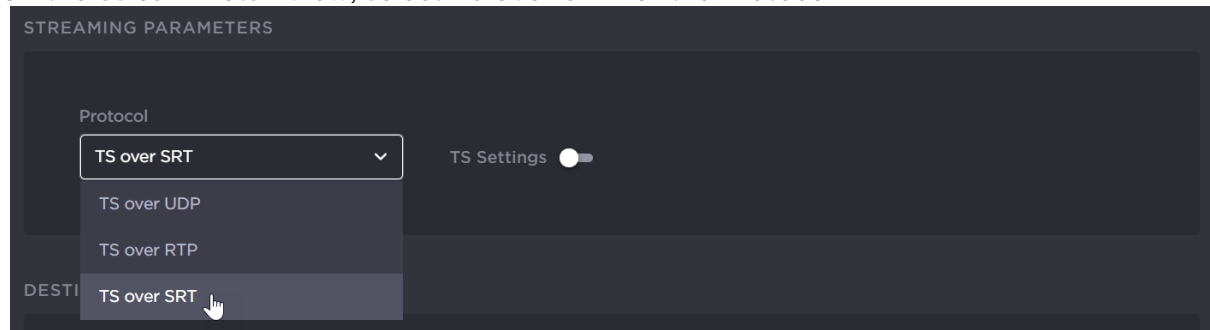
- "SAP" under "Streaming Parameters" in [Stream Settings](#)
- [session](#) (CLI command)

Configuring Secure Reliable Transport (SRT)

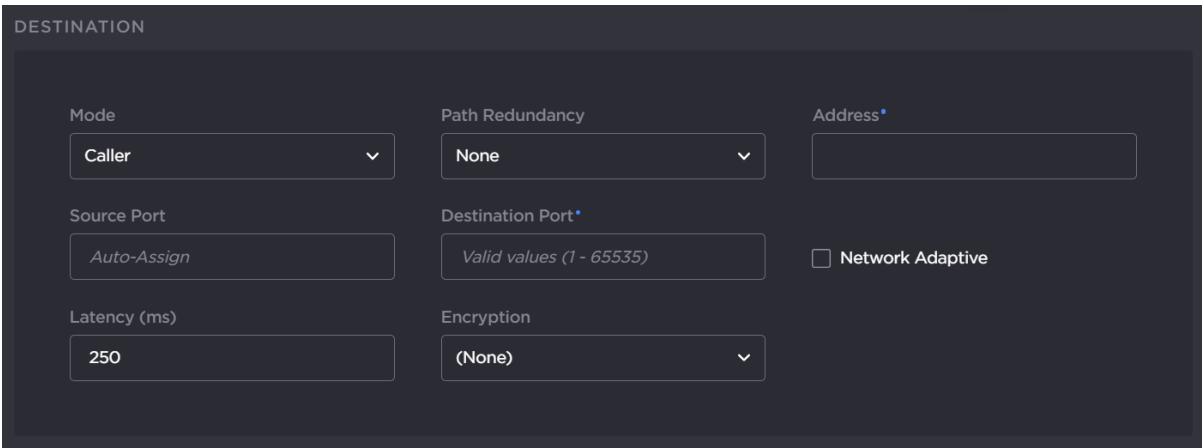
Haivision's Secure Reliable Transport (SRT) streaming protocol is designed to provide reliable and secure end-to-end transport between two SRT-enabled devices (such as Makito X Series encoders and decoders) over a link which traverses the public Internet. For more information, see the [SRT Deployment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

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 Streams](#) to set up the SRT stream.
- 3. On the Stream Detail View, select **TS over SRT** for the Protocol.

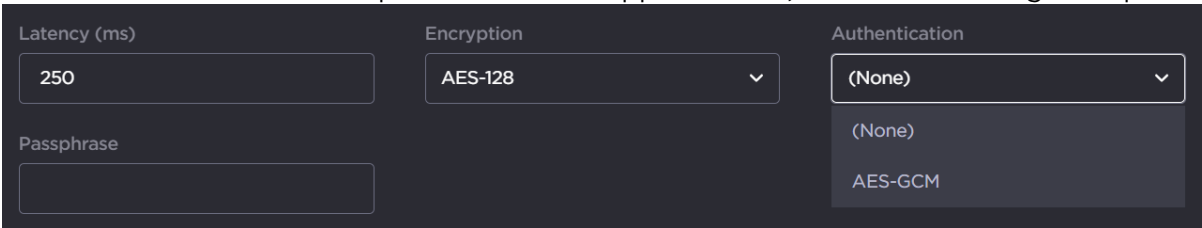


- 4. Fill out the Destination section.



- 5. To enable Authenticated Encryption, begin by selecting an encryption type from the Encryption drop-down menu.

The Authentication and Passphrase fields will appear below, as in the following example:



From the Authentication dropdown, select the appropriate authentication option. Then, enter an

encryption passphrase of your choice in the Passphrase field; passphrases must be at least 10 characters.

**Note**

Authentication options in **Caller** and **Rendez-vous** modes are None (default) or AES-GCM. Authentication options in **Listener** mode are Auto (default) or AES-GCM. Setting the authentication to Auto allows the **Listener** to accept **Callers** with authentication set to either None or AES-GCM. **Listeners** with the authentication set to AES-GCM will only accept **Callers** which are also set to AES-GCM.

- To configure redundant transport paths for the SRT stream, select Active-Active for Path Redundancy and fill in the Destination Parameters for each path. See [Configuring SRT Path Redundancy](#).
- To configure the SRT Access Control parameters, toggle **SRT Access Control** on.

From here, you can assign a Stream Publishing ID. For details, see [Configuring SRT Access Control](#).

- Click **Add Stream** to start the stream connection.
- Once you establish the SRT stream, check the statistics and make adjustments to fine-tune the stream. On the Stream panel, click the **Statistics** icon  to see how the SRT stream is performing.
- 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 [Stream Settings](#)
- For SRT-specific statistics and graphical display, see [Stream Statistics](#)

Configuring SRT Path Redundancy

You can configure the Makito X1 encoder to use redundant transport paths to ensure that content arrives at the decoder during an event. The Makito X1 encoder supports SMPTE 2022-7 style Path Redundancy in SRT Listener and Caller modes. The same content is sent over two SRT connections and network paths. If there is a failure on one of the transport links, the switchover to the other link will be seamless with no glitch on the video output and no interruptions.

To configure SRT path redundancy for a stream:

- 1. Follow the steps in [Configuring Secure Reliable Transport \(SRT\)](#) to set up the SRT stream.
- 2. On the Stream Detail View, select the **TS over SRT** protocol and **Caller** mode.
- 3. Select **Active-Active** or **Active-Backup** for Path Redundancy and fill in the Destination Parameters for each path. For details, see the SRT Settings in [Stream Settings](#).

DESTINATION

Mode

Caller

Path Redundancy

Active-Active

Path 1

Path Name

Optional Descriptive Label

Address*

Source Port

Auto-Assign

Destination Port*

Valid values (1 - 65535)

Path 2

Path Name

Optional Descriptive Label

Address*

Source Port

Auto-Assign

Destination Port*

Valid values (1 - 65535)

☐ Network Adaptive

Latency (ms)

250

Encryption

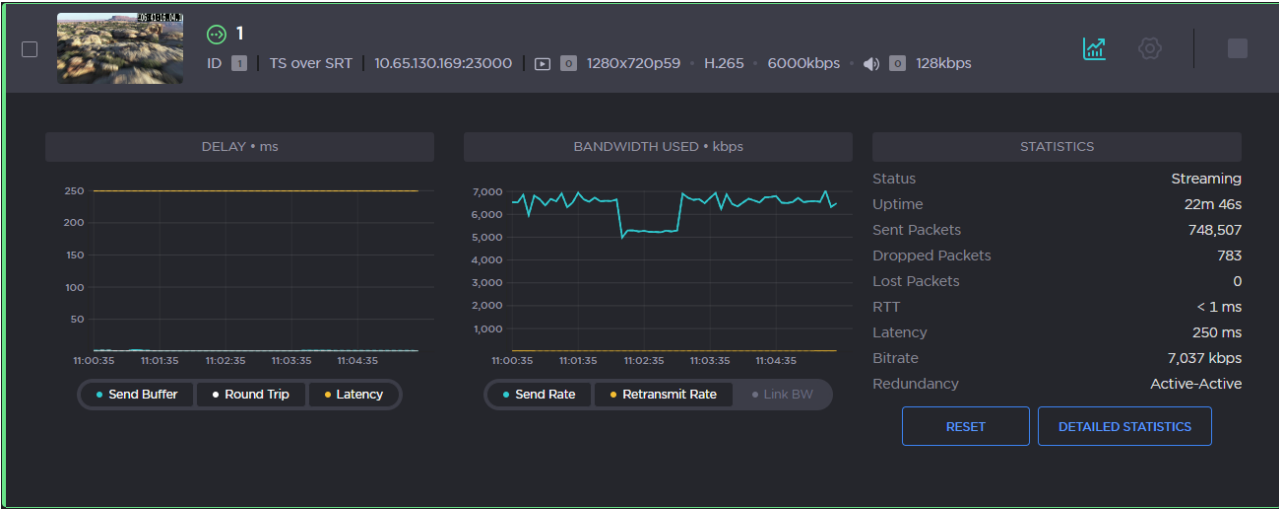
AES-128

Authentication

(None)

Passphrase

- 4. Fill out the remaining Destination, SRT Access Control and Link Parameters.
- 5. Click **Add Stream** to start the stream connection.
- 6. Click the **Statistics** icon  to see how the SRT streams are performing.
The following example shows the graphical statistics display for redundant transport streams:



7. Click **Reset** to reset the stream statistics.

8. Click **Detailed Statistics** to open the detailed statistics page.

[Back to Streams](#)

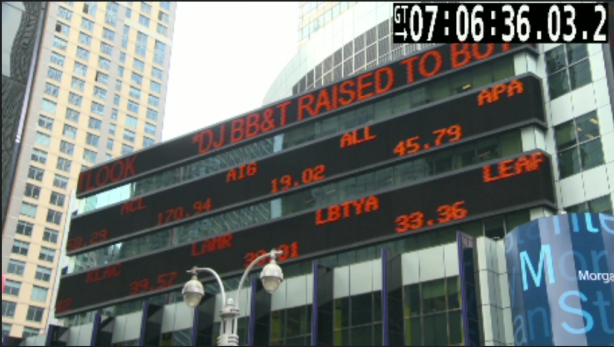
STATISTICS

RESET

DOWNLOAD CSV

1

OUTPUT REVIEW



Last 5 minutes

Last 60 minutes

Last 24 hours

Show Paths
All

DELAY • ms



• Send Buffer

• Round Trip

• Latency

BANDWIDTH USED • kbps



• Send Rate

• Retransmit Rate

• Link BW

STATISTICS

ID	1
Status	Streaming
Encapsulation	TS over SRT
Uptime	48m 16s
Sent Packets	1,734,047
Sent Bytes	2,156,017,800
Unsent Packets	19
Unsent Bytes	23,960
Bitrate	5,280 kbps
Redundancy	Active-Active

SRT (version 1.5.2)

Status	Streaming	2
Peer Version	1.5.2	1.5.2
Reconnections	3	1
Local Port	58509	54418
Resent Packets	0	1
Resent Bytes	0	1,360
Lost Packets	0	1
Dropped Packets	783	0
Dropped Bytes	8,550,664	0
Received ACKs	166,794	162,368
Received NAKs	0	1
Max Bandwidth	8,340 kbps	8,340 kbps
Path Max Bandwidth	111,323 kbps	136,543 kbps
MTU	1376	1376
RTT	< 1 ms	< 1 ms
Local Buffer Level	4 ms	4 ms
Latency	250 ms	250 ms

ERRORS

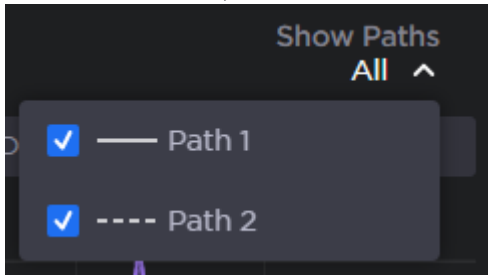
Last Error

104, (Connection reset by peer)

Occurred

45m52s ago

- a. Select which path (or both) to display from the Show Paths dropdown (path redundancy must be enabled).



- b. Adjust graphs to display the Delay and Bandwidth Used in the last: 5 minutes, 60 minutes, or 24 hours.
 - c. Click **Reset** to reset the stream statistics.
 - d. Click **Download CSV** to download the CSV file. The CSV file merges both paths.
9. Click **Back to Streams** to return to the Streams List View.

Related Topics

- [Stream Settings](#)
- [Stream Statistics](#)
- "Haivision Path Redundancy: Hitless Switching and Resilient Video Streaming Over Unpredictable Networks" (White paper, available on <https://www.haivision.com/resources/white-paper/>)

Configuring SRT Access Control

In order to connect with SRT services that use the Stream ID identification mechanism (SRT 1.4 or later), you can assign a Stream ID to an SRT stream. The Stream ID can be used by applications to differentiate between ingest streams and apply user-password access methods, as well as to send more than one stream to a single UDP destination.

The Stream ID is interchanged when a connection is being established in an SRT Caller-Listener connection layout. The Stream ID is a string with a maximum of 512 characters set on the caller side. It can be retrieved at the listener side, and based on this information, the application can accept or reject the connection, select the desired data stream, or set an appropriate passphrase for the connection. The Stream ID uses UTF-8 encoding. For more details, see [Stream Settings](#)>SRT Settings>SRT Access Control.

Here is an example following the recommended convention. `#!::u=admin,r=ietf_107_srt_overview`

To assign a Stream ID to an SRT stream:

1. Follow the steps in [Configuring Secure Reliable Transport \(SRT\)](#) to set up the SRT stream.
2. On the Stream Detail View, select the **TS over SRT** protocol and **Caller** mode.
3. Toggle **SRT Access Control** on and select either **Standard Keys** or **Custom** for the Format.
 - **Standard Keys:** Select to auto-fill the Stream Publishing ID when you fill in the Resource Name and User Name fields.
 - **Custom:** Select to enter the Stream Publishing ID using your own format.
4. Fill out the remaining Destination, SRT Access Control, and Link Parameters.
5. Click **Add Stream** to start the stream connection.

Related Topics

- [Configuring Secure Reliable Transport \(SRT\)](#)
- [Stream Settings](#)
- [Stream Statistics](#)

Stream Settings

The following sections list the Streaming Output controls and settings:

Content

Content

Streami ng 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 .. 1
Audio	Audio Encoder 0	Select the Audio Encoder to assign to the stream. • None (no content source selected) • Audio Encoder 0 .. 3  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  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.
SCTE 35 (Ad Insertion)	None	(Optional - only available as a licensed feature) To enable ad insertion, select one of the following from the SCTE 35 drop down menu: • (None) • Select the defined ad insertion source, e.g., HD-SDI-BNC-1 For more information, see Setting Up Streams and Configuring Ad Insertion Sources
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

Streaming Parameters

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
SCTE 35 PID	64	(Optional) Adinsertion (SCTE-35) 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
TS 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 Stream Settings#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.  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
Metadata Bandwidth	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 estimates the bitrate used by the metadata sources in that stream. - Enter a value in kbps between 0 and 10,000.
Bandwidth Overhead (%)	15%	(CBR/CVBR streams) Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-100%
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)  Important A DiffServ or DSCP (Differentiated Services Code Point) value must be converted to a ToS precedence value. For example, AF41 or DSCP 34 becomes ToS 136. For more information, see RFC2474.  Note The ToS setting must be chosen so as to not interfere with Voice over IP systems and other equipment that may reside on your network. For example, when the ToS value for a stream is set to 0xB8, it can interfere with some third party Voice / IP Telephony systems.
Pro-MPEG FEC Settings (TS over RTP only)		

Level	B	The level of Forward Error Correction (FEC) protection: • A (Column only): uses the column FEC stream. • B (Row and Column): uses both column and row FEC streams.
Columns	10	The number of columns in the FEC matrix.
Rows	5	The number of rows in the FEC matrix.
Block Aligned	Enabled	Specifies the type of FEC matrix scheme. • Check this checkbox to align the FEC blocks in the matrix structure (i.e., sequential columns within a group start on the same row). • If left unchecked, the blocks are a staggered series of FEC packets (i.e., each column starts on the row below the row on which the previous column started).  Note The enabled Block Aligned setting corresponds to the aligned FEC discussed in Annex C of SMPTE 2022-1. The disabled Block Aligned setting corresponds to the non-aligned FEC discussed in Annex B of SMPTE 2022-1.

SRT Settings

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. • Listener: The SRT stream acts like a server, and listens and waits for clients to connect to it.  Note The firewall must be configured to allow incoming Caller connections to reach the Listening device. • Rendezvous: Allows calling and listening at the same time.  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.
Path Redundancy	None	(Optional) 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 Configuring SRT Path Redundancy.
Path Name	n/a	(Path Redundancy must be Active-Active) Type in descriptive labels for Path 1 and Path 2.
Address	n/a	(Caller and Rendezvous modes) Specifies the destination IP address for the SRT stream.  Tip You can also enter a Fully Qualified Domain Name (FQDN).
Source Port	n/a	(Caller mode) Specifies the UDP source port for the SRT stream. If not filled in, a (default) source port will be assigned.  Note This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.
Destination Port	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.

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 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  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
Authentication	n/a	(Only available if Encryption is enabled) Configures Authenticated-Encryption with Associated-Data (AEAD). Options are: None - Default for Caller and Rendez-vous modes. Not available for Listener mode. Auto - Default for Listener mode. Not available for Caller or Rendez-vous modes. AES-GCM - Available for Caller, Listener, and Rendez-vous modes.  Note Setting the authentication to Auto allows the Listener to accept Callers with authentication set to either None or AES-GCM. Listeners with the authentication set to AES-GCM will only accept Callers which are also set to AES-GCM.
Password	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%	(SRT streams only) Specifies the maximum stream bandwidth overhead that can be used for lost packets recovery. Range = 5-50%  Note SRT streams may temporarily overshoot the defined bandwidth overhead limit.
SRT Access Control		

Format	Standard Keys	(SRT Caller only) Select the format to configure the Stream Publishing ID: - Standard Keys: Simplifies defining the Stream Publishing ID. The Stream Publishing ID field is read-only and auto-fills when you fill in the Resource Name and User Name fields. Example Standard Keys format Stream ID: #!::u=admin,r=haivision1,m=publish - Custom: Select Custom to enter the Stream Publishing ID using your own format.  Tip If you first select Standard Keys format and fill in the Resource Name and User Name fields, you can then modify or complete the resulting Stream Publishing ID by switching to Custom format. See Configuring SRT Access Control.
Resource Name	n/a	(Standard Keys only) r : Resource Name identifies the name of the resource and facilitates selection should the listener party be able to serve multiple resources.
User Name	n/a	(Standard Keys only) u : 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.
Stream Publishing ID	n/a	(Standard Keys) Read-only/auto-filled when Resource Name and User Name fields filled in. (Custom Format) Enter the Stream Publishing ID using your own format.

SAP

Session Announcement Protocol (SAP)

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

General

General

Streaming Setting	Icon	Description/Values
These icons become available to control a stream once it has started streaming (after you click Add Stream).		
Stop/Start		Click to stop or start (as applicable) an active stream.
Settings		Click view or modify the stream settings.
Statistics		Click to view the statistics for the stream. See Stream Statistics .

Related Topics

- [Network and Management Interfaces](#) (in [Technical Specifications](#))

Stream Statistics

The following table lists the Streaming Output statistics:


Tip

Scroll down for SRT graphical statistics example.

Output

Output Statistic	Description/Values
State	The current operating status of the stream, either: • STREAMING • STOPPED • LISTENING • CONNECTING • SECURING • RESOLVING • SCRAMBLED • FAILED For details, see Configuring Streams .
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.

SRT

SRT Statistic	Description/Values
Path	(Redundant connections only) Descriptive path names (if assigned), or Path 1 and Path 2.
State	The current operating status of the stream or redundant connections, for example, CONNECTING, STREAMING, STOPPED, or PAUSED.
Peer Version	(Redundant connections only) The SRT version used for the connections.
Reconnections	Number of reconnections since the stream started. Severe network congestion may cause the connection to drop and automatically reconnect.
Source Port	The UDP source port for the SRT stream or redundant connections, i.e., the port from which the encoder is sending the stream.

SRT Statistic	Description/Values
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
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.
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	Encoder buffers in milliseconds. SRT encoder buffers are unacknowledged stream packets (reception not confirmed by the receiver/decoder). The encoder buffer in absence of congestion or packet lost is around the RTT value. In presence of recoverable packets lost, the value should be between the RTT and Latency. Encoder buffers above Latency will most probably have an impact on the decoder and affect the user's experience.  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:

[Back to Streams](#)

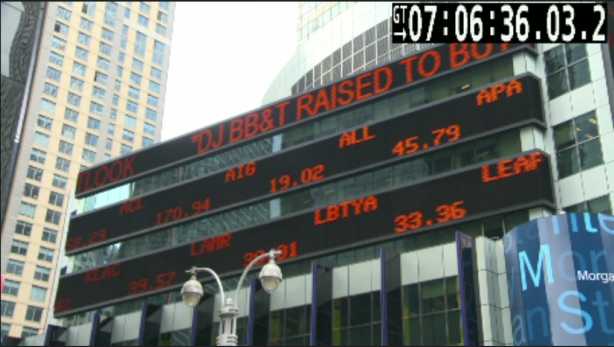
STATISTICS

RESET

DOWNLOAD CSV

1

OUTPUT REVIEW



Last 5 minutes

Last 60 minutes

Last 24 hours

Show Paths

All

DELAY • ms

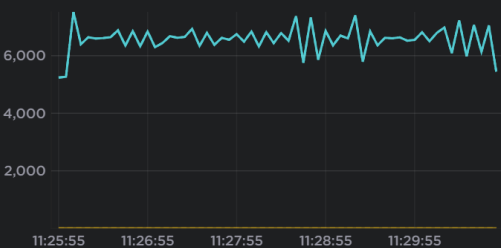


• Send Buffer

• Round Trip

• Latency

BANDWIDTH USED • kbps



• Send Rate

• Retransmit Rate

• Link BW

STATISTICS

SRT (version 1.5.2)

ID	1	1	2
Status	Streaming	Streaming	Streaming
Encapsulation	TS over SRT	Peer Version	1.5.2
Uptime	48m 16s	Reconnections	3
Sent Packets	1,734,047	Local Port	58509
Sent Bytes	2,156,017,800	Resent Packets	0
Unsent Packets	19	Resent Bytes	0
Unsent Bytes	23,960	Lost Packets	0
Bitrate	5,280 kbps	Dropped Packets	783
Redundancy	Active-Active	Dropped Bytes	8,550,664
		Received ACKs	166,794
		Received NAKs	0
		Max Bandwidth	8,340 kbps
		Path Max Bandwidth	111,323 kbps
		MTU	1376
		RTT	< 1 ms
		Local Buffer Level	4 ms
		Latency	250 ms

ERRORS

Last Error104, (Connection reset by peer)

Occurred45m52s ago

HVS-ID-UG-MX1E-13

99

Makito X1 Rugged



Note

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

Configuring Ad Insertion Sources

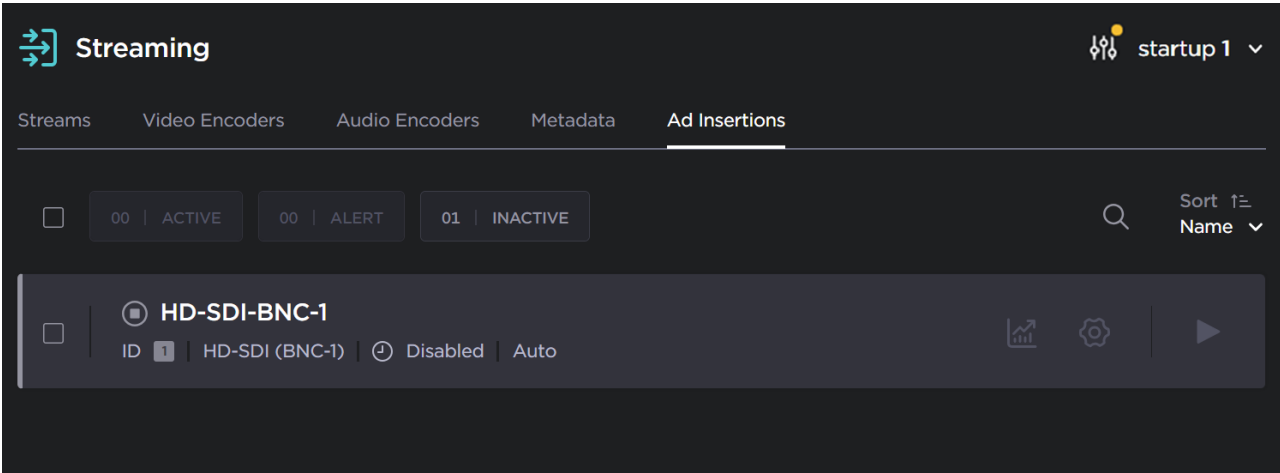


Note

Ad insertion is a licensed feature. For more information on licensing, see [Managing Licenses](#).

To open the Ad Insertions list view:

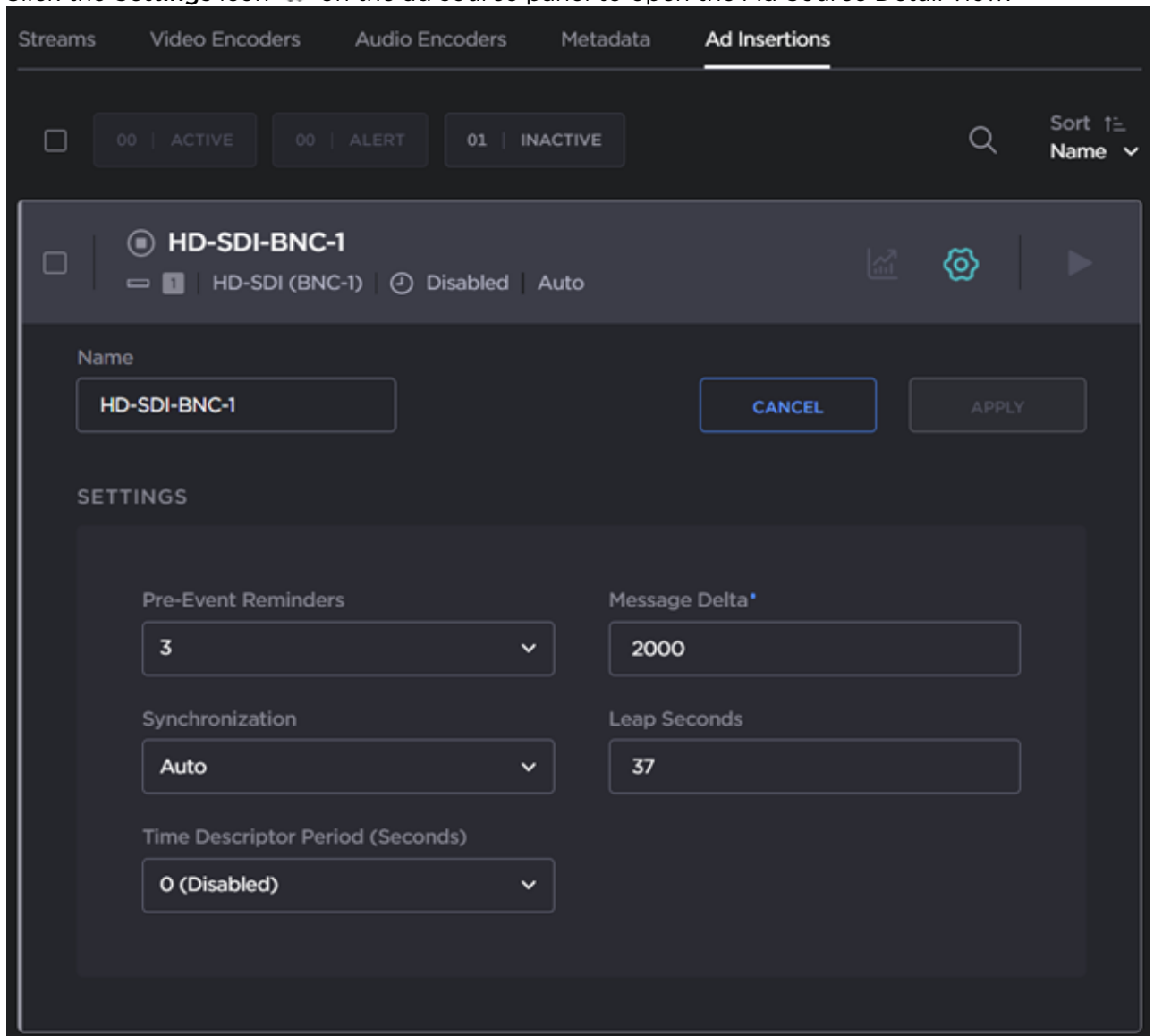
- 1. Click **Streaming** on the sidebar, and select the **Ad Insertions** tab.
The Ad Insertions list view opens, displaying the list of ad sources:



The Ad Insertions list view displays the name, type, timing, synchronization mode, and status of each ad source.

- 2. Click the **Start/Stop** icon (as applicable) to start or stop the ad source.

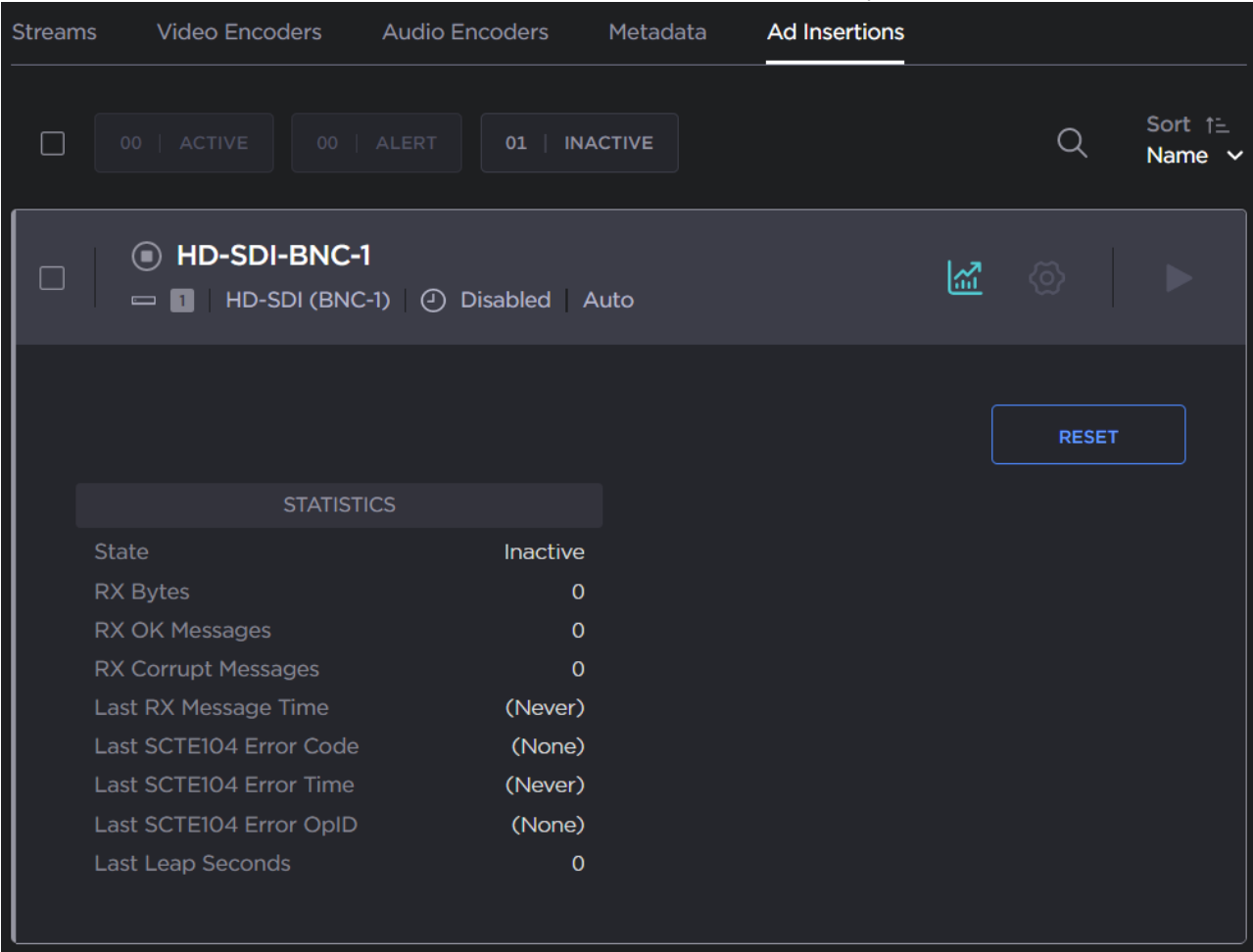
- Click the **Settings** icon  on the ad source panel to open the Ad Source Detail view:



The screenshot shows the 'Ad Insertions' tab in the HAIVISION interface. At the top, there are tabs for 'Streams', 'Video Encoders', 'Audio Encoders', 'Metadata', and 'Ad Insertions'. Below these, there are three buttons: '00 | ACTIVE', '00 | ALERT', and '01 | INACTIVE'. A search icon and a 'Sort ↑ Name' dropdown are also present. The main panel displays the details for 'HD-SDI-BNC-1', which is currently 'Disabled' and set to 'Auto'. Below this, there is a 'Name' field with the value 'HD-SDI-BNC-1' and 'CANCEL' and 'APPLY' buttons. The 'SETTINGS' section contains four configuration options: 'Pre-Event Reminders' (set to 3), 'Message Delta' (set to 2000), 'Synchronization' (set to Auto), and 'Leap Seconds' (set to 37). There is also a 'Time Descriptor Period (Seconds)' dropdown set to '0 (Disabled)'.

From here you can edit the source name, and configure the ad source settings.

4. To view the statistics, click the **Statistics** icon  on the ad source panel.



Tip

You can also configure Ad Insertions through the Command Line Interface (CLI) using the `adinsertion` command. See [adinsertion](#).

Related Topics

- [Managing Licenses](#)
- [Setting Up Streams](#)
- [adinsertion](#) (CLI)

Ad Insertion Settings

Parameter	Default	Description/Values
Name	n/a	A unique descriptive name of up to 63 characters. 'none' can be used to revert to the default name.

Parameter	Default	Description/Values
Pre-Event Reminders	3	Number of event reminders to send to downstream equipment. Range from 1 to 5.
Message Delta	2000 (without parameters)	Interval (in milliseconds) between event reminders. Range from 100 to 10,000ms (with parameters).
Synchronization	Auto	Options are: Auto - Auto-select the sync mode based on what SCTE-104 messages are being received. The priority of selected sync methods is as follows (in decreasing order): Alive, Time, System. Alive - Force the use of the received SCTE-104 alive_request_data() messages as the means to synchronize the time between the upstream SCTE-104 source and the Makito. Time Descriptor - Force the use of the received SCTE-104 insert_time_descriptor() messages as the means to synchronize the time between the upstream SCTE-104 source and the Makito. System - Use the local system time as the means to synchronize the time between the upstream SCTE-104 source and the Makito. NTP should be configured as the local time source.  Note These modes only apply when time deferred SCTE-104 requests are requested from upstream SCTE-104 sources.
Leap Seconds	37	Leap seconds added since Jan 1, 1958 to convert UTC to TAI.
Time Descriptor Period	0 (disabled)	Period (in seconds) to force the insertion of time_descriptor. Range from 0 (disabled) to 60.


Note

You can also configure the Ad Insertion settings from the Command Line Interface (CLI). See [adinsertion](#).

Ad Insertion Statistics

Ad Insertion Statistic	Description/Values
State	The state of the SCTE-104 message processing. Values are: - WORKING - STOPPED
RX Bytes	The number of SCTE-104 message bytes received. Should increment when a SCTE-104 message is received.
RX OK Messages	The number of correctly formatted and parsed SCTE-104 messages processed. Should increment if when a valid SCTE-104 message is received
RX Corrupt Messages	The number of corrupted SCTE-104 messages received/rejected.

Ad Insertion Statistic	Description/Values
Last RX Message Time	The time elapsed (in seconds and milliseconds) since the last received SCTE-104 message.
Last SCTE104 Error Code	A description of the last error encountered.
Last SCTE104 Error Time	The time elapsed (in seconds and milliseconds) since the last encountered error.
Last SCTE104 Error OpID	The last SCTE-104 Operation ID (command type) which generated an error.
Last Leap Seconds	The last value of 'leap seconds' received.



Note

You can also view Ad Insertion statistics from the Command Line Interface (CLI). See [adinsertion](#).

System Administration

This section explains how to manage and maintain the Makito X1 encoder, set up accounts, and configure security settings using the Web interface.

**Note**

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

Topics Discussed

- [Viewing System Status Information](#)
 - [Status Settings](#)
 - [Rebooting the Encoder](#)
 - [Taking a System Snapshot](#)
 - [User Preferences](#)
- [Saving and Loading Presets](#)
- [Installing Firmware Updates](#)
- [Configuring Network Settings](#)
 - [Network Settings](#)
- [Configuring Date and Time](#)
 - [Date and Time Settings](#)
- [Enabling and Disabling Network Services](#)
 - [Services Settings](#)
 - [Enabling ONVIF Support and Milestone Integration](#)
 - [Pairing the Encoder with Haivision EMS](#)
 - [Configuring RTSP](#)
- [Managing Licenses](#)
- [Managing the COM Port](#)
 - [COM Port Settings](#)

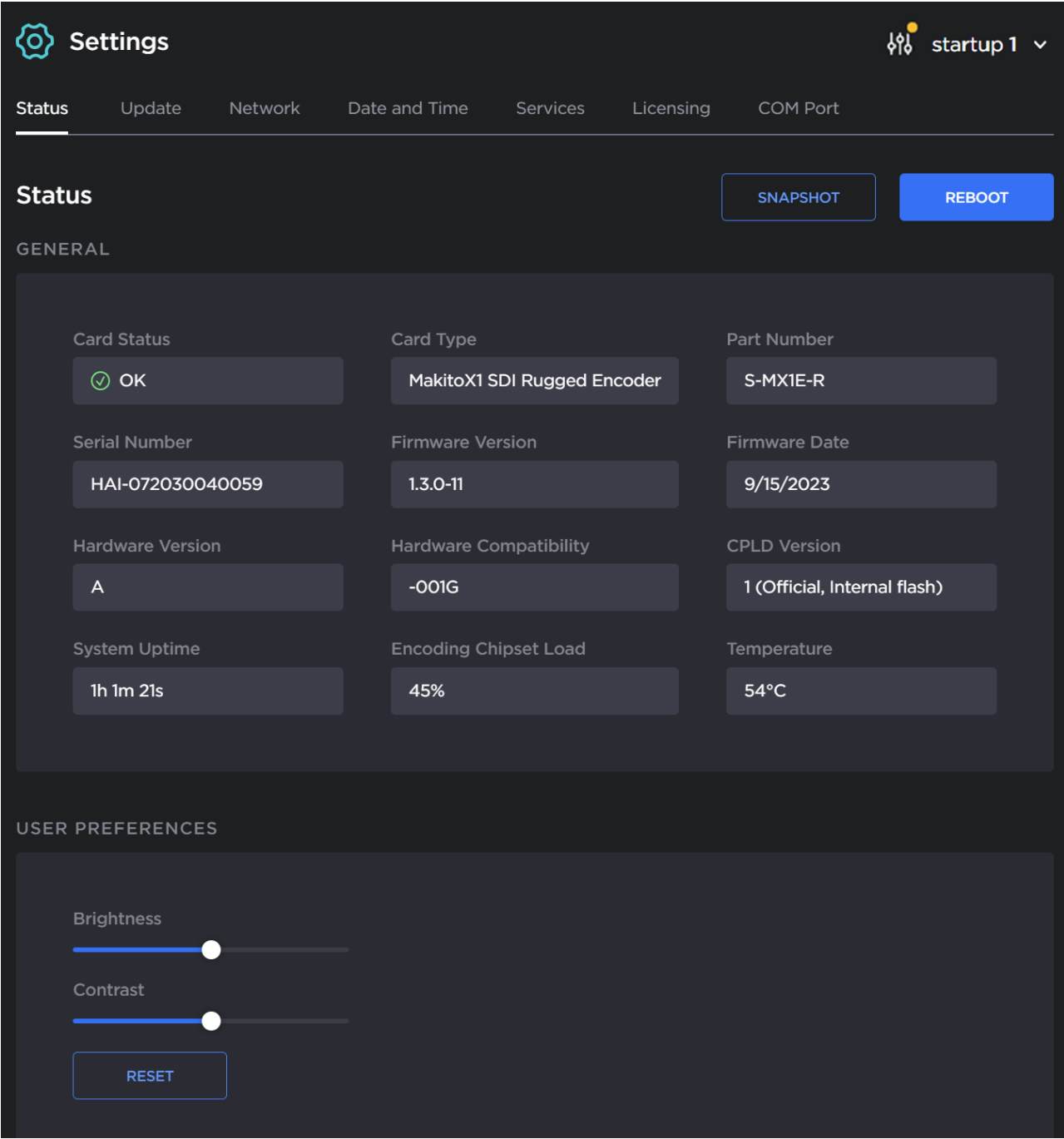
Viewing System Status Information

From the Status page, you can view status information about the Makito X1, such as the operating system uptime, along with information about the hardware and software components. You can also 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 **Settings** from the sidebar, and select the **Status** tab.
The status page opens, as in the following example:



The General Status settings are read-only. For details, see [Status Settings](#).

- 2. To display a snapshot of system information, click **Snapshot**. For details, see [Taking a System Snapshot](#).
- 3. To reboot the encoder, click **Reboot**. For details, see [Rebooting the Encoder](#).
- 4. Scroll down (when applicable) to configure User Preferences. For details, see [User Preferences](#).

Topics Discussed

- [Status Settings](#)
- [Rebooting the Encoder](#)
- [Taking a System Snapshot](#)
- [User Preferences](#)

Status Settings

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

Status Setting	Description/Values
Card Status	OK (or error message if applicable).
Card Type	The type of device, e.g., MakitoX1 SDI Rugged Encoder.
Part Number	The Haivision part number for the encoder or decoder, e.g., S-MX1E-R.
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.
CPLD Version	The Complex Programmable Logic Device (CPLD) version.
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 **Settings** on the sidebar, and select the **Status** tab.
2. Click the **Reboot** button on the top right of the page.

The encoder will reboot and you will be returned to the Sign-in page. If you turned off Preset Auto-Save and did not save your configuration/presets, you will end up with the default configuration with no streams at all.



Tip

You can also reboot the encoder from **Network** and from **Services**. See [Configuring Network Settings](#) and [Enabling and Disabling Network Services](#).

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 **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(hais Secur),512(haioper)

-----
Local Time:
-----
Wed Feb 12 17:28:45 EST 2020

-----
Universal Time:
-----
Wed Feb 12 22:28:45 UTC 2020

-----
System UP Time:
-----
17:28:45 up 35 min,  0 users,  load average: 0.00, 0.03, 0.00

-----
Manufacturing Information:
-----
MAC Address   : 5c:77:57:00:de:60
Serial Number : HAI-031935020010
Boot Revision : U-Boot 2018.01 (Sep 12 2019 - 16:33:51 -0400) Xilinx ZynqMP MakitoX1E

-----
Card Temperature:
-----
Temperature Status:
  Current Temperature : 41 Celsius measured 0s ago
  Maximum Temperature : 42 Celsius measured 11m12s ago
  Minimum Temperature : 41 Celsius measured 35m37s ago
Debug Statistics:
  Invalid Readings    : 0
  Discarded Deltas    : 0

-----
System Information:
-----
Card Type       : "MakitoX1 SDI Rugged Encoder"
Part Number     : S-MX1E-R
Serial Number    : HAI-031935020010
MAC Address      : 5c:77:57:00:de:60
Firmware Version : 1.0.0-18
Firmware Date    : "Feb 12 2020"
Firmware Time    : "16:32:42"
Hardware Version : A
Hardware Compatibility : -001G
Boot Version     : "U-Boot 2018.01 (Sep 12 2019 - 16:33:51 -0400)"

-----
Installed Debian Packages:
-----
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version          Description
++-----+-----+-----+
ii makitox1-boam  0.0.0-1         MakitoX1 Base Operation and Management
```

2. Save the file.

**Tip**

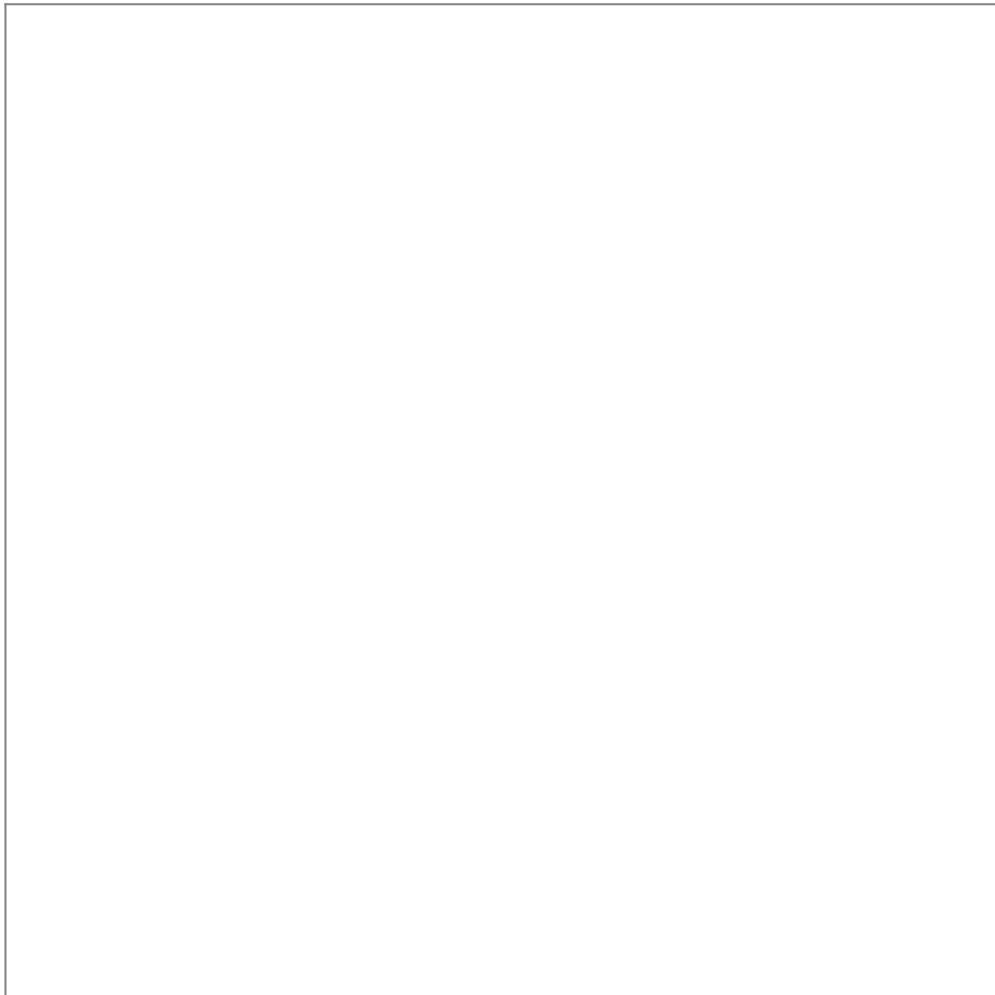
You can also take a system snapshot from the CLI using the [system_snapshot.sh](#) command.

User Preferences

To access the User Preferences, click **Settings** on the sidebar, and select the **Status** tab. Scroll down (if applicable) to see the user preference options.

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

- Adjust Brightness and Contrast display settings using the sliders.
- Click **Reset** to reset the Brightness and Contrast to the default settings.
- Click **Clear** to Clear Stored Preferences, i.e., User Preference settings that are saved by the browser, such as sort order, sort field, current tab, etc.



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.



Note

Preset Auto-Save is enabled by default. This feature is designed to help users who have not saved their configurations into presets, to prevent loss of configuration settings when signing out or rebooting or the power is disconnected on their units. If you disable **Preset Auto-Save**, you will have to manually save your preset configurations.



Info

If the **Preset Auto-Save** function has been disabled, an amber warning indication will appear next to the Device Presets dropdown (in the header) on systems with unsaved configurations.



Streaming

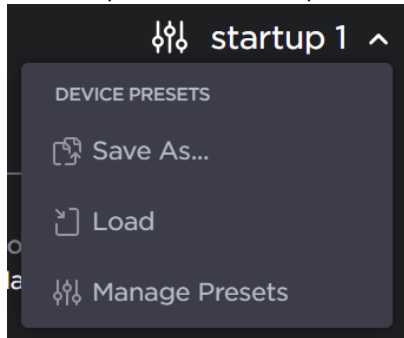


startup 1 ▾

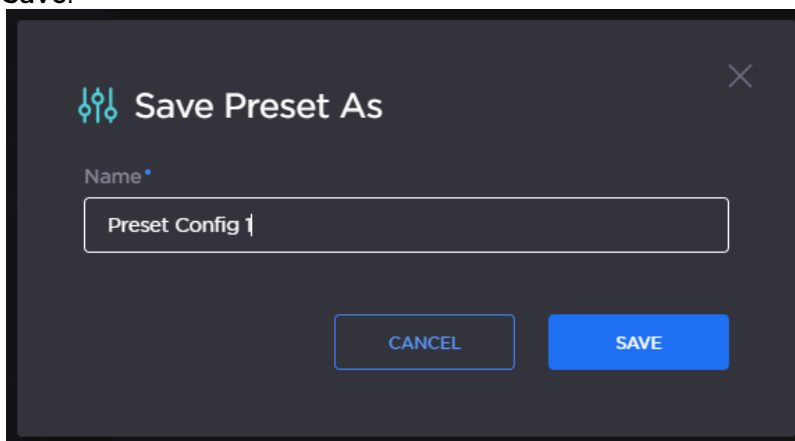
To view and manage presets:

1. From any page, click **Device Presets** dropdown in the header.

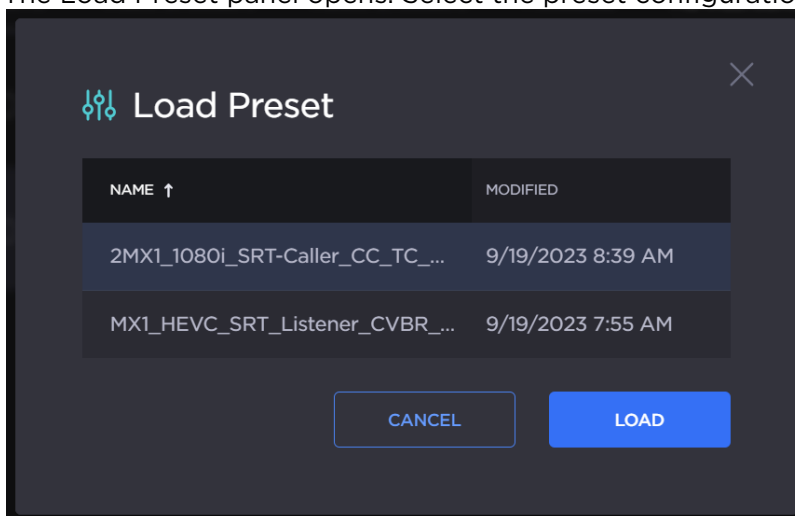
The dropdown menu opens.



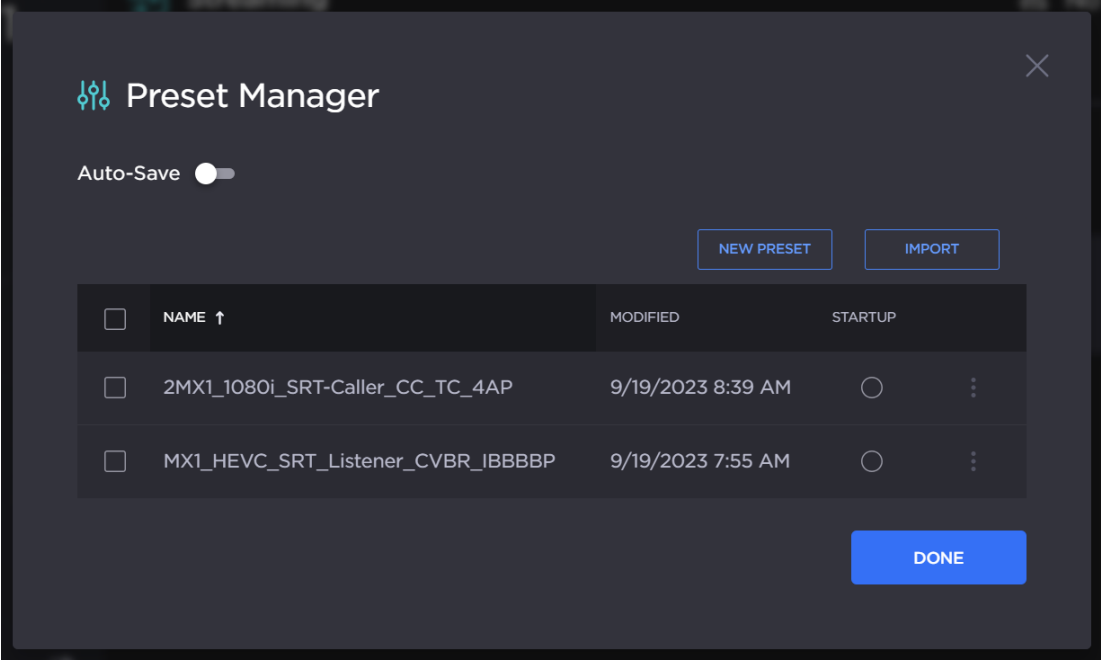
2. To save the current configuration as a new preset, click **Save As...** from the dropdown menu.
 - a. The Save Preset As panel opens. Type in a unique name for the preset in Name field and click **Save**.



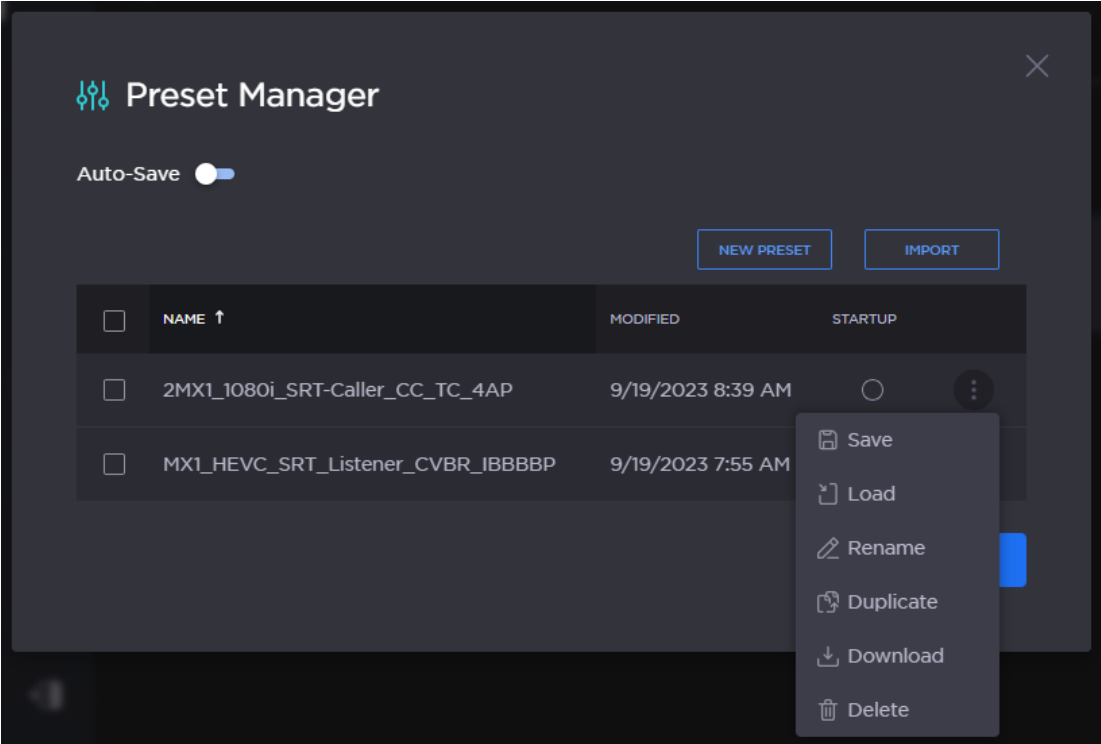
3. To apply an existing preset, click **Load**.
 - a. The Load Preset panel opens. Select the preset configuration from the list and click **Load**.



- 4. To access the preset manager, click **Manage Presets**.
The Preset Manager panel opens displaying the list of saved presets for the encoder.



- a. The startup preset is marked by a blue radio button in the Startup column.
 - b. To enable or disable Preset Auto-Save, toggle **Auto-Save** on or off.
- 5. To load an existing preset into the current session, click the vertical ellipsis menu in the preset row and click **Load**.



- 6. From this menu you can also:

- a. Click **Save** to apply any present changes to a defined preset.
- b. Click **Rename** to rename an existing preset.
- c. Click **Duplicate** to duplicate an existing preset.
- d. Click **Download** to download the preset as a text file to view or export to other Makito X1 encoders.
- e. Click **Delete** to delete the existing preset.
7. To select an existing preset to load at startup, click the radio button under the Startup column in the desired preset row.
8. To create a new preset, click **New Preset**. The New Preset panel opens.
 - a. Type in a unique name for the new preset configuration.
 - b. Click **Create**.

New Preset

Name *

New Preset 1

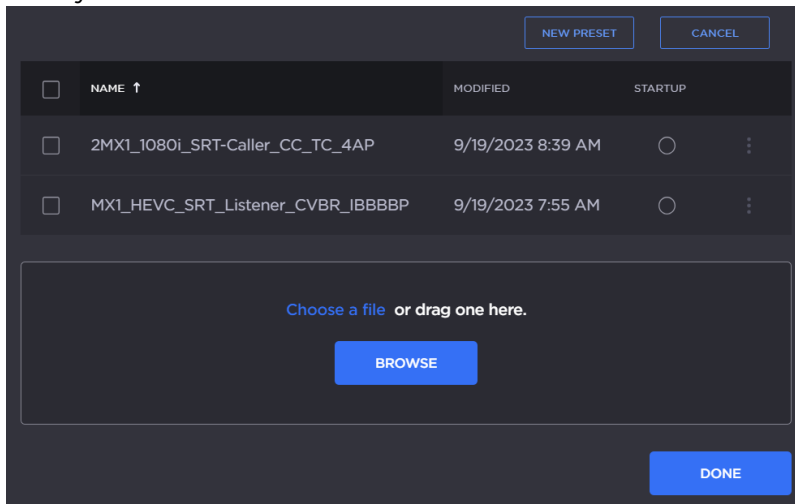
CANCEL CREATE

- c. The New Preset is added to the Presets List.

☐	NAME ↑	MODIFIED	STARTUP
☐	2MX1_1080i_SRT-Caller_CC_TC_4AP	9/19/2023 8:39 AM	☐
☐	MX1_HEVC_SRT_Listener_CVBR_IBBBBP	9/19/2023 7:55 AM	☐
☐	New Preset 1	9/19/2023 3:55 PM	☐

9. To import a preset, for example, from another Makito X1 encoder, click **Import**.

- a. To upload a preset file, drag the file into the File dialogue box, or click Browse to select it from your files.



- b. When you see the file name in the text box, click **Upload**.
10. To Delete one or more existing preset(s), check the checkbox(es) in the preset row(s) and click **Delete**.
 - a. To delete all existing presets, check the checkbox in the header column to select all, and click **Delete**.

Installing Firmware Updates

**Note**

Before you can install a firmware update on the Makito X1, 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 a Makito X Series appliance, the necessary firmware is pre-installed on it. Firmware upgrades 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 upgrade becomes available, you can easily install it from the Web interface. You will first need to copy the upgrade file to your local computer or network.

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

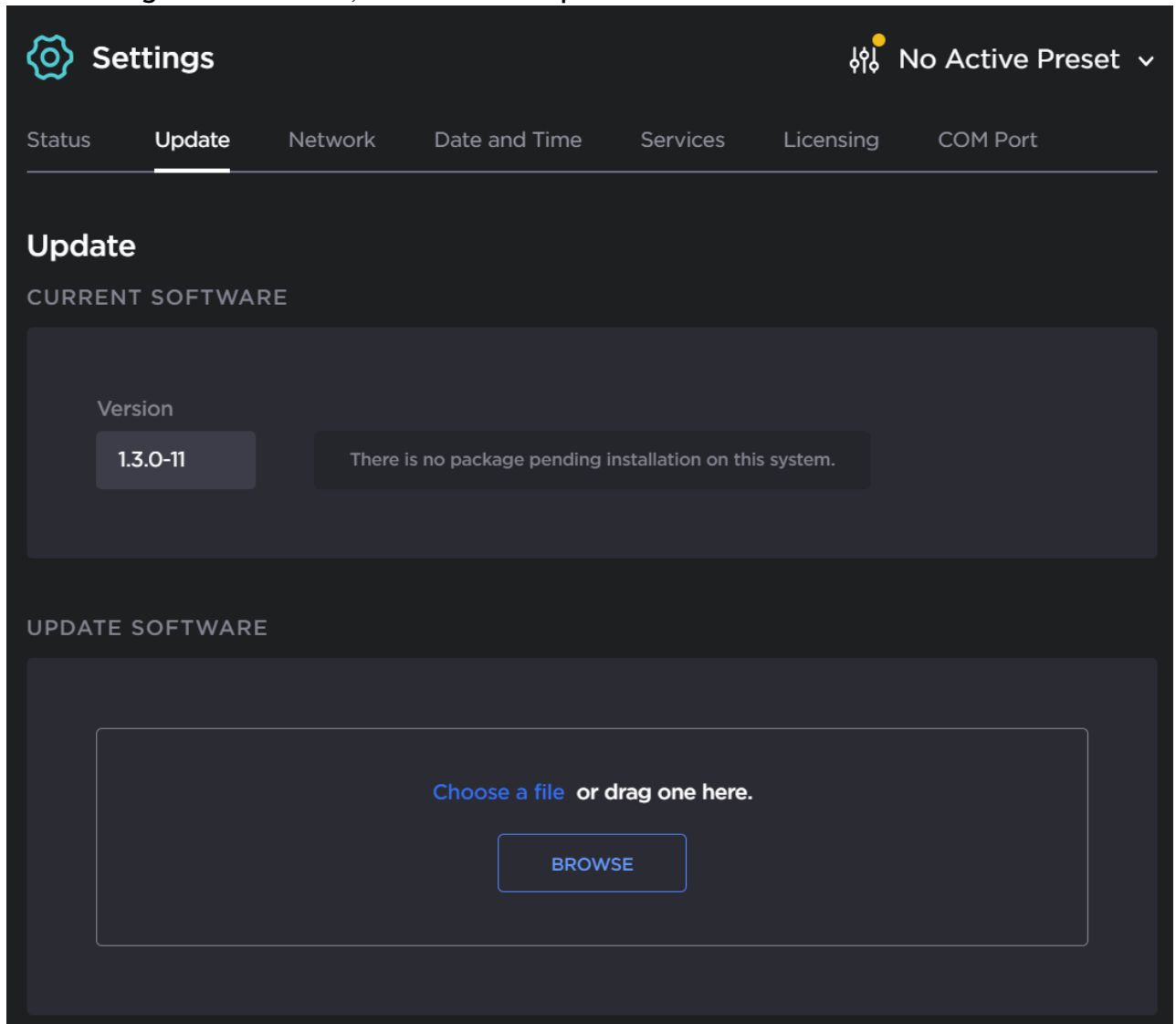
This section provides instructions to install a firmware upgrade from the Web interface.

**Tip**

Do not delete existing licenses before uploading the new license when upgrading to a new release.

To install a firmware update:

1. Click **Settings** on the sidebar, and select the **Update** tab.



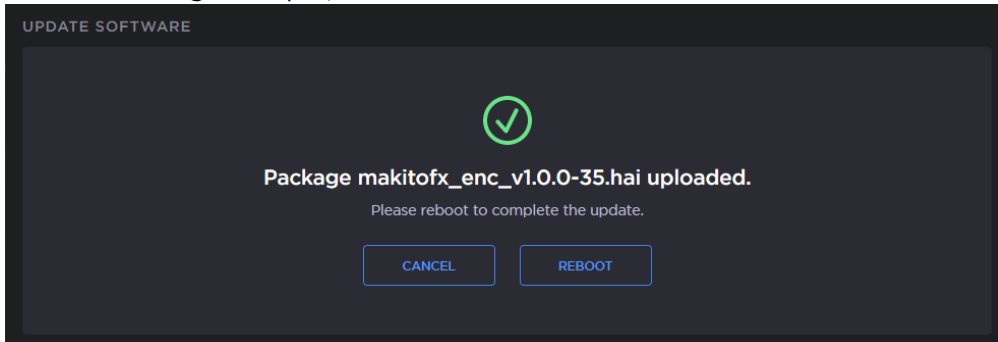
2. Drag and drop the file into the Open File dialogue box, or select the file by clicking **Browse**.
3. When you see the filename in the text box, click **Upload**. If you have chosen an incorrect file, click **Cancel**.
4. Wait for the file to be uploaded and verified and the file system synced.

**Note**

Remain on this page and do not click anything else in the Makito X1 Web interface during the upload.

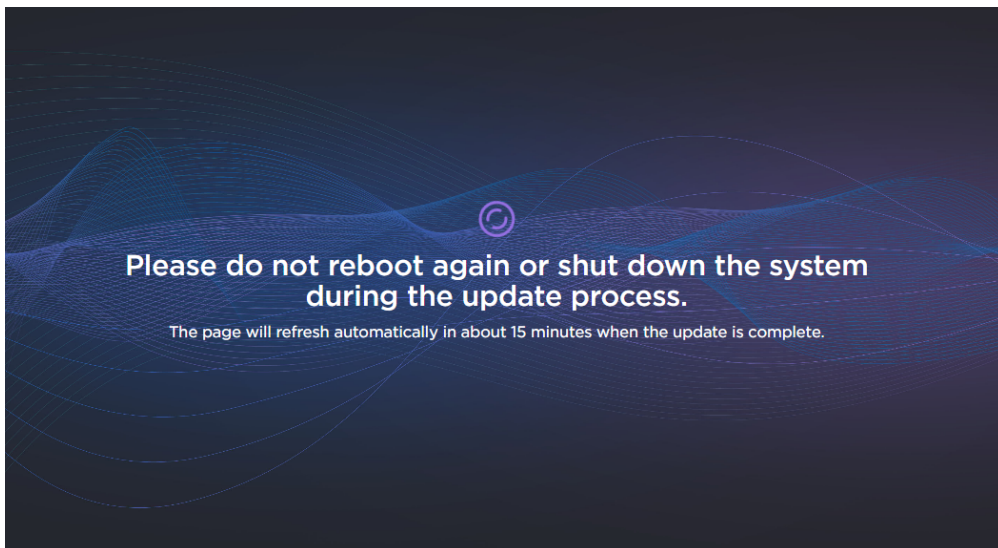
If any of the package components has been modified or is not signed by a valid certificate, the verification will fail and the downloaded package will be discarded.

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.

6. 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.
7. Clear your browser cache after the firmware upgrade.
8. 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

From the Network Configuration page, you can modify the network interface settings for the Makito X1, including configuring the unit with a valid IP address and gateway to work in your environment. You can configure the network to use either IPv4 or IPv6 addressing, or both. The default is IPv4.

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. Click **Settings** on the sidebar, and select the **Network** tab.
The Network Configuration page opens, displaying configuration options for:

a. The Network Hostname and Interfaces

StatusUpdateNetworkDate and TimeServicesLicensingCOM Port

Network

REBOOTAPPLY

GENERAL

Hostname*

MX1-HAI-072030040059

INTERFACE

IPv4

Addressing

Static

IP Address*10.65.131.97

Netmask*255.255.255.0

Gateway*10.65.131.1

IPv6

b. Ethernet settings

LinkAutomatic

SpeedAny

Current Speed1000

DuplexFull

MAC Address5c:77:57:00:f6:93

Total TX Bandwidth*1000000

c. DNS settings

DNS

Domain

eqa.haivision.com

☐ Obtain DNS Settings Automatically

Primary DNS Server Address

10.65.158.10

Alternate DNS Server Address

DNS Precedence

IPv6

☒ Enable mDNS

mDNS Identifier

MX1-HAI-072030040059

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

IPv6:

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

IPv6 ☒

Addressing

Automatic (DHCP) ▾

Automatic

Automatic (DHCP)

Static

Link

Speed

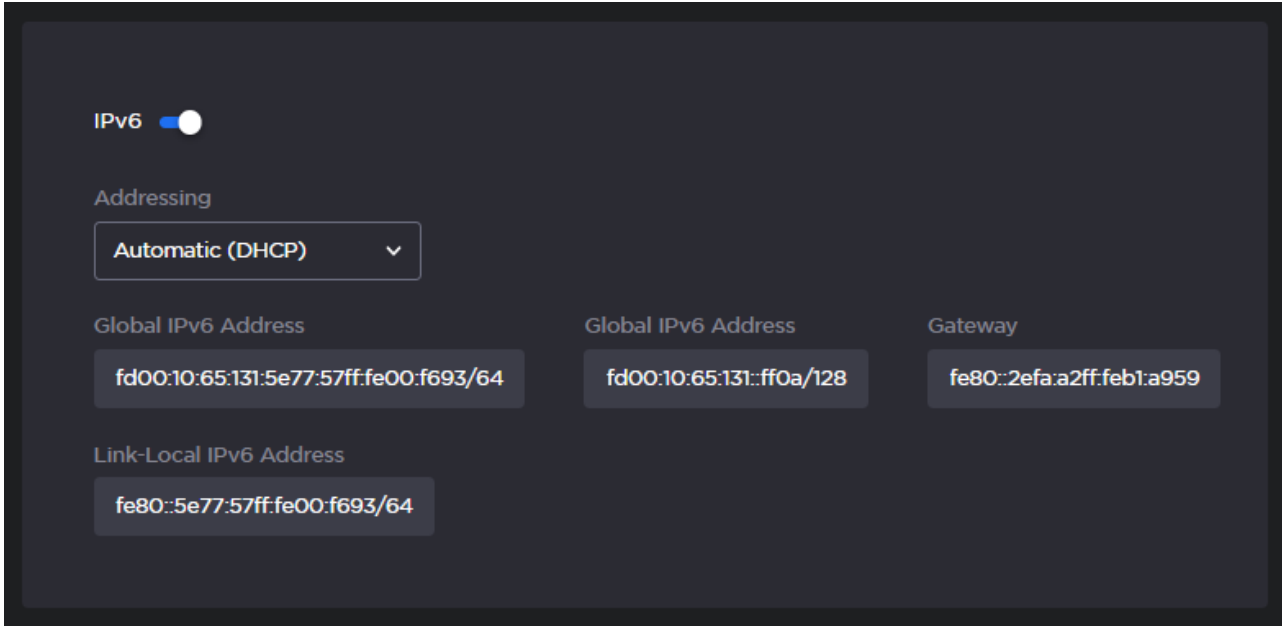
Current Speed

- 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.



Topics Discussed

- [Network Settings](#)

Network Settings

The following table lists the Encoder Network settings:

General

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

IPv4

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" for the 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 Prefix Length	(Static Addressing only) The Prefix Length in IPv6 is the equivalent of the Subnet Mask in IPv4. However, instead of being expressed in four octets as it is in IPv4, it is expressed as an integer between 1 through 128.
Gateway	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-specific	
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.
DNS Precedence	Select either IPv4 or IP v6 to specify the priority for DNS resolution. On systems with both IPv6 and IPv4 enabled, if users use HOSTNAMES instead of specifying IP addresses when creating connections, the default behavior is to resolve to IPv6 first if it is available.
Enable mDNS	Check this checkbox to enable the Multicast DNS (mDNS) protocol as a means for third party entities to discover the IP address of the Makito X.  Tip Enabling mDNS allows an mDNS application to automatically find the Makito X. mDNS is enabled on units shipped from the factory or reset to factory defaults to allow them to advertise their existence. A user can then click Locate (Status page) to start the Status and TX or RX LEDs flashing in order to discover the location of the device, for example, within a large server room.
mDNS Identifier	(Optional) Enter a unique name for the Makito X. By default, the system creates a unique name, e.g. "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.

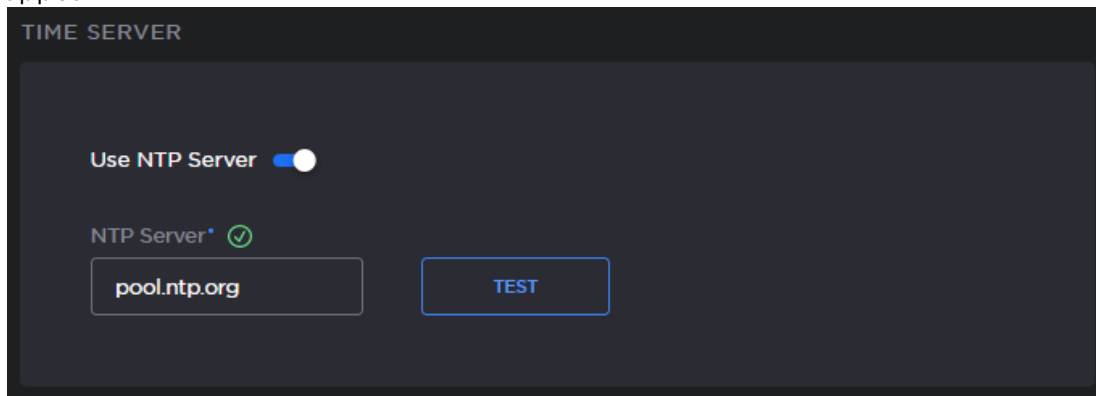
To view and configure the date and time:

1. Click **Settings** on the sidebar and select the **Date and Time** tab
The Date and Time page opens.

The screenshot shows the 'Date and Time' configuration page in the HAIVISION interface. The page has a dark theme. At the top, there is a navigation bar with tabs: Status, Update, Network, Date and Time (selected), Services, and Licensing. Below the tabs, the 'Date and Time' section is visible. It contains three buttons: REBOOT, STATISTICS, and APPLY. Below these buttons, the 'TIME SERVER' section is shown. It includes a toggle for 'Use NTP Server' which is currently turned on. Below the toggle, there is an 'NTP Server*' field containing the text 'pool.ntp.org' and a 'TEST' button. Below the 'TIME SERVER' section, the 'TIMEZONE' section is visible. It features a 'Timezone - Locale' dropdown menu showing '(GMT-05:00) Eastern Time - Montreal' and a 'Current Time' field displaying '5/25/2023 12:16 PM'.

2. Select or enter the new value(s) in the appropriate field(s). For details, see [Date and Time Settings](#).
3. Toggle Use NTP Server off to manually set the date and time.
4. Select the time zone from the **Timezone - Locale** dropdown. The current date and time according to the Timezone will appear in the Current Time field.
5. To apply your changes, click **Apply**.
6. To validate that the NTP server is reachable, click **Test** (next to the NTP server field). Once the test is complete, a 'Valid NTP Server' message will pop up, and a green checkmark will

appear.



7. Click **Reboot** to finish connecting to a valid NTP server, and to apply date and time changes (if configured manually).
8. To view statistics for the NTP server, click **Statistics**.
A pop-up displaying the NTP statistics will appear.

NTP Statistics

Tracking

Reference ID : A29FC87B (162.159.200.123)

Stratum : 4

Ref time (UTC) : Thu May 25 18:10:51 2023

System time : 0.000370087 seconds slow of NTP time

Last offset : -0.000033448 seconds

RMS offset : 0.000665606 seconds

Frequency : 0.287 ppm fast

Residual freq : +0.001 ppm

Skew : 0.084 ppm

Root delay : 0.042611733 seconds

Root dispersion : 0.000938852 seconds

Update interval : 64.2 seconds

Leap status : Normal

Sources

210 Number of sources = 4

MS Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
A+ 192.95.27.155	2	7	377	110	-2773us[-2807us] +/- 49ms
A= 162.159.200.123	3	6	377	48	+1530us[+1496us] +/- 22ms
A- 198.50.127.72	2	6	377	51	-5660us[-5694us] +/- 132ms
A- 216.6.2.70	2	7	377	109	-3120us[-3154us] +/- 67ms

Source Statistics

210 Number of sources = 4

Name/IP Address	NP	NR	Span	Frequency	Freq Skew	Offset	Std Dev
192.95.27.155	19	9	977	+0.054	0.076	-2790us	22us
162.159.200.123	7	5	387	-0.864	1.233	+1488us	58us
198.50.127.72	13	8	775	+0.058	0.108	-5686us	20us
216.6.2.70	19	12	978	-0.087	0.083	-3132us	27us

CLOSE

Topics Discussed

- [Date and Time Settings](#)

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.

Enabling and Disabling Network Services

For security purposes, an administrator may need to stop one or more network services from accessing the Makito X1. From the Services page, you can enable and disable network services, including HTTP, SSH, Telnet, SNMP, RTSP, ONVIF, Haivision EMS, and Product Analytics. 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

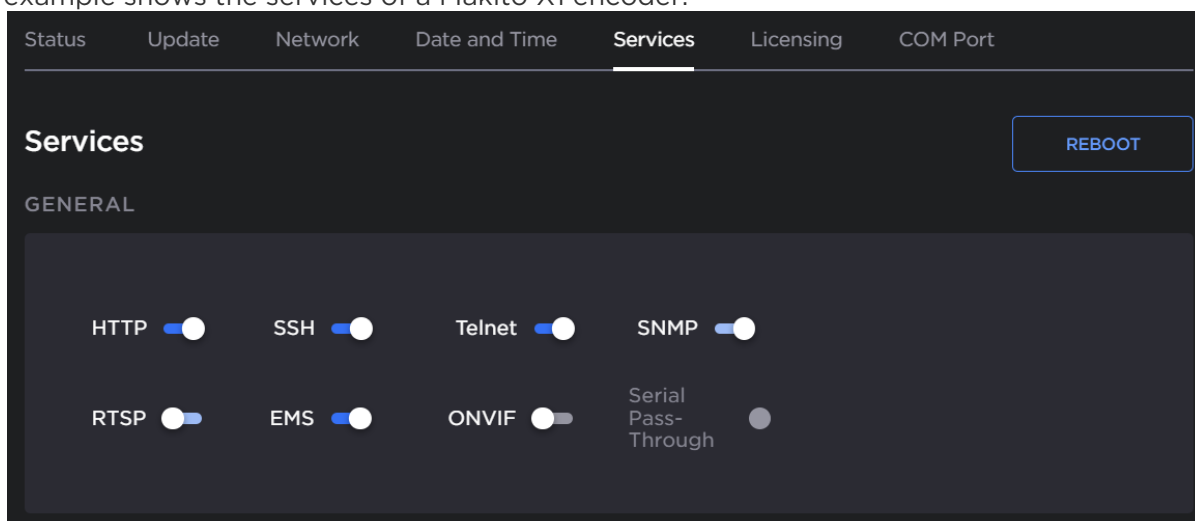
In order to optimize your encoder's performance, it is recommended that *only* the required network services be enabled. Please review the network services to make sure services used for your application are enabled or disabled as appropriate.

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 MX1 Rugged](#)).

To enable or disable network services:

1. Click **Settings** on the sidebar and select the **Services** tab.
The Services page opens displaying the current status of network services. The following example shows the services of a Makito X1 encoder:



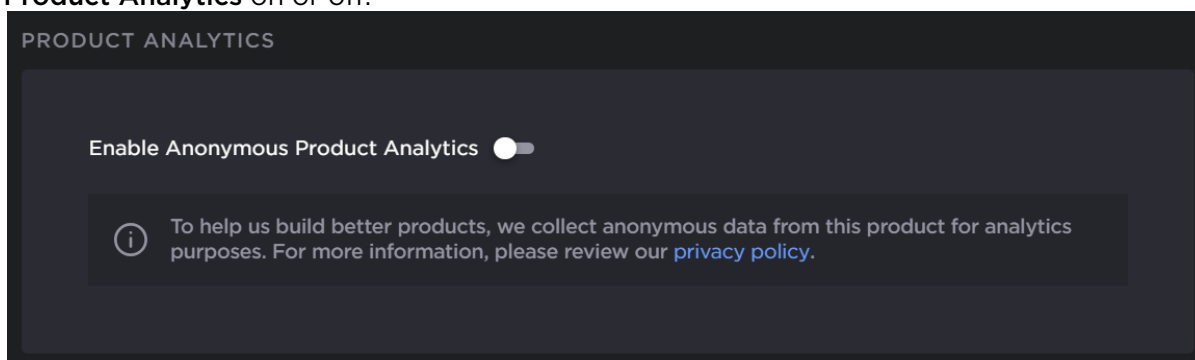


Note

The toggle color indicates the service status:

Color	Indication
Blue	Service is operating.
Grey	Service is disabled.

- To enable or disable a service, toggle the associated Service on or off. For details, see [Services Settings](#).
- To pair the encoder with Haivision-EMS, toggle **EMS** on and Configure the EMS/Cloud Services settings (located on the Services page). For details, see [Pairing the Decoder with Haivision EMS](#).
- To enable or disable the collection of anonymous product analytics, toggle **Enable Anonymous Product Analytics** on or off.



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

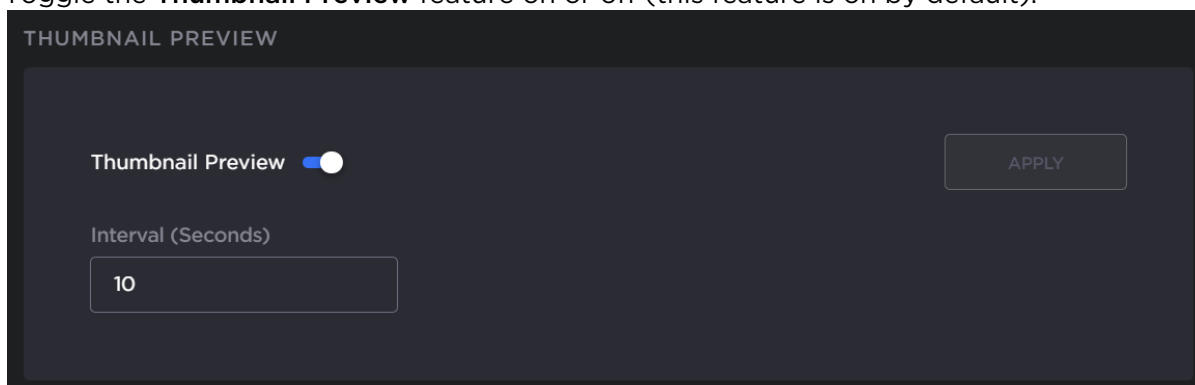


Tip

Network services can also be enabled/disabled using the CLI [service](#) command.

From the Services page you can also configure the Thumbnail Preview:

- Toggle the **Thumbnail Preview** feature on or off (this feature is on by default).



- If on, type the interval time, in seconds, in the Interval field.

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

**Note**

Preview Thumbnails appear on the Dashboard, Streams and Video Encoders pages to provide a visual reference of each video encoder's input. Preview Thumbnails can be enabled/disabled, and preview settings persist through reboot. By default, previews are enabled and set to 10 second intervals.

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)

Enabling ONVIF Support and Milestone Integration

ONVIF Integration Overview

Makito X ONVIF Support and Milestone Integration allows customers to manage Makito X encoders from the Milestone XProtect video management software (VMS) using the ONVIF protocol and API. RTSP Support enables customers to use the RTSP protocol to stream video feeds from the Makito X to the Milestone VMS for archiving and analysis.

This feature is designed to be used in applications where surveillance cameras connect to the encoders. The Milestone VMS sends commands to the encoder using the ONVIF API. The encoder sends video received from the cameras to the Milestone VMS via RTSP and Direct-RTP. The Milestone VMS stores the video as well as sends it for display.

This functionality is a licensed feature and must be purchased using the SWO-292-ONVIF part number. Enabling and disabling of the ONVIF management API is done either from the Makito X Web Interface Services page or using the CLI (`service` command).

About ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products. For more information, see <https://www.onvif.org/>.

The Makito X supports subsets of ONVIF API Profiles S and T. Both profiles are designed for IP-based video systems.

ONVIF Profile S is used for basic video streaming and configuration.

ONVIF Profile T is used for advanced video streaming and includes the following:

- H.264 / H.265 video compression
- Imaging settings
- Motion alarm and tampering events
- Metadata streaming
- Bi-directional audio



Note

The ONVIF API "GET" parameters are implemented; however, the "SET" parameters are not. This means that you can use ONVIF commands to monitor Makito X operations, but cannot control the Makito X; for example, you cannot configure the video bit rate or resolution. For details on the ONVIF APIs, please see the ONVIF documentation:
<https://www.onvif.org/profiles/profile-s/>
<https://www.onvif.org/profiles/profile-t/>
HEVC/H.265 is not supported with the initial release of the Makito X ONVIF feature.

Integration Steps

To enable the ONVIF service on the Makito X1 Rugged encoder:

Makito X1 Web Interface

1. On the Makito X1 Services page, toggle ONVIF on.
The RTSP button is automatically toggled to **On** (since RTSP is required for stream creation).
2. Select the Interface for the service (**All**, **eth0**, or **eth1**).
3. Optionally, configure the parameters, including WS-Discovery and Location, in the ONVIF panel (which appears upon enabling the service).



Note

The Makito X1 supports the ONVIF "WS-Discovery" feature (which enables network probing to locate ONVIF-capable devices). This feature is enabled by default when the ONVIF service is enabled. It is recommended to keep WS-Discovery enabled.

4. If you made changes on the ONVIF parameters, click **Apply**.
5. Scroll to the top of the Services page and click **Reboot**. The encoder must be rebooted for changes to take effect.

Milestone XProtect VMS Interface

6. To add the Makito X1 encoder to the Milestone VMS, select **Add Hardware** → **Express**.
OR
To add the Makito X1 manually, select **Add Hardware** → **Manual** → **Hardware Model** → **ONVIF Conformant Device (2-16 channels)**.
7. Select **Devices** → **Camera** → **Makito Device** → **Settings** and select the Streaming Method: either **RTP/UDP** or **RTP/RTSP/TCP**.



Note

Video is supported by XProtect in either "RTP/UDP" or "RTP/RTSP/TCP" mode. **RTP/RTSP/TCP mode** is the default selection.

8. Click **Apply**.

**Note**

If the video playback does not start, the first troubleshooting step is to completely disable the firewall on the PC that has the Milestone XProtect software. If this works, then ask your system administrator to edit the firewall rules accordingly.

Streaming should begin from the cameras.

Related Topics:

- [Enabling and Disabling Network Services](#)
- [service](#) (CLI command)
- [Rebooting the Encoder](#)

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 EMS on.
2. On the EMS/Cloud Services panel, 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.

3. (Optional) You may change the EMS Address and Port in order to override the defaults extracted from the pairing 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.

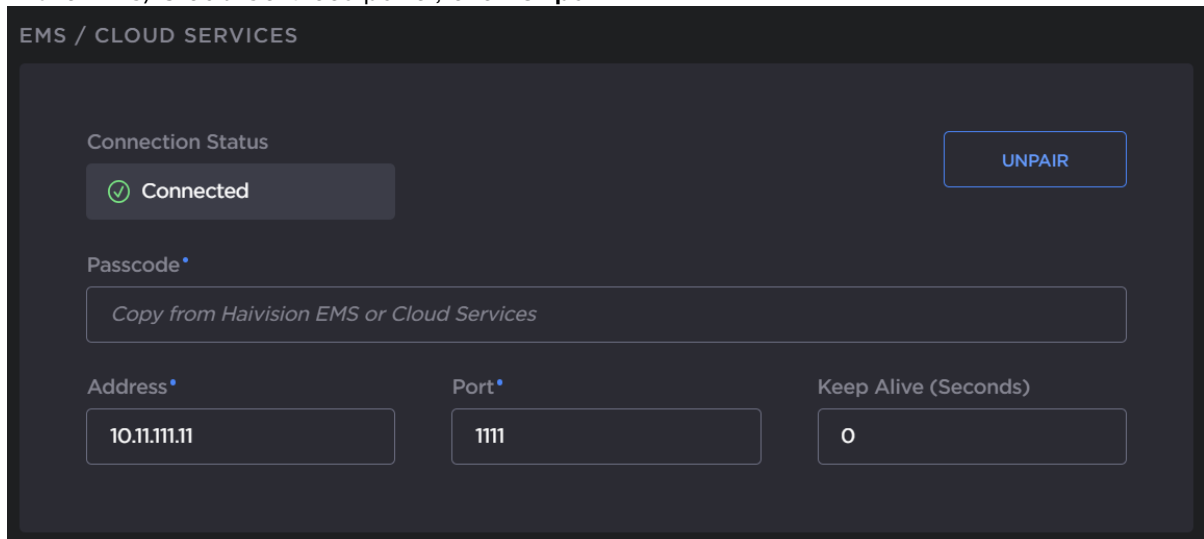
The Keep Alive value is also filled in when the pairing code is pasted in. "Keep Alive" is the time interval in seconds in which the device will ping the EMS server to maintain its connection.

5. Click **Pair**.

This initiates the pairing and communication with the EMS server.

To unpair the Makito X device from Haivision-EMS:

1. In the EMS/Cloud Services panel, click **Unpair**.



The screenshot shows a dark-themed interface for the 'EMS / CLOUD SERVICES' panel. At the top left, the title 'EMS / CLOUD SERVICES' is displayed. Below it, the 'Connection Status' is shown as 'Connected' with a green checkmark icon. To the right of the status is a blue button labeled 'UNPAIR'. Below the status is a 'Passcode' field with a red asterisk, containing the text 'Copy from Haivision EMS or Cloud Services'. At the bottom, there are three input fields: 'Address' (containing '10.11.111.11'), 'Port' (containing '1111'), and 'Keep Alive (Seconds)' (containing '0').

The unpairing takes effect immediately.

Configuring RTSP

From the Services page, you can configure the Makito X or Makito X4 encoder to interoperate with Real-Time Streaming Protocol (RTSP)-based software players such as QuickTime, VideoLan VLC, or Wowza Server (Flash) for real-time streaming.

To configure RTSP:

1. On the Services page, toggle the RTSP button on.
2. To access the RTSP stream from the decoder, you must specify the correct RTSP URL. The format should be:

`rtsp://ip_address[:port]/videncID[_audencID]`

Where:

- *ip_address* is the IPv4 address of the Makito encoder hosting the RTSP service.
- *port* is optional and only needs to be specified if the RTSP server port is not set to the default 554.
- *videncID* is mandatory and specifies the ID of an H.264 or H.265 video encoder on the Makito (from the 0-3 range for Makito X H.264 encoders, plus encoders 4-5 for HEVC mezzanines to use for H.265 streaming; and 0-7 for Makito X4).
- *audencID* is optional to include audio in the rtsp stream and specifies the ID of an audio encoder (from the 0-7 range for Makito X or 0-32 for Makito X4).



Note

Port only needs to be specified if the RTSP server port is not set to the default 554. You can use RTSP for video-only streams (typical use case is surveillance applications).

For specific examples of RTSP URLs, see below.

Customizing Stream Characteristics

Makito X v2.5 and Makito X4 v1.2 added the ability to specify optional stream link parameters in the URL. The RTSP servers in the Makito X and Makito X4 now support this URL format:

`rtsp://ip_address[:port]/videncID[_audencID][?param1=value1¶m2=value2, ...]`

Where:

- *param* are optional stream link parameters for which you provide desired values. Configurable stream link parameters values are listed below.

Supported stream link parameters:

- *tos* = 0x00 to 0xFF (for hex) or 0 to 255
- *ttl* = 1 to 255
- *mtu* = 232 to 1500
- *mcast_addr* = A valid multicast address
- *mcast_port* = A valid multicast port

Examples

An RTSP URL with an IP address of 10.65.131.50, which is using server port 554 (default), video encoder 0, and audio encoder 0 will look like this:

- `rtsp://10.65.131.50/0_0`

An RTSP URL with the same parameters as above, but using a different port (8554 in this case), will look like this:

- `rtsp://10.65.131.50:8554/0_0`

An RTSP URL with an IP address of 10.65.131.50, which is using server port 554 (default), video encoder 0, and no audio encoder, with stream link parameters `tos` (value=10), `mtu` (value=1300) and `ttl` (value=2) will look like this:

- `rtsp://10.65.131.50/0?tos=10&mtu=1300&ttl=2`

You can also stream from a Makito X to a Milestone server using RTSP. See [Enabling ONVIF Support and Milestone Integration](#).

Managing Licenses

For a list of license file errors, see:

- [License File Errors](#)

Feature licensing allows you to view the licensed [capabilities](#) of your Makito X 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:
 - a. Audio/Video Inputs

The screenshot shows the 'Licensing' page in the Haivision interface. At the top, there is a navigation bar with tabs: Status, Update, Network, Date and Time, Services, **Licensing** (selected), and COM Port. Below the navigation bar, the page title 'Licensing' is displayed. Underneath, there is a section titled 'INSTALLED LICENSES' with an 'INSTALL' button on the right. A table lists the installed licenses, with one entry: 'HAI-072030040059-Full'. Below this, there is a section titled 'LICENSE FEATURES'. Under 'System', there are two settings: 'Maximum Upgradable Release' set to '9.9' and 'Firmware Expiration Date' set to 'Never'. Under 'Audio/Video Inputs', there is a setting for 'Maximum input resolution' set to 'FHD'.

- b. Video and Audio capabilities

Video

Number of Video Encoders

2

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

High Dynamic Range (HDR)

On

Audio

Number of Audio Encoders

4

MPEG-2 AAC-LC ADTS

On

MPEG-4 AAC-LC LOAS/LATM

On

c. Metadata and Ad Insertion capabilities

Metadata

Key-Length-Value Metadata (KLV)

On

Cursor-on-Target Metadata (CoT)

On

Ad Insertion

Capture of SCTE-104/SDI and Conversion to SCTE-35

On

d. Stream and Misc capabilities

Stream

Secure Reliable Transport (SRT)

On

TS/RTP

On

TS/UDP

On

Misc

Open Network Video Interface Forum (ONVIF)

On



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.

- To install a license, click the **Install** button at the top of the Licensing page. Then, click **Browse** to select the license file, or drag and drop the file in the Open File dialog box.

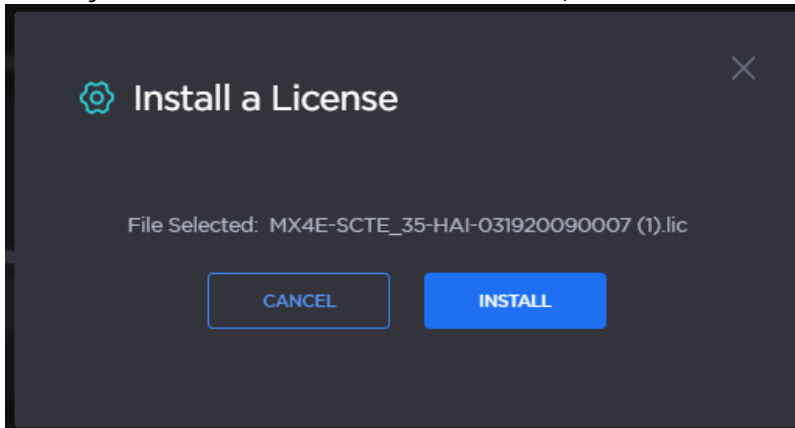
Install a License

×

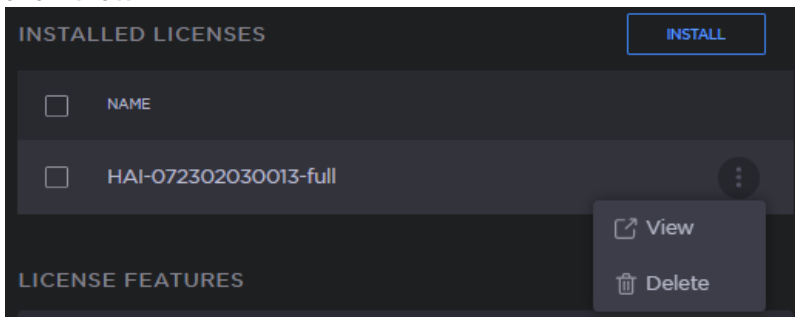
Choose a file or drag one here.

BROWSE

- When you see the filename in the text box, as in the following example, click **Install**.



- To apply your changes, click the **Reboot** button.
The encoder will reboot and you will be returned to the Sign-in page.
- To view an installed license file, click the vertical ellipsis menu in the listed license, and click **View**.



- The license file opens in a separate window, as in the following example.

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

[ADINSERTION]
SCTE-35.Descr=Capture of SCTE-104/SDI and Conversion to SCTE-35
SCTE-35=On

#wlicopt adinsertion adinsertion 0n SCTE-35

#----END LICENSED FEATURE---- adinsertion.lcf ----
#----BEGIN LICENSED FEATURE---- audio.lcf ----

[AUDENC]
Qty.Descr=Number of Audio Encoders
Qty=4

#wlicopt audio audenc 04 4

#----END LICENSED FEATURE---- audio.lcf ----
#----BEGIN LICENSED FEATURE---- avin.lcf ----

[VIDRES]
Max.Descr=Maximum input resolution
Max=UHD

#wlicopt avin vidres 40 UHD

#----END LICENSED FEATURE---- avin.lcf ----
#----BEGIN LICENSED FEATURE---- metadata.lcf ----

[METADATA]
COT.Descr=Cursor-on-Target Metadata (CoT)
COT=On

#wlicopt metadata metadata 0n CoT

KLV.Descr=Key-Length-Value Metadata (KLV)
KLV=On

#wlicopt metadata metadata 0n KLV

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

- To delete a license, click **Delete** from the vertical ellipsis menu, or check the check box next to the listed license(s) and click **Delete**.

License File Errors

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

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

Related Topics

- [license](#) (CLI command)

Managing the COM Port



Note

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

The Makito X Rugged Encoders provide 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.

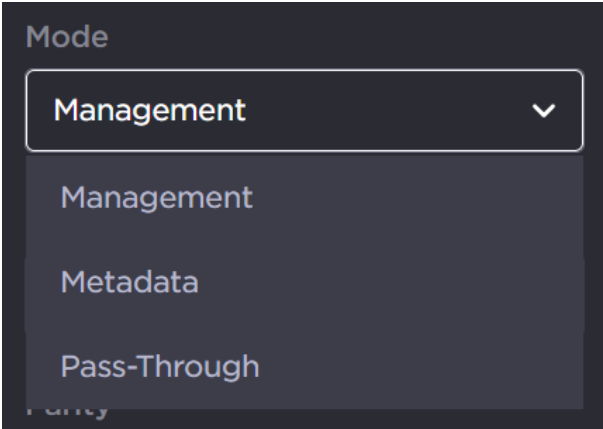
In order to configure the COM port settings to capture metadata, you need to set the COM Port Mode to Metadata and then reboot the encoder. You can then configure the COM port settings from the Metadata page.

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. Click **Settings** on the sidebar and select the **COM Port** tab.
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](#)
- [\(1.3 2\) Install the Makito X1 Rugged Encoder](#)
- [Configuring Metadata Capture](#)

COM Port Settings

The following table lists the 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" (link below).

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.
Standard	RS-232	(Read-only) The serial mode standard: • RS-232 or • RS-422

COM Port Setting	Default	Description/Values
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

Related Topics:

- [Metadata Settings](#)

Managing Users and Security

This section explains how to set up accounts and configure security settings for the Makito X1 using the Web interface.

**Note**

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

Topics Discussed

- [Managing User Accounts](#)
 - [Account Management](#)
 - [Account Settings](#)
 - [Managing Public Key Authentication](#)
- [Managing Messages](#)
- [Managing Banners](#)
- [Managing Security Policies](#)
 - [Policy Settings](#)
- [Managing Certificates](#)
 - [Generating a Certificate](#)
 - [Importing a Certificate](#)
 - [Viewing Certificate Details](#)
 - [Certificate Settings](#)
- [Managing Audits](#)
 - [Audit Settings](#)

Managing User Accounts



Note

The Accounts pages are available to administrators only (i.e., users assigned Administrator role). From here, administrators can create and manage user accounts for the Makito X (including their own accounts).

The My Account page is available to users assigned either Operator or Guest roles to change their own account password. For information, see [Changing Your Password](#).



Important

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

From the Accounts pages, administrators can create, delete and modify user accounts for the Makito X1.

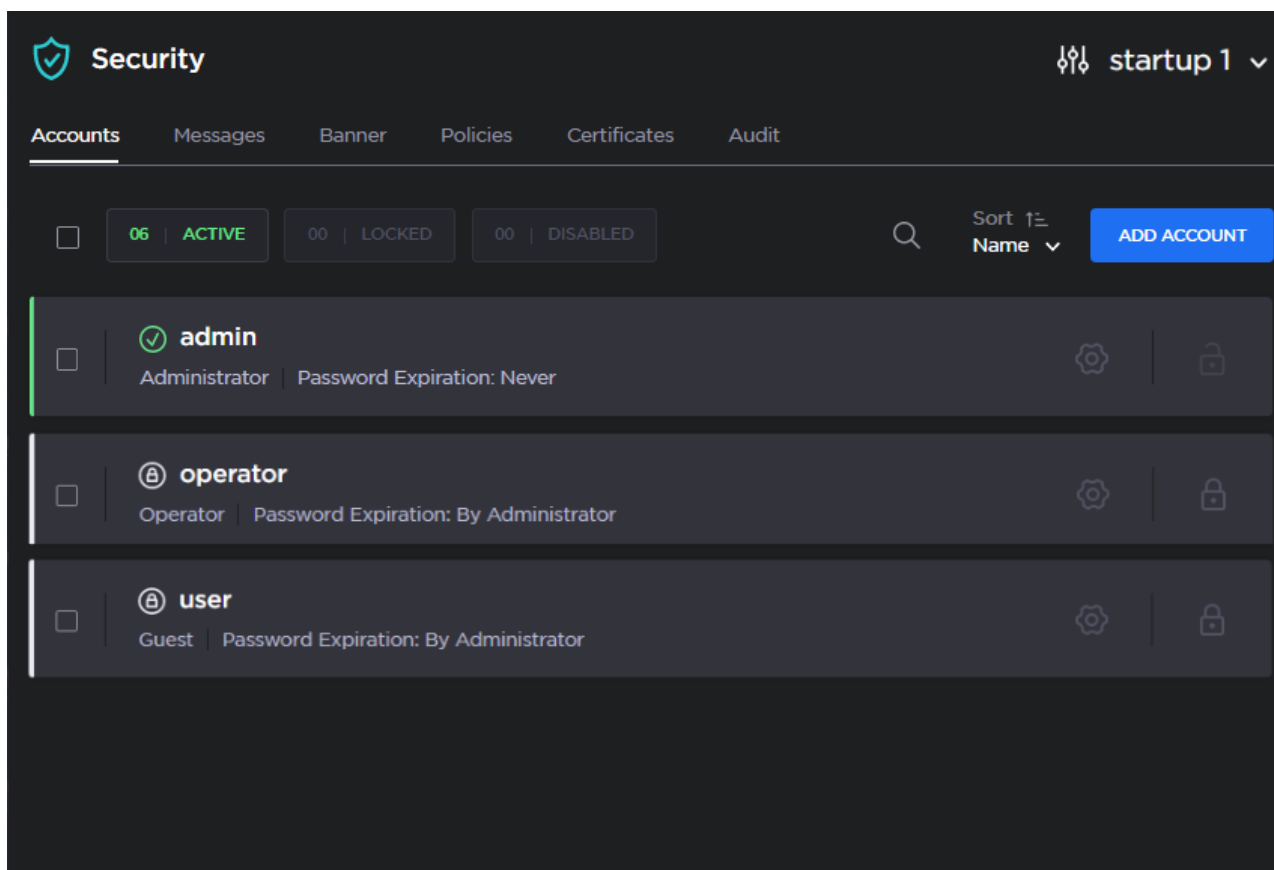
An account can be allocated to each user of the system so that the identity of the user can be uniquely determined. The Makito X1 provides three defined account roles to assign privileges to users: Administrator, Operator and Guest. For details, see [Role-based Authorization](#).

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 X1 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. Click Security on the sidebar, and select the Accounts tab.
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. From here you can lock, unlock or delete an account, as well as re-enable a disabled account.

2. To view or modify user account details (including the Username, Role, Password, and Public Keys) click the **Settings** icon  to open the Account Settings. For details, see [Account Management](#).
3. To add a new account, click the **Add Account** button. For details, see [Account Management](#).
4. To lock or unlock an account, click the **Lock/Unlock** icon  /  on the account panel.
5. If **Disable Inactive Accounts** has been turned on (see [Managing Security Policies](#)), certain accounts may be disabled. To re-enable an account, check the checkbox next to the account name, and click the **Enable** button.
6. To delete one or multiple account(s), check the checkbox(es) next to the account name(es), and click the **Delete** button.
7. To apply your changes, click **Apply**. The changes will take effect immediately.

Account Management



Tip

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

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

To add a new account:

1. From the Accounts List View, click the **Add Account** button.
2. In the Add Account panel, type a unique user name in the Username text box.



Tip

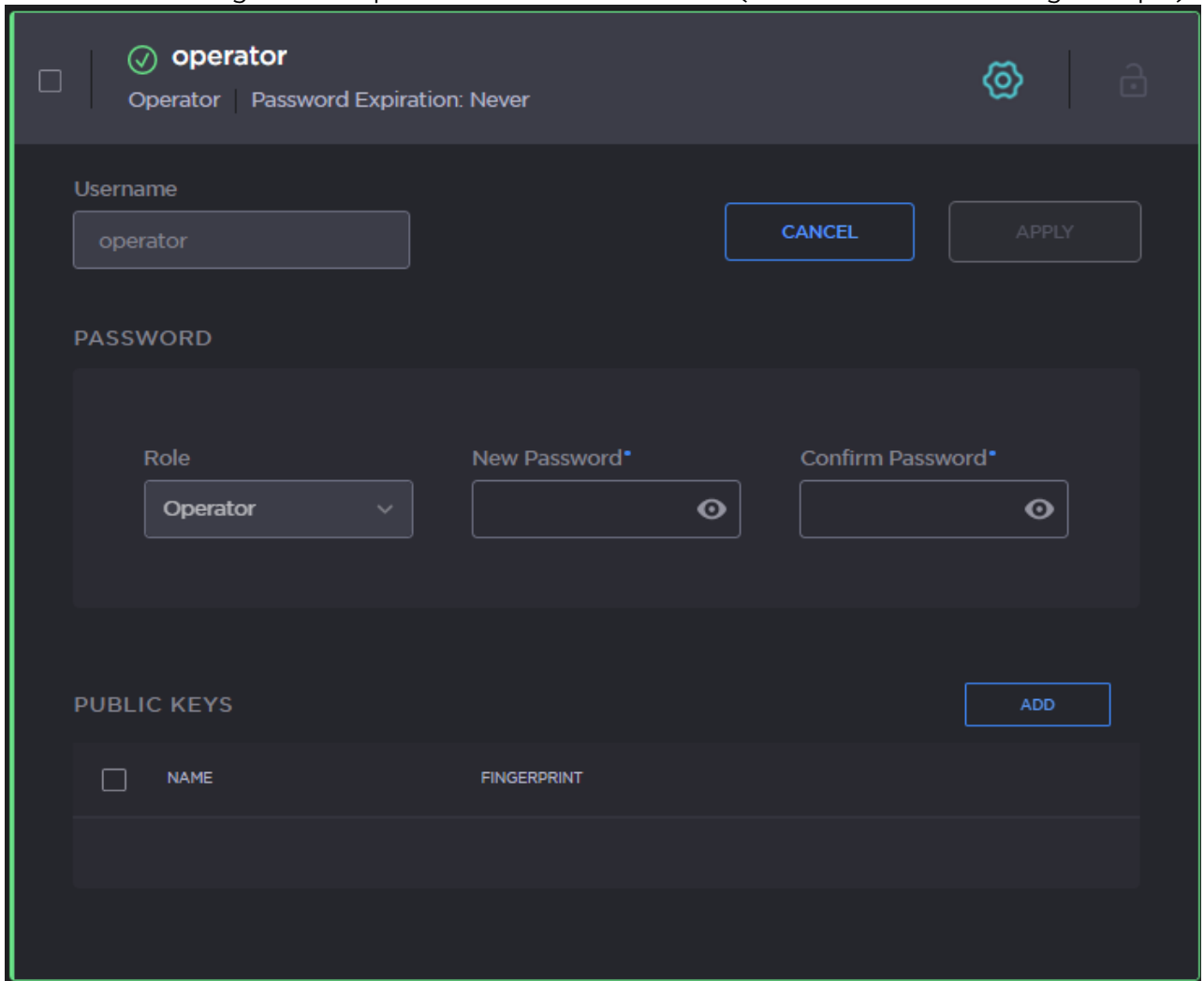
The user name must comply with Unix restrictions (lower case letters a-z, numbers 0-9, hyphen and underscore).

3. Select the Role for the user. See "Role" in [Account Settings](#).
4. Type the initial password in the Password field and again in the Confirm Password field. For the allowed characters, see "Password Requirements" in [Changing Your Password](#).

5. Click **Add Account**.

To manage existing accounts:

1. From the Accounts List View, click the **Settings** icon  in an existing account panel to view or configure the account settings.
The account settings details open for the selected account (as shown in the following example).



☐  **operator**
Operator | Password Expiration: Never

Username
operator CANCEL APPLY

PASSWORD

Role
Operator

New Password* Confirm Password*

PUBLIC KEYS ADD

☐	NAME	FINGERPRINT
☐		

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 new password into both the New Password and Confirm Password fields. For the allowed characters, see "Password Requirements" in [Changing Your Password](#).
3. To change your own password, type the current password in the Current Password field, and then type the new password in the New Password and Confirm Password fields.

**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**.

Related Topics

- [Account Settings](#)

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

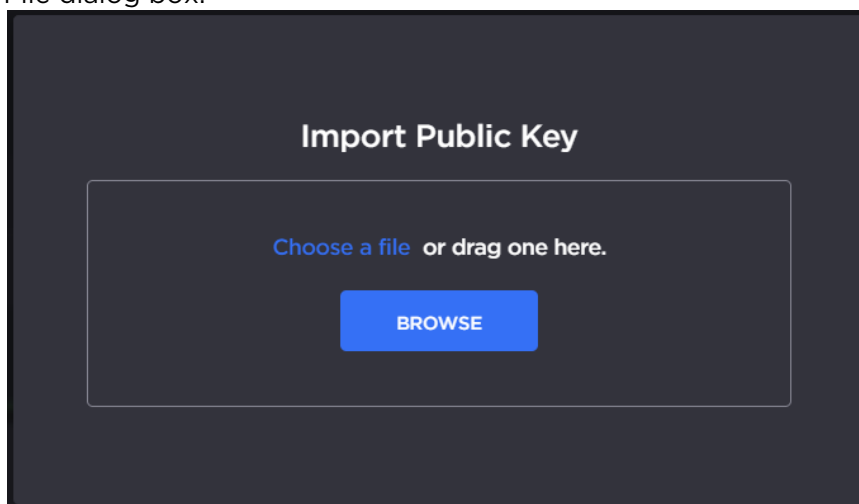
- [Role-based Authorization](#)
- "Password Requirements" in [Changing Your Password](#)
- [Managing Public Key Authentication](#)

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 the settings icon  on an existing account.
2. On the account settings drop-down, 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**.
 - a. To select a different public key file, click **Change**. To remove the selection, click **Cancel**.
4. 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.



Tip

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` server, Power-On Self Test (POST) errors, and other noteworthy events.

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

The log of the actions recorded includes the following:

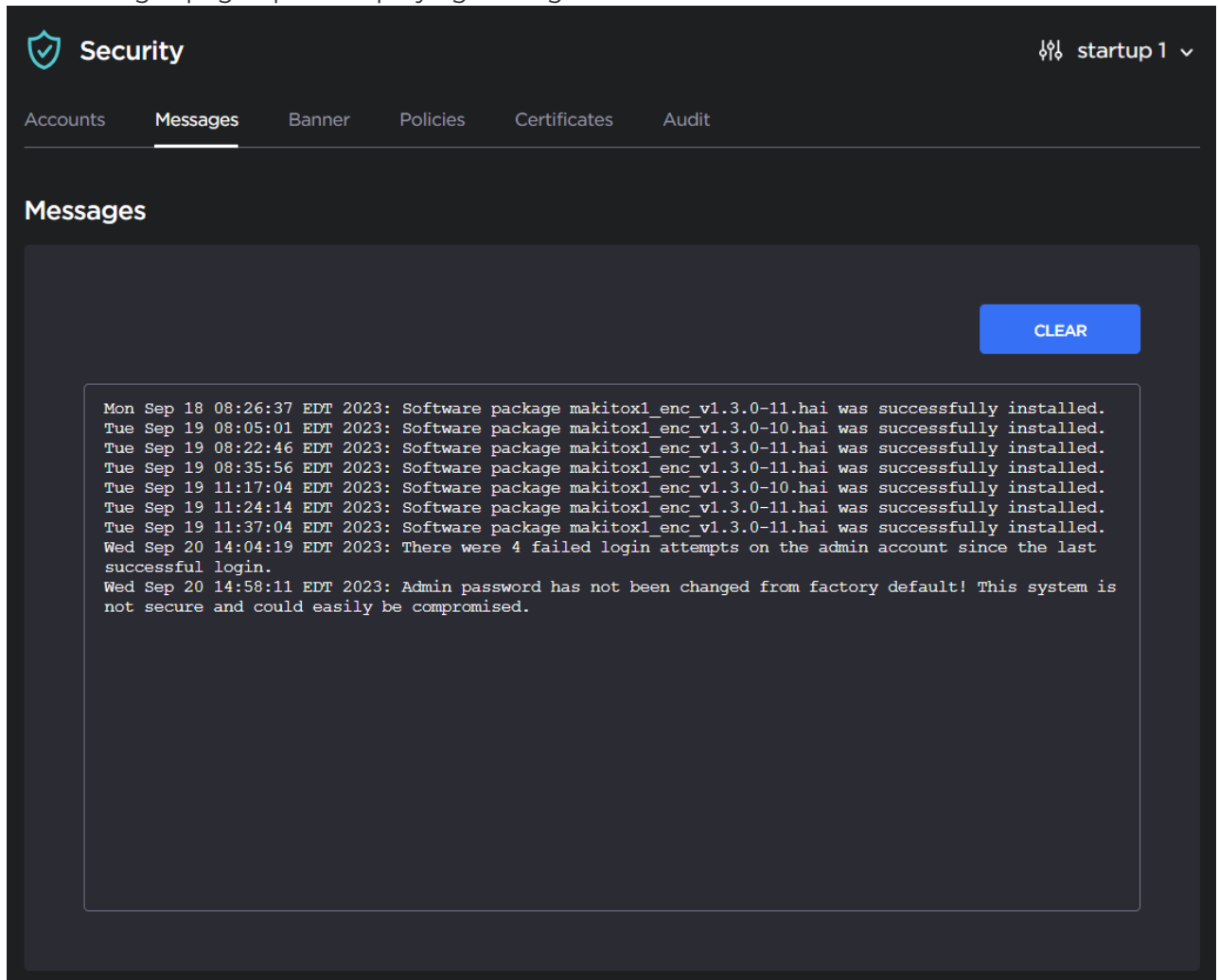
- The user initiating the action and the action being initiated.
- The time of the action.
- The results of the action (success/failure).

**Note**

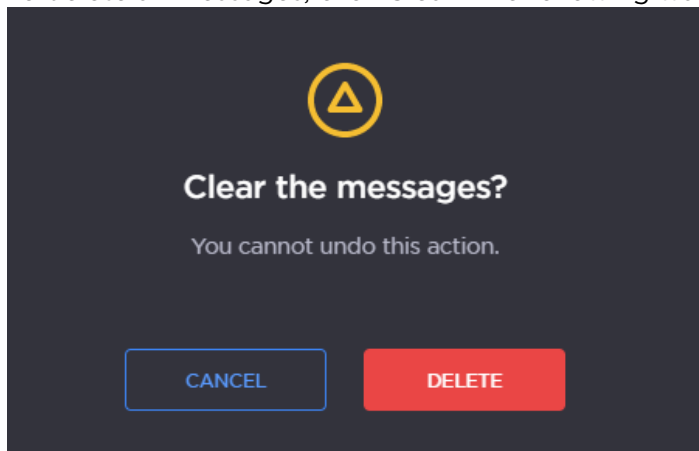
Messages starting with "POST" are Power-On Self Test events. If you repeatedly get POST errors, the cryptographic module of the encoder or decoder may be compromised, and it is recommended to re-install the firmware.

To view the messages:

1. Click **Security** on the sidebar, and select the **Messages** tab.
The Messages page opens displaying the log.



2. To delete all messages, click **Clear**. The following warning panel appears:



3. To cancel this action, click **Cancel**. To delete the messages, click **Delete**.

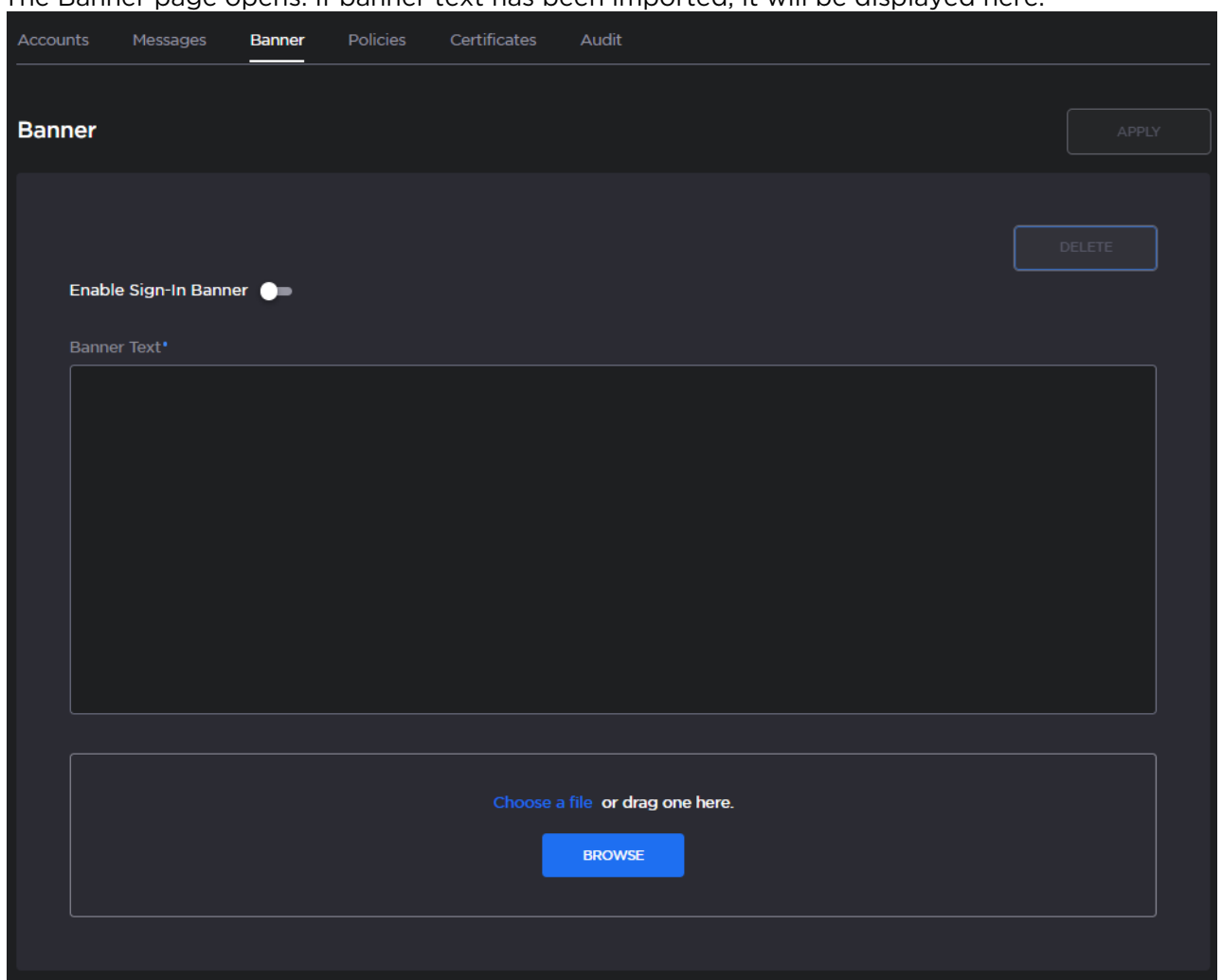
Managing Banners

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.

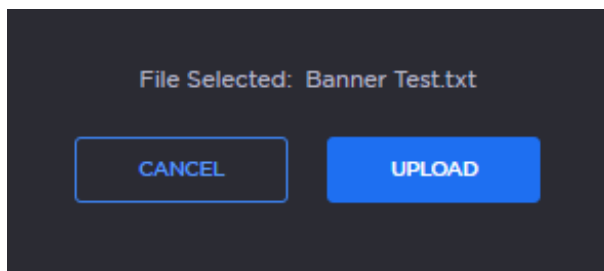
To upload a text file for the Banner page:

1. Click **Security** on the sidebar, and select the **Banner** tab.
The Banner page opens. If banner text has been imported, it will be displayed here.



The screenshot shows the 'Banner' configuration page within a dark-themed application. At the top, there is a navigation bar with tabs: 'Accounts', 'Messages', 'Banner' (selected), 'Policies', 'Certificates', and 'Audit'. Below the navigation bar, the page title 'Banner' is displayed on the left, and an 'APPLY' button is on the right. The main content area contains a toggle switch labeled 'Enable Sign-In Banner' which is currently turned off. Below this is a large text input field labeled 'Banner Text*'. At the bottom of the page, there is a file upload section with the text 'Choose a file or drag one here.' and a blue 'BROWSE' button.

2. Toggle **Enable Sign-In Banner** on to display the Advisory Notice and Consent Banner upon user sign-in.
3. Click **Browse** 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 **Cancel**.

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

**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.

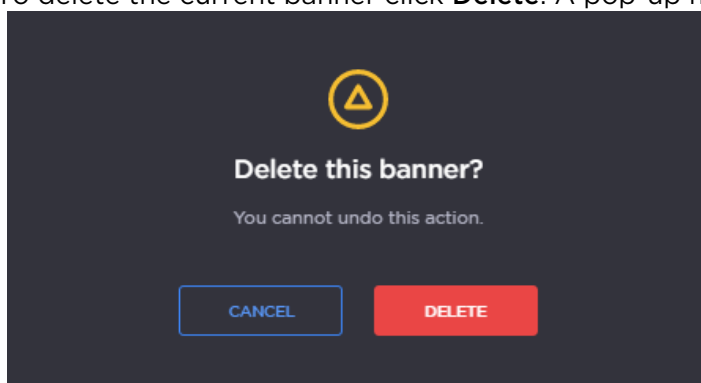
**Important**

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**. A pop-up message will appear:



If you are sure you wish to delete the banner message, click **Delete** again.

**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.

Related Topics

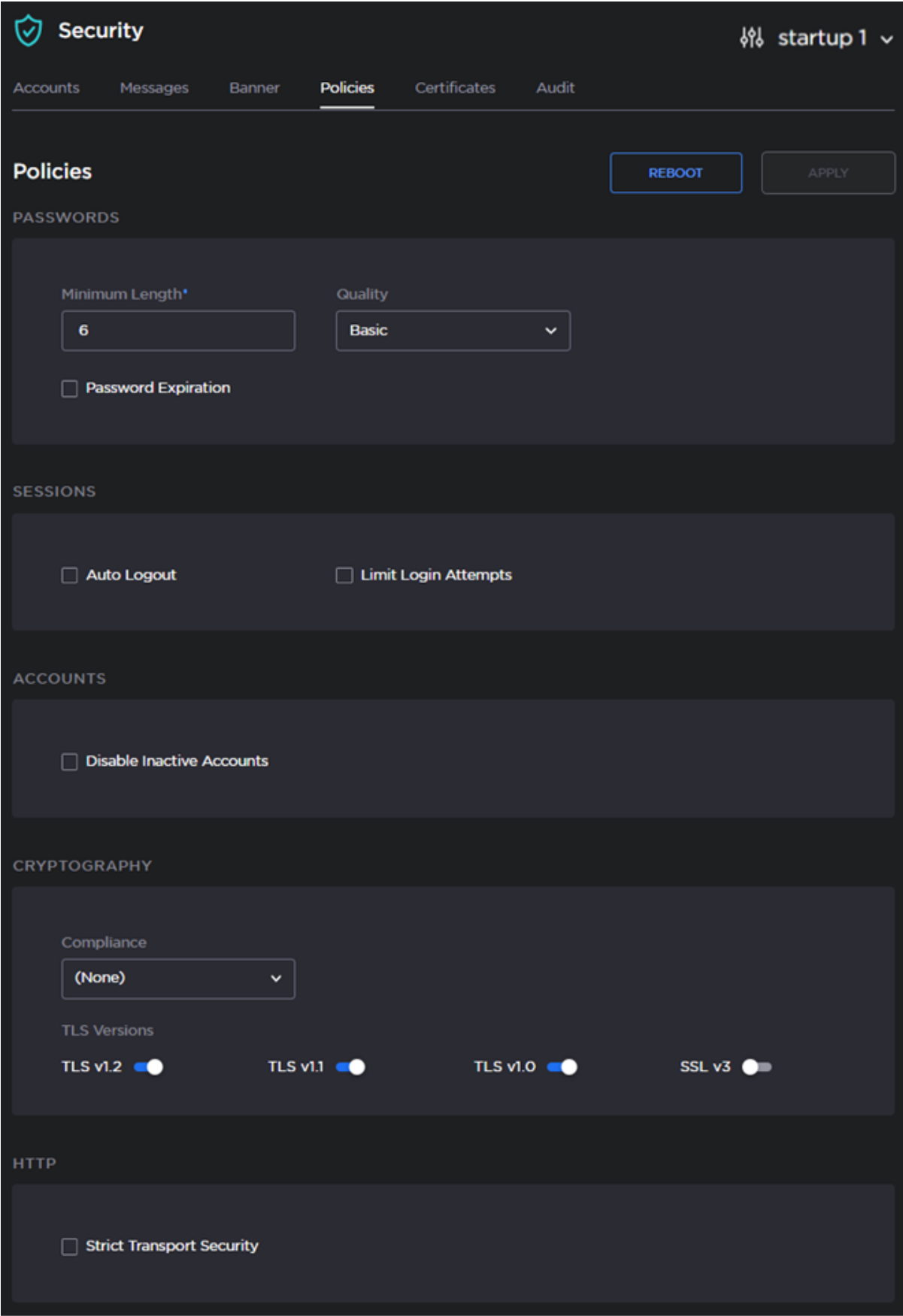
- [banner](#)

Managing Security Policies

From the Policies page, administrators can set policies for passwords, session timeout, cryptographic strength, and other security criteria for Makito X Series 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. Click **Security** on the sidebar, and select the **Policies** tab.
The Policies page opens.



- 2. Select or enter the new value(s) in the appropriate field(s).
- 3. To specify additional password quality criteria, select "Strong" from the **Quality** dropdown and adjust the values as required.

Policies

REBOOT

APPLY

PASSWORDS

Minimum Length*

6

Quality

Strong

☐ Password Expiration

Strong Requirements

Uppercase Letters*

0

Digits*

0

Symbols*

0

Remembered Last (Passwords)*

5

Minimum Lifetime (Days)*

0

- 4. Check the **Auto Logout** checkbox to log users out after a certain period of inactivity. Enter the desired time (in minutes) in the 'Logout when Idle for' field.
- 5. To improve login security, check the **Limit Login Attempts** checkbox and enter values for the desired Max Failed Attempts as well as the Failed Interval (Minutes) fields.

SESSIONS

☒ Auto Logout

Logout when Idle for (Minutes)*

15

☒ Limit Login Attempts

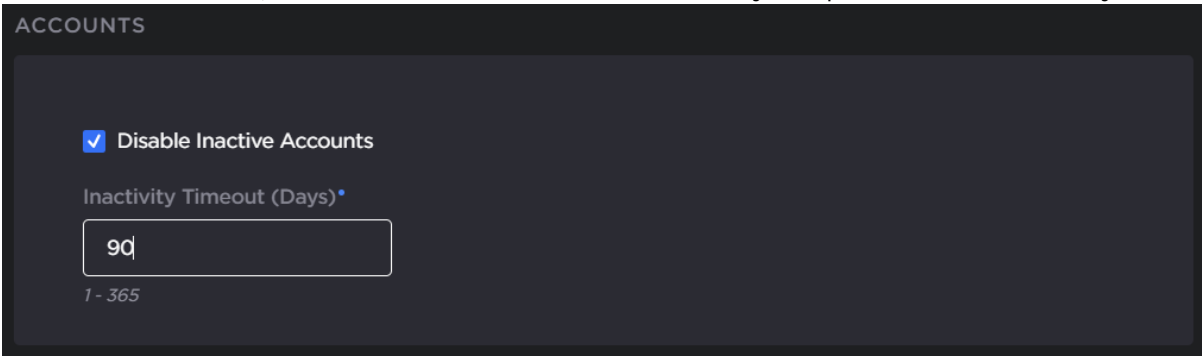
Max Failed Attempts*

3

Failed Interval (Minutes)*

15

6. To automatically disable accounts after a certain period of inactivity, check the **Disable Inactive Accounts** checkbox, and enter the number of inactive days required for an Inactivity Timeout.



7. To apply your changes, click **Apply**.
8. To ensure your changes are saved, reboot your Makito device by clicking **Reboot**.

Topics Discussed

- [Policy Settings](#)

Policy Settings

The following table lists the Policy settings for the Makito X1 Rugged encoder:

Password Policies

Policy Setting	Default	Description/Values
Minimum Length	6 characters	Type in the minimum password length (from 6-40 characters).  Note Passwords can be up to 80 characters.
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.

Policy Setting	Default	Description/Values
Strong Requirements	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 (Passwords)	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.
Minimum Lifetime (Days)	0	(Password quality must be Strong) This option restricts the user's ability to change their password. Enforcing a minimum password lifetime helps prevent repeated password changes to defeat the password reuse or history enforcement requirement. The range is from 0 (no restriction) to 7 days.
Password Expiration	Disabled	Check this checkbox to enable Password expiration.

Session Policies

Policy Setting	Default	Description/Values
Auto Logout	Disabled	Check this checkbox to automatically log users out after a specified period of idle time. When enabled, if a user has been inactive for longer than the specified period of time, he/she will be logged out and redirected to the Sign-in page. Systems that are left logged on may represent a security risk for an organization.  Note Enabling the Auto-Logout Session policy also limits the number of concurrent sign-ins per account to 4.
Logout when idle for	N/A if Disabled ----- 15 minutes if Enabled	(Auto Logout must be enabled) Specifies the maximum length of time the system may be idle before the user will be logged out. Range: 1 - 1440 minutes.
Limit Login Attempts	Disabled	Check this checkbox to lock a user account after the specified number of consecutive failed sign-in attempts during the specified time period. This may be used to reduce the risk of unauthorized system access via user password guessing.
Max Failed Attempts	N/A if Disabled ----- 3	(Limit Login Attempts must be enabled) Specifies the maximum number of consecutive failed sign-in attempts allowed during the specified time interval before the account will be locked. Range: 3..10

Policy Setting	Default	Description/Values
Failed Interval (Minutes)	N/A if Disabled ----- 15 minutes if Enabled	(Limit Login Attempts must be enabled) Specifies the time period during which the consecutive failed sign-in attempts will be counted to lock out the account. Range: 5..60 minutes  Note If a user fails the "Max Failed Attempts" within the "Failed interval", the account will be locked for 10 minutes.

Account Policies

Policy Setting	Default	Description/Values
Disable Inactive Accounts	Disabled	Check this checkbox to enable automatic disabling of user accounts after the specified number of days of account inactivity.
Inactivity Timeout (Days)	N/A if Disabled ----- 90 Days if Enabled	(Disable Inactive Accounts must be enabled) Specifies the number of days (since the last login) after which the user account will be disabled. Disabled accounts can be re-enabled either via the "account <uname> enable" CLI command or from the Web Interface Admin>Accounts List View where the Action drop-down list will include an option to re-enable a disabled account.  Tip The system adds one (1) day (or 24hour grace period) to the setting configured by the user.

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 (deprecated): Applies cryptographic modules accredited under the National Institute of Standards and Technology (NIST) Special Publication 800-52, Revision 1. - SP800-52 Revision 2: Supersedes SP800-52 Revision 1. Applies cryptographic modules accredited under the NIST Special Publication 800-52, Revision 2.  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.

Policy Setting	Default	Description/Values
TLS Versions	TLSv1.2, TLSv1.1, TLSv1.0	Specifies which TLS (Transport Layer Security) versions are accepted from the HTTPS client. • TLSv1.2 • TLSv1.1 • TLSv1.0 • SSLv3  Note SSLv3 can be enabled only if Compliance is set to None. At least one TLS version must be enabled.  Tip For backward compatibility considerations, you may choose to disable the older TLS versions not needed by the organization's TLS peers (i.e., browsers, <code>syslog</code> server) and plan the upgrade of those not supporting the latest TLS version with the objective of enabling only the latest TLS version.

HTTP Policies

Policy Setting	Default	Description/Values
Strict Transport Security	Disabled	Check this checkbox to enable HTTP Strict Transport Security (HSTS). HSTS forces web browsers to only contact the Web interface over HTTPS, instead of using HTTP.

Related Topics

- [Managing User Accounts](#)

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.

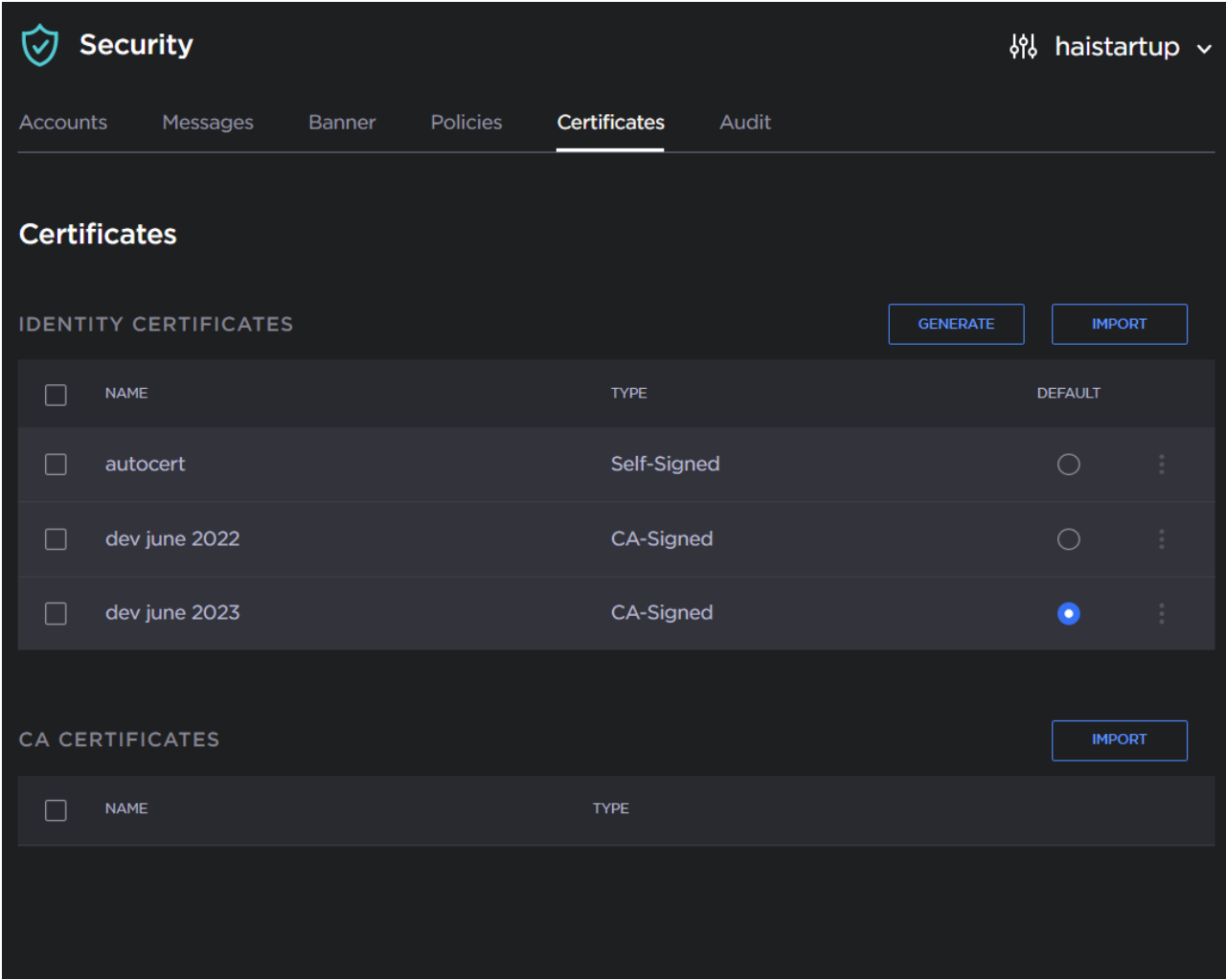
Topics Discussed

- [Generating a Certificate](#)
- [Importing a Certificate](#)
- [Viewing Certificate Details](#)
- [Certificate Settings](#)

Generating a Certificate

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

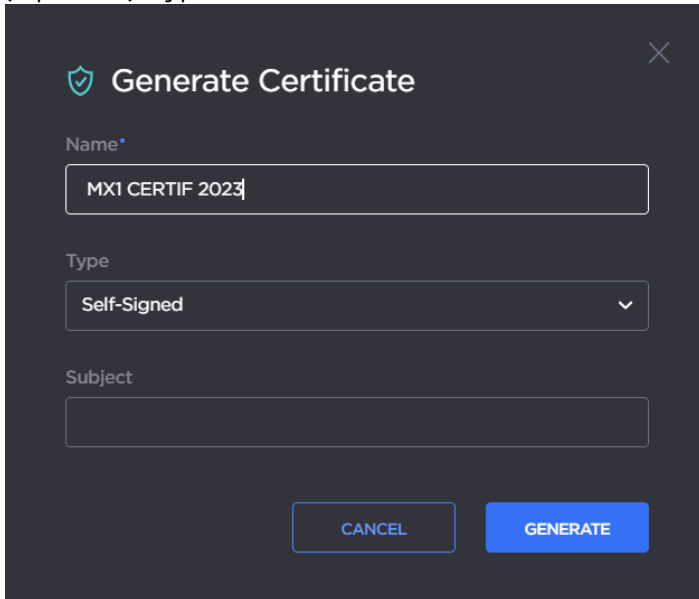
1. Click **Security** on the sidebar, and select the **Certificates** tab.
The Certificates page opens.



The default Identity Certificate is indicated with a blue radio button.

- 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".

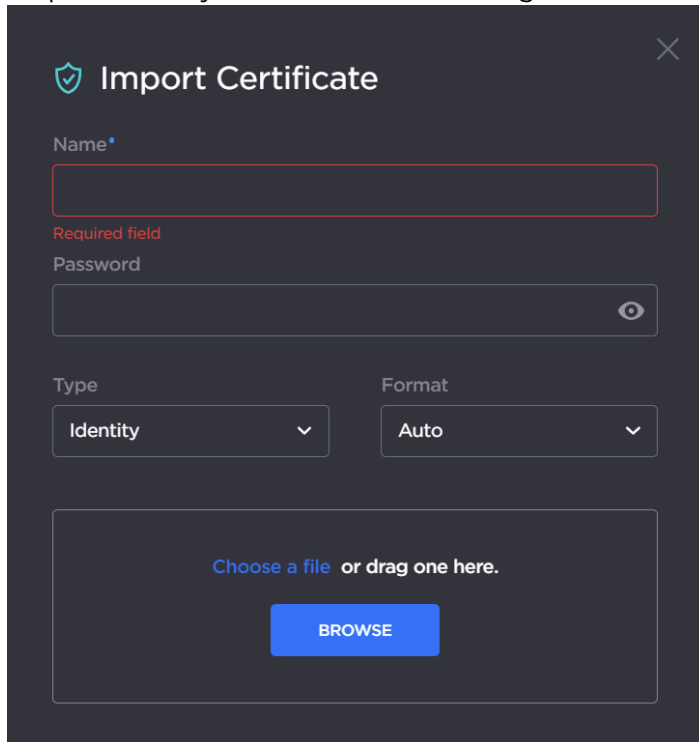
Related Topics:

- [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).

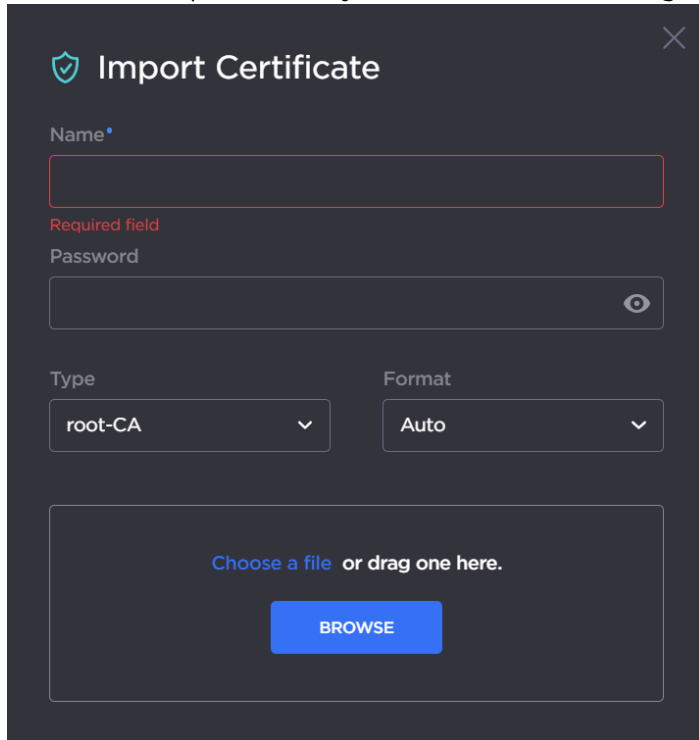
The image shows a dark-themed 'Import Certificate' dialog box. At the top left is a shield icon with a checkmark, followed by the title 'Import Certificate' and a close button (X) at the top right. Below the title is a 'Name' field with an asterisk, which is currently empty and has a red border. Underneath the name field is the text 'Required field' in red. Below that is a 'Password' field with a toggle icon (an eye) on the right. Under the password field are two dropdown menus: 'Type' with 'Identity' selected, and 'Format' with 'Auto' selected. At the bottom of the dialog is a large rectangular area with the text 'Choose a file or drag one here.' and a blue 'BROWSE' button centered below it.

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).



The image shows a dark-themed dialog box titled "Import Certificate" with a shield icon and a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name***: A text input field with a red border, indicating it is a required field. Below it, the text "Required field" is displayed in red.
- Password**: A text input field with a toggle icon (an eye) on the right side.
- Type**: A dropdown menu currently showing "root-CA" with a downward arrow.
- Format**: A dropdown menu currently showing "Auto" with a downward arrow.
- File Selection**: A large rectangular area containing the text "Choose a file or drag one here." and a blue button labeled "BROWSE".

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 vertical ellipsis menu of any listed certificate (Identity or CA Certificates) and click **View**.

The certificate file opens in a new window (as shown in the following example).

```
Certificate Fingerprints:
MD5: 84:DE:EC:DE:EC:93:48:8D:CE:5A:42:FC:90:83:E9:F5
SHA1: A9:B8:80:A7:22:0B:81:B0:BB:D3:84: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-----
MIIDPCCAISgAwIBAgIJAPpFnA0Smg8yMA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME2dwbTR1LmhhaXZpc21vbi5jb20wHhcNMjIwMTc0ODAxMjIwMTc0ODAxMjIw
-----END CERTIFICATE-----
```

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: <code>"/C=US/ST=Maine..."</code> 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:

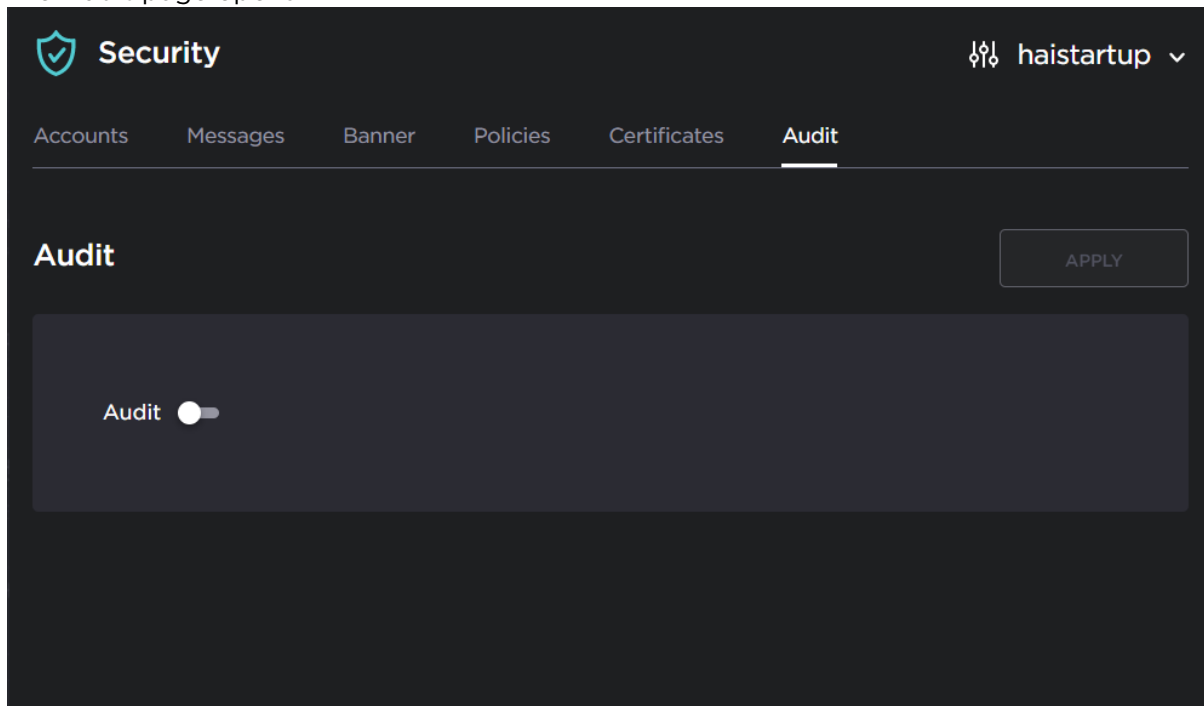
- [Configuring Network Settings](#)

Managing Audits

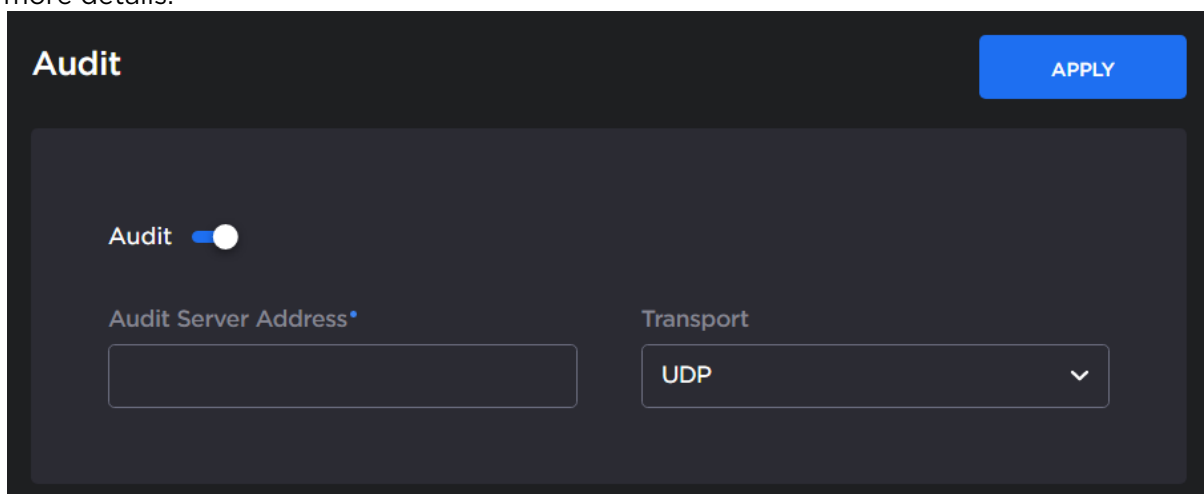
From the Audits page, administrators can set up logging to an Audit server for the Makito X.

To configure an Audit server:

1. Click **Security** on the sidebar, and select the **Audit** tab.
The Audit page opens.



2. Toggle **Audit** on to start logging to the audit server.
3. Type the audit server address and port in the Audit Server Address field. See [Audit Settings](#) for more details.



The server address must be the Common Name or one of the Subject Alternative Names in the

server’s certificate for successful authentication if Transport is set to TLS and Trusted Server is set to CA-Signed.

- 4. Set the type of transport protocol that will be used to send the logs to the audit server.
- 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".

Audit

APPLY

Audit ☒

Audit Server Address*

Transport

TLS

Trusted Servers

Self-Signed

Fingerprint*

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

Related Topics

- [Managing Certificates](#)
- [Audit Settings](#)

Audit Settings

The following table lists the Audit controls and settings:

Audit Setting	Default	Description/Values
Audit	disabled	Toggle Audit on or off to enable or disable audits for the system.

Audit Setting	Default	Description/Values
Audit Server Address	n/a	Type in the address and port of the remote server, in one of the following formats: <code>fqdn[:port]</code> <code>ipv4_addr[:port]</code> <code>ipv6_addr[:port]</code> <code>hostname[:port]</code> 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

This section provides information required to manage the Makito X1 through the Simple Network Management Protocol (SNMP). SNMP-based management uses Network Management Stations (NMSs) to collect data or configure devices (SNMP agents) across a TCP/IP network. The NMS communicates with the Makito X1 through the exchange of SNMP messages.

**Note**

This content is intended for users who are familiar with SNMP-based management and who will be developing applications such as provisioning services, or creating and modifying existing network management systems to manage the Makito X1.

**Tip**

To develop new SNMP applications, see the list of [Supported MIBs](#).

Topics Discussed

- [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 X1 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.

Supported MIBs	Standard	Description
HAI-MAKITO-X1-ENC-CAPS.txt	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X1 (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.



Note

You can download the MIBs directly from your Makito X1 under: `/usr/share/snmp/mibs/HAI-*.txt`

SNMP Agent Components

This section presents key components used to set up SNMP management on the Makito X1.

- `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/net-snmp/snmpd.conf` persistent data file, which maintains the USM user database and other SNMP agent persistent information. The script also performs `snmpget` commands to display the list of USM users, which is not available in a human readable form in any configuration file.

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

Following is an example of the `nmcfg` configuration script output:

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

model      perm/group      level      user/community      source
-----
usm        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} [{noauth|auth|priv}]
```

```
nmcfg access usm delete <uname>
nmcfg community help
nmcfg community permit <community> {<group>|ro|rw} [<host>]
nmcfg community delete <community> [{<group>|ro|rw} [<host>]]
nmcfg system help
nmcfg system define <param> "<value>"
nmcfg system delete <param>
nmcfg user help
nmcfg user define <uname> [{MD5|SHA} "<apwd>" [{DES|AES} ["<ppwd>"]]]
nmcfg user delete <uname>
```

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 passphrase 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 <i>all</i> 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.	snmpwalk
 Note The retrieval of a complete subtree is referred to as "walking the MIB."	

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
<code>haiAvtStreamNewID.0</code>	none	Next available stream ID
<code>haiAvtStreamInverseTable</code>	<code>IP address type</code> <code>IP address</code> <code>Port</code>	Table to retrieve the stream ID from the IP address and port
<code>haiAvtStreamTable</code>	<code>Stream ID</code>	Stream configuration and status
<code>haiAvtStreamStatsTable</code>	<code>Stream ID</code>	Stream statistics
<code>haiAvtStreamPgmTable</code>	<code>Stream ID</code> <code>Program Index</code>	Transport Stream programs. Only SPTS (Single Program Transport Stream) supported. Not present for non Transport Streams (directRTP, QuickTime).
<code>haiAvtStreamContentTable</code>	<code>Stream ID</code> <code>Program Index</code> <code>Content Index</code>	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` , `destroy`). See the description in the SNMPv2-TC.txt file of the MIBs directory. Stream writable objects can only be set at creation time (RowStatus is `createAndGo` or `createAndWait`) or while the stream is not active (RowStatus is `notInService` or `notReady`).

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

Examples

The following example, using `net-snmp` 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 of the Makito X1 Encoder via the CLI is possible through a telnet session, SSH, or RS-232. This alphabetical command reference lists and describes the available Command Line Interface (CLI) commands to configure and manage the 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](#)).

Topics and Commands Discussed

- [Syntax Conventions](#)
- [Command Summary and Access Control](#)
- [Operation Commands](#)
 - [adinsertion](#)
 - [audenc](#)
 - [leds](#)
 - [metadata](#)
 - [passthrough](#)
 - [rtsp](#)
 - [session](#)
 - [stream](#)
 - [temperature](#)
 - [videnc](#)
 - [vidin](#)
- [Administration Commands](#)
 - [account](#)
 - [audit](#)
 - [banner](#)
 - [certificate](#)

- `config`
- `date`
- `dtconfig`
- `emspair`
- `ethercfg`
- `haiversion`
- `ipconfig`
- `ipv6config`
- `license`
- `messages`
- `nmcfg`
- `package`
- `passwd`
- `policy`
- `pubkey`
- `reboot`
- `routes`
- `service`
- `system_snapshot.sh`
- `tzconfig`

Syntax Conventions

The following syntax conventions are used in this appendix:

Convention	Description
Monospaced font	Indicates command names and options, filenames and code samples.
<i>italic font</i>	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 X1 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 X1, or reboot, when the current configuration has not been saved in a preset. See [config](#).

Expand the sections below to view a list of CLI commands and other functionalities supported by the system, the privileges for each role, and their descriptions.

Operation Commands

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	Control the behavior of the Status LED (on the Makito X1 face-plate) at startup.
metadata	Yes	Yes	"get" only	Manage metadata sources to capture metadata (either KLV or CoT) and then incorporate data information within the MPEG Transport Stream.
passthrough	Yes	Yes	"get" only	On encoders with a serial port, enable bi-directional serial passthrough for controlling serially attached devices.
rtsp	Yes	Yes	"get" only	Manage rtsp settings.
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.

Command	Role			Description
	Admin	Operator	Guest	
General				
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

Administration Commands

Command	Role			Description
	Admin	Operator	Guest	
Network and Management				
config	Yes	Yes	"list" only	Manage configurations on the Makito X.
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 X.
ipconfig	Yes	—	—	View and set the parameters that specify the networking context for the Makito X, including the IP settings, hostname, and DNS.
ipv6config	Yes	—	—	View and set the parameters that specify the IPv6 network configuration.
license	Yes	—	—	Manage licensed features.
nmcfg	Yes	—	—	Used by system administrators or GUI/Web interface applications in the configuration of SNMP for the Makito X.
package	Yes	—	—	View and manage software packages, including firmware upgrades.
passwd	Yes	operator password only	user password only	Change the password for a user account.
reboot	Yes	—	—	Halt and restart the Makito X.
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.

Access

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

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 X1, see [Role-based Authorization](#).

Operation Commands

- [adinsertion](#)
- [audenc](#)
- [leds](#)
- [metadata](#)
 - [metadata Command Examples](#)
 - [CoT Retransmission](#)
 - [KLV Metadata Insertion](#)
 - [Metadata Decimation](#)
 - [UAS KLV Metadata Tag Filtering](#)
- [passthrough](#)
- [rtsp](#)
- [session](#)
- [stream](#)
- [temperature](#)
- [videnc](#)
- [vidin](#)

adinsertion

The adinsertion command is used to manage the ad insertion source.

**Note**

Ad insertion is a licensed feature. For more information on licensing, see [Managing Licenses](#).

Synopsis

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

Actions

Action	Description
start	Starts the adinsertion source.
stop	Stops the adinsertion source.
set	Configures adinsertion source settings. A series of one or more <code>parameter=value</code> pairs can be provided at once. See Parameters below.
get	Displays information on the adinsertion source. You can select to display the configuration (config), stats, or all.
clear	Clears the adinsertion source's statistics.
help	Displays usage information for the adinsertion command.

Parameters

Parameter	Default	Description/Values
name	n/a	A unique descriptive name of up to 63 characters. 'none' can be used to revert to the default name.

Parameter	Default	Description/Values
synchronization	auto	Options are: Auto - Auto-select the sync mode based on what SCTE-104 messages are being received. The priority of selected sync methods is as follows (in decreasing order): Alive, Time, System. Alive - Force the use of the received SCTE-104 alive_request_data() messages as the means to synchronize the time between the upstream SCTE-104 source and the Makito. Time Descriptor - Force the use of the received SCTE-104 insert_time_descriptor() messages as the means to synchronize the time between the upstream SCTE-104 source and the Makito. System - Use the local system time as the means to synchronize the time between the upstream SCTE-104 source and the Makito. NTP should be configured as the local time source.  Note These modes only apply when time deferred SCTE-104 requests are requested from upstream SCTE-104 sources.
leapseconds	37	Leap seconds added since Jan 1, 1958 to convert UTC to TAI.
timedescperiod	0 (disabled)	Period in seconds to force the insertion of time_descriptor. Range from 0 (disabled) to 60.
eventreminders	3	Number of event reminders to send to downstream equipment. Range from 1 to 5.
messagedelta	2000 (without parameters)	Interval in ms between event reminders. Range from 100 to 10,000ms (with parameters).

Examples

```
# adinsertion get all
```

Returns configuration information for the adinsertion [source](#):

```
AdInsertion ID      : 1
Name                : "HD-SDI-BNC-1"
Configuration:
  Type              : HD-SDI
  Input             : BNC-1
  Synchronization Type : AUTO
  Leap Seconds      : 37 seconds
  Time Descriptor Period : Disabled
  Event reminders    : 3
  SCTE35 Message Delta : 2000 ms
```

```
# adinsertion 1 set synchronization=alive
```

Sets the adinsertion source's synchronization mode to alive:

AdInsertion source configured successfully.

adinsertion 1 clear

Clears the adinsertion source statistics:
AdInsertion source stats cleared successfully.

Related Topics

- [Setting Up Streams](#)
- [Managing Licenses](#)

audenc



Tip

Starting release 1.2, you can specify a comma-separated list of IDs as well as a range of IDs for the operation, for example, `audenc c 3,2,0 start` or `audenc 3-0 stop`.

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 31.
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.

Action	Description
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 <code>parameter=value</code> pairs can be specified at once. See Parameters below.
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 <code>audenc all get table</code>.
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

Parameter	Default	Description/Values
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.
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.

Parameter	Default	Description/Values
bitrate	128 kbps	The Audio Bitrate for the encoder. 4..576  Note The available bitrate range depends on the current <code>mode</code> and <code>sample rate</code>. 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

<pre># audenc 0,2,3 start</pre> Starts audio encoders 0, 2 and 3. You will receive the following confirmation: 3 audio encoders started successfully.
<pre># audenc 0-3 stop</pre> Stops audio encoders 0, 1, 2 and 3. 4 audio encoders stopped successfully.
<pre># audenc 0,2,4-6 stop</pre> Stops audio encoders 0, 2, 4, 5 and 6 5 audio encoders stopped successfully.
<pre># audenc 0 set input=SDI1CH1+2</pre> Sets the Audio Input to SDI1CH1+2
<pre># audenc 0 set bitrate=128</pre> 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 set mode` command may be used to control the behavior of the Status LED at startup.

- If `normal` mode is used (default), wait two to five minutes for the Status LED to blink green. After blinking for approximately 15 seconds, the Status LED will become solid green, indicating that the unit is running and accessible. It will remain solid green while the system is fully operational.



Note

If the Status LED does not turn solid green after at least five minutes, you can attempt to connect to the network via:

- The Web User Interface, using the device's IP address, or,
- The CLI, through an SSH using the device's IP address.

If neither of these options work, perform a factory reset to re-configure the MX1 Rugged. For details, see [Resetting the MX1 Rugged](#).

- If `timeout` mode is used, the Status LED will blink for a short while when booting and will become solid green for a specified amount of time in seconds before going off.
- The `duration` of time for which the LED remains lighted up can range from 5 to 3600 seconds.
- When `mode` is set to `off`, the Status LED never lights up.

Synopsis

```
leds get
leds set mode=off,normal,timeout [duration=10]
```

Actions

Action	Description
set	Configures LED parameters. A series of one or more <code>parameter=value</code> pairs can be specified at once. See Parameters below.
get	Displays LED status information for the Makito X1.

Parameters

Parameter	Default	Description/Values
duration	n/a	The blinking duration can be set from 5 to 3600 seconds (60 minutes). If no duration is set, blinking will last for 10 minutes.

Examples

<pre># leds set mode=normal [duration=10]</pre> Sets the Status led to blink for 10 seconds while when booting and to become solid green and remain that way once the system is fully operational.
<pre># leds get</pre> Displays current LED status for the encoder (blinking initiated above): LED States: Status : Green Mode : Normal

Related Topics

- [Viewing System Status Information](#)

metadata

The `metadata` command is used to manage metadata sources. This command configures the Makito X1 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 X1 supports three metadata input types: either from the Serial port (**DC In & I/O**), 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 of one or more <code>parameter=value</code> 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 <code>parameter=value</code> 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 <code>metadata all get table</code>.
clear	Clears the metadata source's statistics.
<code>enable_metadata_on_serial_port</code>	(Makito X4/Makito X1 Rugged Encoders only) Enables metadata capture from the serial port.
<code>enable_console_on_serial_port</code>	(Makito X4/Makito X1 Rugged Encoders only) Enables console management from the serial port. (default)

Parameters

Parameter	Default	Description/Values
General parameters		

Parameter	Default	Description/Values
type	network	Specifies the type of metadata source to create, either <code>network</code> or <code>hdsdi</code> .  Note Additional HD-SDI sources can be created to stream KLV over SDI at different rates.
name	-	(optional) A name of up to 63 characters.
Network Source-specific parameters		
port	-	Specifies the UDP port for a network metadata source (i.e., the port on which to listen for KLV messages). Range: 1025–65,535
address	-	(optional) Specifies the IP address for a network metadata source. The address is only required to: - receive messages from a source that is multicasting. In this case, you need to provide the multicast IP address to which the data is being sent. OR - accept KLV messages coming from a specific sender.
HD-SDI Source-specific parameters		
input	bnc1	(optional, HD-SDI source only) Specifies the Input port for the metadata source: - bnc1 - bnc2 (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 <code>videncX</code> 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. <code>minimum</code>: Includes the list of uastags as specified in MISB 0902. <code>all</code>: Includes the list of uastags as specified in MISB 0601. <code>none</code>: filters <i>out</i> everything for the given set.

Parameter	Default	Description/Values
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. <code>minimum</code>: Includes the list of sectags as specified in MISB 0102. <code>all</code>: Includes the list of sectags as specified in MISB 0102. <code>none</code>: filters <i>out</i> everything for the given set.  Note <code>sectags</code> filtering requires <code>uastags tag #48</code> to be included as part of the list.
Static KLV Insertion parameters (See KLV Metadata Insertion)		
missionid	-	A string of up to 127 characters.
reclassify	off	(KLV input only) When set to on, enables reclassification of received UAS KLV messages.
classification	unclassified	Specifies the classification of the security data set: <code>unclassified</code>, <code>restricted</code>, <code>confidential</code>, <code>secret</code>, <code>topsecret</code>
classcountry	-	The ISO 3166-1 3-letter code for the classifying country.
objectcountry	-	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. <code>ipaddr1:port1[:ttl1[:tos1]],ipaddr2:port2[:ttl2[:tos2]]..</code>
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 = <code>1..255</code>

Parameter	Default	Description/Values
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
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>
```

Example:

```
# metadata create 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>
```

Example (showing multiple metadata streams):

```
# 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
```

Example:

```
# 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.

KLV Metadata Insertion

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

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

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

Example

To define a mission ID (up to 127 characters long):

```
# metadata 1 set missionid="XYZ"
```

To unconfigure the insertion/modification of the mission ID element:

```
# metadata 1 set missionid=none
```

To enable security modification/insertion:

```
# metadata 1 set reclassify=on classification=confidential objcountry=afg  
classcountry=usa
```

To disable the insertion and modification of the security data set:

```
# metadata 1 set reclassify=off
```

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.

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

Parameter	Default	Description/Values
baudrate	9600	Specifies the baud rate for the passthrough: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200
databits	8	Specifies the number of data bits in each character. 8, 7
stopbits	1	Specifies the number of stop bits sent at the end of every character. 1, 2
flowctrl	none	The flow control for the serial port: none, xonxoff 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](#)

rtsp

The `rtsp` command is used to manage rtsp settings.

Synopsis

```
rtsp start
rtsp stop
rtsp set parameter=value [parameter=value...]
rtsp get [config, stats, all]
```

Actions

Action	Description
start	Starts listening for rtsp clients.
stop	Stops rtsp, disconnecting clients.
set	Configures rtsp settings. See Parameters below.
get	Displays rtsp information. You can specify to display the configuration (config), stats, or all.

Parameters

Parameter	Default	Description/Values
port	554	TCP port on which to listen for rtsp clients.

Examples

```
# rtsp get all
```

Returns rtsp configuration information for the encoder:

Configuration:

```
TCP Port      : 554
Keepalive Idletime : 7,200 secs
Keepalive Interval : 1 secs
Keepalive Probes  : 5
```

Statistics:

```
State      : LISTENING
```

```
# rtsp set port=10554
```

Sets the rtsp port to 10554 and provides the following confirmation.

RTSP configured successfully.

Related Topics

- [Configuring RTSP](#)

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 <code>parameter=value</code> 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 <code>"stream get all"</code> 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.

Parameter	Default	Description/Values
author	n/a	(Optional) Enter the name of the program's author.
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 X1 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]] [adinsertionsrc=id/name]
[shaping=yes,no [ceiling=percentage] [idlecells=yes,no]
[delayaudio=yes,no]] [databitrate=auto,valueinkbps]
[atacarriage=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"] [authentication=none, auto, aes-gcm]
[latency=250] [overhead=percentage] [adaptive=yes,no]
[resource="resid"] [user="username"] [publishid="string"]
[redundancy=none, active-active, active-backup] [secaddr=ip addr] [secport=udpport]
[seccsourceport=udpport]
```

Parameters available for all ts-based streams:

```
[videopid=pid] [audiopid=pid[,pid,pid]] [datapid=pid] [adpid=pid]
[pcrpip=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 <code>parameter=value</code> pairs can be specified at once.
start	Starts the specified stream ID or name.  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	A unique number assigned to the stream.  Note When creating a stream, you can specify a unique id to assign to it or let the system assign one (a sequential number) for you. Most commands will accept the stream id or name (see below) in order 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 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 <code>id</code> is either <code>0</code>, <code>1</code>, <code>2</code>, <code>3</code>, <code>4</code>, <code>5</code>, <code>6</code>, or <code>7</code>. See Note and Tip above in the videosrc description.  Note To configure multi-track audio TS streams (TS over UDP or RTP), you can put more than one <code>audiosrc</code> (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. <code>id/name</code> (<code>0=serial</code>, <code>1=SDI</code>; all others are <code>UDP</code>)  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.: <code>stream create data=1,2</code>
adinsertionsrc	none	(Optional) The ad insertion source. <code>id/name(1)</code>
shaping	no	(Optional) To enable Traffic Shaping for the stream, specify <code>shaping=yes</code>. For some limited networks such as satellites or some dedicated network pipes, it may be necessary to enable Traffic Shaping to smooth the traffic and respect the absolute upper limit configured.  Note Using Traffic Shaping on streams above 7Mbps will create audio/video artifacts.
ceiling	n/a	(Optional, shaping must be <code>yes</code>) 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. <code>5..100%</code>, default = <code>15</code>
idlecells	no	(Optional, shaping must be <code>yes</code>) When enabled, Idle TS cells will be inserted into a TS stream when necessary. <code>yes,no</code>
delayaudio	no	(shaping and idlecells must be <code>yes</code>) 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. <code>yes,no</code>
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. <code>auto</code>: 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
adpid=pid	64	(Optional) Adinsertion (SCTE-35) Packet Identifier. 16-8190
prcpid	34	(Optional) (Program Clock Reference) Packet Identifier. Timestamp in the TS from which the decoder timing is derived. 16..8190
pmtpid	32	(Optional) (Program Map Table) Packet Identifier. 16-8190
program	1	(Optional) Program Identifier used in the Program Map Table (PMT) of the TS stream. 0-65535
tsid	0	(Optional) Transport Stream ID. Identifies the transport stream in the Program Association table (PAT) of the TS stream. 0-65535
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
sourceport	auto	(SRT connection mode must be caller) Specifies the UDP source port for the SRT stream.
encryption	none	Enables AES encryption and specifies the key length, either: none, AES-128, or AES-256
password	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

authentication	none	(Only available when encryption is enabled; encapsulation must be ts-srt) Configures Authenticated-Encryption with Associated-Data (AEAD). Options are: None - Default for Caller and Rendez-vous modes. Not available for Listener mode. Auto - Default for Listener mode. Not available for Caller or Rendez-vous modes. AES-GCM - Available for Caller, Listener, and Rendez-vous modes.  Note Setting the authentication to Auto allows the Listener to accept Callers with authentication set to either None or AES-GCM. Listeners with the authentication set to AES-GCM will only accept Callers which are also set to AES-GCM.
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). Range = 20 - 8000 ms  Note Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the 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.
publishid	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.
---------------	-----	---

Examples

<pre># stream create addr=192.0.2.106 port=2000 start=yes</pre> 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
<pre># stream create addr=192.0.2.235 port=1234 stillimage=haivision.mp4</pre> Creates and starts a streaming session. Specifies a static image to replace the "real" video stream when streaming is paused.
<pre># stream create addr=10.64.1.124 port=1234 encap=ts-udp videosrc=1 audiosrc=1 datasrc=1,3</pre> Creates and starts a multiple metadata streaming session.
<pre># stream create addr=10.64.1.124 port=1234 encap=ts-udp videosrc=1 audiosrc=0,2,4 audiopid=36,37,38</pre> Creates a TS stream with multi-track audio using audio encoders 0, 2 and 4. The corresponding audio PIDs are 36, 37 and 38.
<pre># stream 3 pause</pre> Pauses the stream created above (stream ID 3), which activates the still image.
<pre># stream 3 resume</pre> Resumes the stream created above.
<pre># 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</pre> Creates two streams, the first using Video and Audio encoder 0, and the 2nd using Video and Audio encoder 1.
<pre># stream create addr=192.0.2.235 port=1234 videosrc=4 audiosrc=0</pre> 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.

Related Topics

- [Configuring Streams](#)
- [Stream Settings](#)
- [Configuring Secure Reliable Transport \(SRT\)](#)
- [metadata](#)

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 or all. As of Makito X4 v1.5 and Makito X1 v1.2, 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: the Makito X4 offers eight encoding cores (encoder IDs 0 - 7), while the Makito X1 offers two encoding cores (encoder IDs 0 - 1).

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 <code>parameter=value</code> pairs can be specified at once. See Parameters below.
get	Displays encoder video status information. You can specify to display the configuration (config), stats, or all.  Tip To display a summary of all the encoders in a table format, you can use <code>videnc all get table</code>.
clear	Clears the encoder's statistics.
reset	Resets the encoder.
help	Displays usage information for the <code>videnc</code> command.

Parameters

Parameter	Default	Description/Values
algorithm	H265	The codec algorithm for the encoder: - H264 (AVC) - H265 (HEVC)

Parameter	Default	Description/Values
input	BNC1	The Video Input port for the encoder: - BNC1 - BNC2 (Makito X4 only) - BNC3 (Makito X4 only) - BNC4 (>Makito X4 only)
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 timecode 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 (under Network Settings).
countmode	SMPTE 12M-1	(TimeCode Source must be System) Selects the TimeCode Counting Mode: - SMPTE12M-1: Drops values 00 and 01 every minute, except every 10 mins (as per the SMPTE12M-1 standard). - UTC-Conversion: Derives the generated timecode (in HH:MM:SS:FF format) from UTC (Coordinated Universal Time). Dropped timecode values occur as needed to avoid drift and not at predetermined points in the timecode count sequence.
dailyresync	On	(timecode must be System with SMPTE12M-1 specified for countmode) Enables or disables timecode daily resyncs.  Note dailyresync and resynchour available starting release 1.3.1.
resynchour	0 (midnight)	(dailyresync must be enabled) Specifies the time for the resync to occur (ranging from 00:00 (midnight) to 23:00).
aspectratio	Auto	Specifies the aspect ratio of the video source and signals it into the MPEG stream: Auto : Aspect ratio is derived from the incoming video source resolution. 3:2 , 4:3 , 5:3 , 5:4 , 16:9 , 16:10 , 17:9 : Forces aspect ratio to specified value. WSS/AFD : Extracts aspect ratio from incoming video source based on WSS (Wide Screen Signaling) or AFD (Active Format Description) if detected.  Note WSS is only supported with analog PAL video; AFD is only supported with SDSDI video.

Parameter	Default	Description/Values
<code>dynamicrange</code>	Auto-Detect	(10-bit chromasubsampling must be selected) Select to configure the encoder to detect the inbound High Dynamic Range (HDR) transfer function signaling and forward that information within the encoded stream. • SDR: Off (SDR/BT.709) • Auto-Detect: the encoder detects HDR transfer function from the source • HLG: HDR content is based on the Hybrid Log Gamma (HLG, BT.2100) transfer function • PQ: HDR content is based on the Perceptual Quantizer (PQ, SMPTE ST 2084/BT.2100) transfer function
<code>bitrate</code>	6000 kbps	The Video Raw Elementary Stream bitrate (kbps). Range: <code>32-120000</code>
<code>resizemode</code>	Scale	(<code>resolution</code> 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" (under Video Encoder Settings).
<code>gopsize</code>	120	The Group of Pictures size for the encoded video. Range: <code>1-1000</code>  Note For intra-refresh mode, the GOP size is the number of frames between the sequence and picture parameter set NAL transmission.
<code>gopstructure</code>	IP	The GOP structure (i.e., video compression mode) for the encoded video: (See "Framing" under Video Encoder Settings) • <code>I</code> : I frames only (lowest delay; lowest quality) • <code>IP</code> : I and P frames only • <code>IBP</code> : I, B and P frames • <code>IBBP</code> : I, BB (two B frames in sequence) and P frames (highest delay; highest quality) • <code>IBBBP</code> : I, BBB (three B frames in sequence) and P frames • <code>IBBBBBP</code> : I,BBBBB (four B frames in sequence) and P frames (highest delay; highest quality)  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.

Parameter	Default	Description/Values
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	(<code>ratecontrolmode</code> 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" (under Video Encoder Settings).
picrate	Auto	The video frame rate per second: <code>Auto</code>: 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.
slices	1	Configures the encoder to use multiple slices per frame instead of the normal 1 slice per frame encoder configuration. Encoding latency is improved since encoded slices can be transmitted on the network without having to wait for the whole frame to be encoded. 1..11  Note Latency improvements are only seen on decoders that do not buffer entire video frames before decoding and can actually decode and output slices. Multiple slices cannot be used in conjunction with skipframes or gopstructure, i.e., Framing containing B-frames (IBP, IBBBBP).
closedcaption	Off	This parameter enables Closed Captioning on the encoder stream. <code>Off</code> , <code>On</code>
chromasubampling		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)
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: <code>0..120000</code> (<code>0</code> is Auto configure)  Note <code>maxbitrate</code> should be greater than or equal to <code>bitrate</code>.
ptsoffset	50 ms.	Offset video timestamps by this value in ms. Range: <code>-1000..1000</code>

Parameter	Default	Description/Values
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 0,2,3 start
```

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

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

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

```
# videnc 0 set gopsize=120
```

Sets the video GOP to 120.
Encoder configured successfully.

```
# videnc 4-7 set gopsize=60
```

Sets the GOP to 60 for video encoders 4, 5, 6, and 7.
4 video encoders 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
```

```
Aspect Ratio     : Auto-Detect
```

```
Dynamic Range    : SDR
```

```
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
```

```
Number Of Slices   : 1
```

```
Partial Frame Skip : Off
```

```
Chroma Subsampling : 4:2:0 8-bit
```

```
RateControl Mode   : CBR
```

```
Video MaxBitrate   : Auto
```

```
Intra Refresh      : Off
```

```
Video MaxPictureSizeRatio : 12.00
```

```
# videnc 0 get stats

Returns encoder statistics:
Encoder ID      : 0
Name           : "Video Encoder 0"
Statistics:
  State         : WORKING
  Up Time       : 24m44s
  Input Present  : Yes
  Input Type     : SDI
  Input Format   : 1920x1080p29
  Input Aspect Ratio : 16:9
  Input Color Primaries : BT.709
  Input Transfer Characteristics : BT.709
  Input Matrix Coefficients : BT.709
  Output Resolution : 1920x1080p
  Number Of Slices : 1
  Video SubFrame Latency : Off
  Encoded Frames  : 44,477
  Encoded Bytes   : 1,111,971,625
  Encoded Frame Rate : 29.97
  Encoded Bitrate : 6,264 kbps
  Encoder PTS     : 0x00841c86d
  Encoder Load   : 13%
  Closed Captioning : Disabled
  H.265 Profile   : Main
  H.265 Tier      : Main
  H.265 Level     : 4.1
  Entropy Coding  : CABAC
```

Related Topics

- [Configuring Video Encoders](#)
- [Video Encoder Settings](#)
- [Configuring Network Settings](#)

vidin

The `vidin` command is used to view and manage video input parameters on the encoder. ID is used to select the video input, or all.

The number of inputs varies with the platform: The Makito X4 has four video inputs (0 for BNC-1, 1 for BNC-2, 2 for BNC-3, 3 for BNC-4), while the Makito X4 Single Channel and the Makito X1 have one video input (0 for BNC-1).

Synopsis

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

Actions

Action	Description
set	Configures video input parameters. A series of one or more <code>parameter=value</code> 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 <code>vidin</code> 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.

Examples

<pre># vidin get all Input ID : 0 Name : "BNC-1" State : ACTIVE Input Type : SDI FIR Filter : Off Input Format : 720x480i29 (NTSC) Lock Status Changes : 1 Last Status Change : 2h16m2s ago</pre> Returns information for the video input.
<pre># vidin 0 set filter=Off</pre> Sets the filter to Off.

Related Topics

- [Configuring Video Encoders](#)
- [Video Encoder Settings](#)

Administration Commands

- [account](#)
- [audit](#)
- [banner](#)
- [certificate](#)
- [config](#)
- [date](#)
- [dtconfig](#)
- [emspair](#)
- [ethercfg](#)
- [haiversion](#)
- [ipconfig](#)
- [ipv6config](#)
- [license](#)
- [messages](#)
- [nmcfg](#)
- [package](#)
- [passwd](#)
- [policy](#)
- [pubkey](#)
- [reboot](#)
- [routes](#)
- [service](#)
- [system_snapshot.sh](#)
- [tzconfig](#)

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 enable
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.

Action	Description
lock	Locks the user account (if Enabled).
unlock	Unlocks the user account (if Locked).
enable	Re-enables a previously disabled user account.
delete	Deletes the user account.

Parameters

Parameter	Default	Description/Values
role	Administrator	Use with the <code>account create</code> 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 Settings](#)
- [Managing Public Key Authentication](#)
- [Changing Your Password](#) (lists allowed characters under "Password Requirements")
- [Role-based Authorization](#)
- [pubkey](#) (CLI command)

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 <code>parameter=value</code> 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: <code>fqdn[:port]</code> <code>ipv4_addr[:port]</code> <code>[ipv6_addr][:port]</code>  Note When configuring an IPv6 server, the address must be enclosed in square brackets. <code>hostname[:port]</code>
transport	UDP	The transport protocol, either: <code>UDP</code> (User Datagram Protocol): Default UDP port = <code>514</code> <code>TLS</code> (Transport Layer Security): Default TLS port = <code>6514</code>
trusted	All	If transport is TLS, the type of server authentication: <code>All</code>: No server authentication <code>CA-signed</code>: Root-CA certificate imported <code>Self-signed</code>: Fingerprint
fingerprint	n/a	If trusted is self-signed, specify the audit server certificate fingerprint (<code>md5</code> or <code>sha1</code>): <code>md5-fingerprint:</code> <code>sha1-fingerprint:</code>

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 <code>sign</code> and <code>subject</code> can be specified. See Parameters below.
delete	Deletes the selected certificate. The <code>type</code> can be specified. See Parameters below. Note The <code>type</code> 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 <code>infile</code> , i.e., the file to import the certificate from, must be provided. The file's <code>type</code> and <code>format</code> 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: <code>self</code> : Creates a self-signed identity certificate. <code>Request</code> : Creates an identity Certificate Signing Request (CSR)
subject	query	Sets the certificate's distinguished name parameters: <code>auto</code> : Automatically gets the subject Common Name which is <code>HOSTNAME.DOMAIN</code> if DNS is configured, or <code>IPADDR</code> otherwise. The subject Alt Name is set to <code>DNS:HOSTNAME.DOMAIN, DNS:HOSTNAME, IPAddress:IPADDR</code> <code>query</code> : Prompts the user for Distinguished Name (DN) attributes <code>DN</code> : Distinguished Name in the form: <code>" /C=US/ST=Maine..."</code> 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. <code>id</code> : Identity certificate (for HTTPS service and audit (<code>syslog</code> client)) <code>chain</code> : Identity certificate CA chain (Import only) <code>ca</code> : Certificate Authority Certificate (for peer certificate validation, Import only)
fmt	auto	The format in which the certificate is encrypted: <code>auto</code> : Detects the certificate format based on file extension when importing. <code>pem</code> : Privacy Enhanced Mail Base64 encoded DER certificate <code>p7</code> : PKCS#7 <code>p12</code> : PKCS#12 <code>pfx</code> : PKCS#12 <code>der</code> : Distinguish Encoding Rules

Parameter	Default	Description/Values
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. The `config` command also includes a Preset `autosave` setting.



Note

This is equivalent to saving and loading Presets in the Web interface.

Synopsis

```
config save [cfgname startup=yes,no [overwrite=yes]]
config load [cfgname startup=yes,no]
config delete [cfgname, all]
config duplicate cfgname
config rename oldname newname [-f, --force]
config set [autosave=on,off]
config list
```

Actions

Action	Description
save	Saves the current configuration. Saves every parameter in the system, including encoder settings and stream destination and status (excluding the system IP address). All configuration files are stored in <code>/usr/share/haivision/config</code>. See <code>cfgname</code> parameter below for naming conventions. When saving a named configuration, using the overwrite option prevents a prompt for confirmation when a configuration with the same name already exists. Note Using <code>config save</code> with no other parameters will store the current settings to the last loaded and currently active configuration. If the system was started without a startup configuration and no configuration was ever loaded, a new startup configuration named <code>haistartup.cfg</code> will be created.
load	Loads a previously saved configuration identified by <code><cfgname></code>. Reassigns every parameter in the system, including encoder settings and stream destination and status (excluding the system IP address). Note Using <code>config load</code> with no other parameters will load the current startup configuration. The startup option on <code>config load</code> is only available when autosave is disabled, since loading a configuration with autosave enabled will always set that loaded configuration as the startup configuration.

Action	Description
duplicate	Duplicates a saved configuration identified by <code><cfgname></code> .
rename	Renames a saved configuration identified by <code><oldname></code> to <code><newname></code> . See <code>cfgname</code> parameter below for naming conventions.
delete	Deletes a previously saved configuration identified by <code><cfgname></code> . If no filename is specified, the system deletes the default startup configuration (<code>haistartupcfg.ini</code>).
set	Configures the <code>autosave</code> setting.
list	Configuration files are stored under <code>/usr/share/haivision/config</code> . You can use <code>config list</code> to display available config files
help	Displays usage information for the <code>config</code> command.

Parameters

Parameter	Default	Description/Values
<code>cfgname</code>	n/a	Name of the configuration to load or save.  Note The following special characters are <i>not</i> supported for use in the configuration name (<code>cfgname</code>) unless they are escaped using the backward slash (\) character before being used: • Single Quote ` • Ampersand & • Parentheses (or) • Semicolon ; • Apostrophe ' • Double Quote " • Left and Right Angle Brackets < or >
<code>overwrite</code>	no	When saving a named configuration, the <code>overwrite</code> option can be used to prevent a prompt for confirmation when a configuration with the same name already exists. <code>yes, no</code>
<code>startup</code>	no	Sets saved configuration as the startup configuration. <code>yes, no</code>

Parameter	Default	Description/Values
autosave	on	When enabled, <code>autosave</code> automatically saves any applied changes to the encoder and stream settings in the startup configuration. This feature is designed to help users who have not saved their configurations into Presets and want to prevent loss of configuration settings when signing out or rebooting, or when the power is disconnected on their units. A warning indication already appears in the Web Interface title bar on systems with unsaved configuration changes. Preset <code>autosave</code> is enabled by default on new units and after a factory reset, but disabled when upgrading from an older version of firmware that did not support this feature (in order to avoid confusing users accustomed to the old preset workflow). The current state is displayed at the end of the <code>config list</code> output.

Examples

<pre># config save Class430 startup=yes</pre> Saves the current configuration under the name "Class430" and sets it to be the startup configuration.
<pre># config load Class430</pre> Loads a previously saved configuration identified by the name "Class430" (located in the active (local) directory).
<pre># config set autosave=on</pre> Enables auto-save and returns the following confirmation message. Auto-save of configuration changes enabled successfully.
<pre># config list</pre> Returns the available configuration files, as well as the auto-save state. Config Files (in /usr/share/haivision/config/): <pre>4xSRT_MX4E.cfg 4xSRT_MX4E_2xHUB.cfg (startup) 4xUDP_MX4E.cfg Backup-20210706.cfg Default.cfg</pre> 5 config files are available. Auto-save of configuration changes is disabled.

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

Action/ Operation	Option/ Argument	Description
unpair	-f	Unpairs the Makito X Series device from the EMS server: Forces unpairing
status		Queries agent status

Examples

```
# emspair pair -c Clqn9+kFUncKDDEwLjY1LjExLjE4NxCzRVJkCkNmZTBIMD
A1ZGYyNzM3Mml4MmY0Njc1ODUzZGQ3MDhhZDk4MWE2NGJjNDEyODliNDNIMDaxYzJjNTJmMmZhODZhEi
A4N2YyM2ZkNiIkNGEYLWExNGYtNzNhZiOyMjliNmRiZA==
```

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 Encoder 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    : 1000000kbps
```

Synopsis

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

Options

Option		Description/Values
-a	--autoneg	Enables (on) or disables (off) autonegotiation.
-s	--speed	If autonegotiation is disabled, sets the speed: 10, 100, 1000. If autonegotiation is enabled, this is the advertised supported speed which will be available for the peer Ethernet switch to use.
-d	--duplex	If autonegotiation is disabled, sets the duplex mode: half, full. If autonegotiation is enabled, this will be the advertised duplex mode.
-c	--ceiling	Puts a "ceiling" (in kbps or Mbps) on the bandwidth available to the Ethernet port.
-w	--write	If yes, skips the save settings prompt.



Note

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

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

Parameter

N/A

Actions

N/A

Example

```
# ethercfg -s 100
```

Sets the line speed to 100 Mbps (which also modifies the advertised mode, see example below).

```
# ethercfg -s 100
```

```
Speed      : 100mbps
```

```
Duplex     : Full
```

```
Auto-Negotiation : On
```

```
Advertised Mode : 100mbps Full-Duplex
```

```
Link Detected  : Yes
```

```
Ceiling      : 100000kbps
```

```
Do you wish to save these settings ? (y,n): y
```

```
Settings saved successfully.
```

Related Topics

- [Configuring Network Settings](#)

haiversion

The `haiversion` command is used to display status information about 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       : "MakitoX1 SDI Rugged Encoder"
Part Number     : S-MX1E-R
Serial Number   : HAI-031935020010
MAC Address     : 5c:77:57:00:de:60
Firmware Version : 1.0.0-19
Firmware Date   : "Feb 11 2020"
Firmware Time   : "14:40:37"
Hardware Version : A
Hardware Compatibility : -001G
Boot Version    : "U-Boot 2018.01 (Sep 12 2019 - 16:33:51 -0400)"
```

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.

Action	Description
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.
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 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        : QA-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-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        : MX1-129-69
```

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 : QA-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-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 <code>/usr/share/haivision/licenses</code> .
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):
OnVIF-MX1R-HAI-031935020010.lic
fully_loaded_makito4x-HAI-031935020010.lic
max_version_2.0_makito4x-rugged-HAI-031935020010.lic
no_expiry_makito1x-rugged-HAI-031935020010.lic

license view HAI-031935020010.lic

Displays the contents of the specified license.

license verify HAI-031935020010.lic

Verifies the specified license:
Verifying license /usr/share/haivision/licenses/HAI-031935020010.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` script reads and edits the standard SNMP configuration files, and then restarts the SNMP agent (`snmpd`) to apply the new settings.

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

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

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.
```

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

- [Role-based Authorization](#)
- [Managing User Accounts](#)
- [account](#) (CLI command)
- [Changing Your Password](#)

policy

The `policy` command is used to configure and manage security policy settings for passwords, session timeout, cryptographic strength, and other security criteria for user accounts. These policies apply to all user accounts; therefore, it is recommended to set the policies before beginning to create accounts.

Security policies may be applied to bring the Makito X Series device to its Common Criteria (CC) evaluated configuration.



Note

The policy command can only be used by an administrator.

Synopsis

```
policy account set [disableinactive=no] [inactivitytimeout=90]
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] [limitpwdretries=no] [maxpwdretries=3]
[pwdfailinterval=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
account set	Configures the Makito X device to automatically disable user accounts after the specified number of days of account inactivity.
password set	Modifies the password policy parameters. A series of one or more <code>parameter=value</code> pairs can be specified at once. See "password" under Parameters below.
session set	Modifies the session policy parameters. A series of one or more <code>parameter=value</code> pairs can be specified at once. See "session" under Parameters below.
crypto set	Specifies the cryptographic policy. The <code>compliance</code> 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 X device.

Parameters

Parameter	Default	Description/Values
crypto		
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  Note Either selection reinforces security for all management functions of the device in terms of cryptography. This setting takes effect upon the next reboot.
sslsv3	See Note	Enables or disables SSLv3 as a supported TLS version: Yes, No  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		
hsts	No	Enables or disables HTTP Strict Transport Security (HSTS). When enabled, HSTS forces web browsers to only contact the Web interface over HTTPS, instead of using HTTP.  Note When preparing a Makito X Series device for hardening, you need to enable the HSTS policy.
account		
disableinactive	no	Enables or disables automatic disabling of user accounts after the specified number of days of account inactivity: Yes, No

Parameter	Default	Description/Values
inactivitytimeout	90	Specifies the number of days (since the last login) after which the user account will be disabled: 1..365 days Disabled accounts can be re-enabled either via the “ <code>account <uname> enable</code> ” CLI command or from the Web Interface Admin>Accounts List View where the Action drop-down list will include an option to re-enable a disabled account.  Tip The system adds one (1) day (or 24hour grace period) to the setting configured by the user.
password		
quality	Basic	Specifies the required password strength, either: • Basic • Strong
minlen	6	Specifies the minimum password length. Range: 6..40
minupper	See Note	(quality must be Strong) Specifies the minimum number of uppercase letters. Range: 0..40  Note Default is N/A if quality=Basic, 0 if quality=Strong.
mindigits	See Note	(quality must be Strong) Specifies the minimum number of digits. Range: 0..40  Note Default is N/A if quality=Basic, 0 if quality=Strong.
minsymbols	See Note	(quality must be Strong) Specifies the minimum number of symbols. Range: 0..40  Note Default is N/A if quality=Basic, 0 if quality=Strong.
expiry	No	Enables or disables password expiration: Yes, No
lifetime	90 days	(expiry must be Yes) Specifies the number of days after which users must change their passwords. Range: 1..180 days
minlifetime	0	(quality must be Strong) Specifies the minimum number of days before a password can be changed, i.e., the minimum lifetime of the password. Range: 0 (no restriction)..7 days
remember	5	(quality must be Strong) Saves the specified last number of passwords used for the Makito X device, and prevents users from changing their password to any password used within the specified history count. Range: 5..400
session		

Parameter	Default	Description/Values
autologout	No	Enables or disables Auto-Logout after the specified length of time: Yes, No  Note Enabling the Auto-Logout Session policy also limits the number of concurrent sign-ins per account to 4.
idletimeout	15 minutes	(autologout must be Yes) Specifies the maximum length of time the system must be idle before the user is logged out: Range: 1..1440 minutes
limitpwdretries	No	Enables or disables limiting the number of consecutive <i>failed</i> sign-in attempts by a user during the specified time period. This may be used to reduce the risk of unauthorized system access via user password guessing: Yes, No
maxpwdretries	3	(limitpwdretries must be Yes) Specifies the maximum number of consecutive <i>failed</i> sign-in attempts allowed during the specified time interval. Range: 3..10
pwdfailinterval	15	(limitpwdretries must be Yes) Specifies the time period during which the consecutive failed sign-in attempts will be counted to lock out the account. Range: 5..60 minutes

Examples

<pre># policy crypto set compliance=NDPP11</pre> Sets the required cryptographic compliance to Network Device Protection Profile v1.1.
<pre># policy password set quality=strong minlen=10 minuppers=1 minsymbols=1 expiry=yes lifetime=30</pre> 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 X device such as:

Crypto:

```
Compliance      : (None)
SSLv3           : No
TLSv1.0         : Yes
TLSv1.1         : Yes
TLSv1.2         : Yes
```

HTTPS:

```
HSTS            : No
```

Account:

```
DisableInactive : No
```

Password:

```
Quality         : Strong
MinLen          : 6
MinUppers       : 1
MinDigits       : 15
MinSymbols      : 3
Remember        : 5
Expiry          : No
```

Session:

```
Autologout      : Yes
IdleTimeout     : 15 minutes
LimitPwdRetries  : Yes
MaxPwdRetries    : 3
PwdFailInterval : 15 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 (<code>.pub</code> 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](#)
- [account](#) (CLI command)

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](#)

routes

The `routes` command is used to manage configured static routes. This enables you to store the user-configured routes so they are not lost when devices are rebooted.

✓

Tip

You can add or delete a static route using the linux `route` command. For more information, see [Configuring Static Routes with IP Commands](#).

Synopsis

```
routes [save | load | delete [ipv4 | ipv6 | all]]
```

Actions

Action	Description
save	This saves the currently active routing tables of the selected IP protocol so that they can be restored on the next system startup.
load	This restores and activates the saved routing table.
delete	This deletes the saved routing table.

Parameters

Parameter	Default	Description/Values
ipv4 ipv6 all	all	The IP protocol family on which the chosen action will be performed. When no IP protocol family is specified, the one(s) currently in use on the device are saved, load or deleted.

service



Important

If the serial COM port (**DC In & I/O**) is not configured for CLI Management, and all remote management interfaces (HTTP, telnet, SSH, and SNMP) are disabled, the only way to re-enable these services is by a Factory Reset. Once the serial port is configured for metadata or passthrough use, it is no longer usable for CLI management.

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](#)

- (1.3 2) Reset the Encoder

system_snapshot.sh

The `system_snapshot.sh` command is used to 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 Makito X Series devices. `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 Makito X 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 X1 Rugged Video Encoder.

Topics Discussed

- [Video Input Interfaces](#)
- [Video Encoding](#)
 - [Supported Video Encoding Input and Downscale Resolutions](#)
- [Audio Encoding](#)
- [Advanced Features](#)
- [ISR Metadata](#)
- [Network and Management Interfaces](#)
- [Dimensions, Weight, Power](#)
- [Regulatory/Compliance Specifications](#)

Video Input Interfaces

Makito X1 Video Interfaces		
Composite	RS-170 RS-170A CCIR	NTSC/PAL/PAL-M
SD-SDI	SMPTE-259M-C	270 Mbps interface
HD-SDI	SMPTE-292M	1,485 Gbps interface
	SMPTE-274M	1920 x 1080 video format
	SMPTE-296M	1280 x 720 video format
3G-SDI	SMPTE-424M (Level A only)	3 Gbps interface
	SMPTE-425M	1080p60 video format
Impedance		
SDI	75 Ohms	

Video Encoding

Makito X1 Video Encoding - H.264 AVC (MPEG-4 Part 10) /H.265 HEVC	
SD/HD/3G-SDI Input Resolutions	1920x1080p 60/59.94/50/30/29.97/25/24/23.98 Hz 1920x1080i 60/59.94/50 Hz 1280x720p 60/59.94/50/30/29.97/25 Hz 720x480/576i 60/59.94/50 Hz (interlaced shown in fields per second)  Note For supported video encoding resolutions, see Supported Video Encoding Input and Downscale Resolutions.
Video Encoding Highlights	• H.264/AVC (MPEG-4 part 10) • H.265/HEVC • Multiple Simultaneous Cores • Bitrates from 32Kbps to 15Mbps • Configurable Group of Picture (GOP) size • Configurable Frame Rate, Resolution

Supported Video Encoding Input and Downscale Resolutions

Encoded Output Resolutions		Input Resolutions and Frame Rates														
		1920x1080p							1920x1080i		1280x720p				720x480i	720x576i
Name	Resolution	60/59.94	50	30	29.97	25	24	23.98	30/29.97	25	60/59.94	50	30/29.97	25	30/29.97	25
HD 1080p	1920x1080p	1	1	2	2	2	2	2	1	1	1	1	1	1	1	1
HD 1080i	1920x1080i	-	-	-	-	-	-	-	2	2	-	-	-	-	1	1
3/4 HD 1080p	1440x1080p	1	1	1	1	1	1	1	1	1	-	-	-	-	-	-
3/4 HD 1080i	1440x1080i	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-
1/2 HD 1080p	960x1080p	1	1	1	1	1	1	1	1	1	-	-	-	-	-	-
1/2 HD 1080i	960x1080i	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-
HD 720	1280x720p	1	1	1	1	1	1	1	1	1	2	2	2	2	1	1
3/4 HD 720	960x720p	-	-	-	-	-	-	-	-	-	1	1	1	1	-	-
1/2 HD 720	640x720p	-	-	-	-	-	-	-	-	-	1	1	1	1	-	-
SD 480p	720x480p	1	-	1	1	-	1	1	1	-	1	-	1	-	1	-
SD 480i	720x480i	-	-	-	-	-	-	-	1	-	-	-	-	-	2	-
SD 576p	720x576p	-	1	-	-	1	1	-	-	1	-	1	-	1	-	2
SD 576i	720x576i	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-
4CIFp	704x576p	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
4CIFi	704x576i	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
3/4 D1 NTSCp	540x480p	1	-	1	1	-	1	1	1	-	1	-	1	-	1	-
3/4 D1 NTSCi	540x480i	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-
3/4 D1 PALp	540x576p	-	1	-	-	1	1	-	-	1	-	1	-	1	-	1
3/4 D1 PALi	540x576i	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1
70% VGA	448x336p	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Half-D1 NTSCp	352x480i/p	1	-	1	1	-	1	1	1	-	1	-	1	-	1	-
Half-D1 NTSCi	352x480i/i	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-
Half-D1 PALp	352x576i/p	-	1	-	-	1	1	-	-	1	-	1	-	1	-	1
Half-D1 PALi	352x576i/i	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1
CIFp	352x288i/p	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
CIFi	352x288i/i	-	-	-	-	-	-	-	1	1	-	-	-	-	1	1

Legend:

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



Note

Resolutions marked "-" are not supported.

Only video encoder 0 can scale or deinterlace video. Video encoder 1 can encode at the native resolution if the aggregate (total) encoding does not surpass 1080p60. For example:

- A 1080p60 SDI signal is ingested into MX1 on encoder 0 and then downscaled to 720p60.
- In this case, video encoder 1 can encode the 1080p60 resolution but must frame-decimate to 1080p30 to avoid oversubscribing the aggregate encoding capacity of the MX1.

Audio Encoding

Audio Encoding - MPEG AAC ¹	
Audio Channels	Up to 8 embedded audio channels in 4 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 17 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
Network Adaptive Encoding
Multi-bitrate (MBR) Streaming
HD/SD De-interlacing
Built-in Downscaling
CTA-608/SDI and CTA-708/SDI Closed Captioning as per SMPTE 334-1/2
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

Metadata Inputs	Metadata Outputs
• CoT to KLV conversion • KLV or CoT over serial (RS-232/422) • KLV or CoT over UDP • KLV over SDI (SMPTE 336) • SMPTE 336M compliant • MISB 0601.10 compliant • MISB 0604.2 compliant • SMPTE 12M Timecode • SMPTE 334-1/2 closed captioning • SCTE 104 insertion markers	• Asynchronous & synchronous modes (as per MISB 0604.2) • High precision timecode insertion (as per MISB 0604.2) • KLV Metadata Processing (SMPTE 336, MISB 0601, 0102 and 0605 support) • SCTE 35 insertion markers New - following datasheet - TBD

Metadata Inputs and Processing

- KLV over UDP, SDI (SMPTE 336M)
- MISB 0601, 0604 Compliant
- SMPTE 12M
- Asynchronous and Synchronous modes
- KLV Metadata Processing and Filtering
- High Precision Timestamps

Old Specs - TBD

Network and Management Interfaces

IP Network Interfaces

Standard	• Single Ethernet 10/100/1000 Base-T, auto-detect, Half/Full-duplex • Unicast streaming (IPv4/IPv6) • Multicast streaming (Internet Group Management Protocol v3 (IGMPv3) & IPv6) • Multiple unicast streaming • 10G SFP Port (future use)
AVC/H.264 Streaming Protocols	• MPEG Transport Stream • Secure Reliable Transport (SRT) • Real Time Streaming Protocol (RTSP) • TS over SRT, UDP or RTP
HEVC/H.265 Streaming Protocols	• MPEG Transport Stream • Secure Reliable Transport (SRT) • TS over SRT, UDP or RTP

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 v1, v2c, and v3 • ONVIF

Dimensions, Weight, Power

Appliance

Makito X1 Rugged Appliance	Appliance Dimensions	Appliance Weight	Power	Temperature*
#S-MX1E-R-SDI1	30.5mm H x 72.5 mm W x 94 mm D (1.20" H x 2.85" W x 3.55" D)	363 g (0.80 lbs)	6W at 5VDC at 70°C 5W at 5VDC at 40°C	Operating: -40° to 70°C (-40° to 158°F) Non-operating: -45° to 85°C (-49° to 185°F) Humidity: 0-100% condensing *Ambient environmental temperature
#S-MX1E-R-V2-SDI1	32.8 mm H x 72.5 mm W x 94 mm D (1.29" H x 2.85" W x 3.55" D)	254 g (0.56 lbs)	6W at 5VDC at 70°C 5W at 5VDC at 40°C	Operating: -40° to 70°C (-40° to 158°F) Non-operating: -45° to 85°C (-49° to 185°F) Humidity: 0-100% condensing *Ambient environmental temperature
#S-MX1E-R-V2-28V-SDI1-ISR	32.5 mm H x 72.5 mm W x 94 mm D (1.29" H x 2.85" W x 3.55" D)	308 g (0.68 lbs)	8.43W at 28VDC at 70°C 6.95W at 28VDC at 40°C	Operating: -40° to 70°C (-40° to 158°F) Non-operating: -45° to 85°C (-49° to 185°F) Humidity: 0-100% condensing *Ambient environmental temperature

OEM Board

Makito X1 Rugged Board (#B-MX1E-I-SDI1-ISR)	
Board Dimensions	58.0 mm H x 66.0 mm W (2.28" H x 2.60" W)
Board Weight	45g (0.11 lbs)
Power	6W at 5V DC at 70°C 5W at 5V DC at 40°C
Temperature*	Operating: -40° to 70°C (-25° to 160°F) Non-operating: -45° to 85°C (-49° to 185°F) Humidity: 0-100% condensing *Ambient environmental temperature

Regulatory/Compliance Specifications

- IP-67 Rated for Dust and Water Resistance
- RTCA-DO-160 - (Radio Technical Commission for Aeronautics) Environmental Conditions and Test Procedures for Airborne Equipment
- STANAG 4609 Compliant (NATO Digital Motion Imagery Standard)
- MISP 2019 Compliant (International Conference on Machine Intelligence and Signal Processing)
- MIL-STD-810G Compliant (Environmental Engineering Considerations and Laboratory Tests)

**Note**

This standard applies to #S-MX1E-R-V2-SDI1 and #S-MX1E-R-V2-28V-SDI1-ISR.

- MIL-STD-704 Compliant (Aircraft Electrical Power Characteristics)

**Note**

This standard applies to #S-MX1E-R-V2-28V-SDI1-ISR.

Accessing the REST API

The Makito X1 Application Programming Interface (API) is a modern Representational State Transfer (REST) API stack that provides all functionality from the Makito X1 Web Interface and is harmonized with other Haivision appliances.

To access the API endpoint documentation, simply type in the IP hostname of your Makito X1 Encoder into your browser's address bar, followed by `/apidoc`.

The API Documentation page opens, as shown in the following example:

Filter... X

Audio Encoder

GET - get all audio encoder /apis/audenc

GET - get audio encoder /apis/audenc/:id

GET - get audio encoder /apis/audenc/:id/stats

POST - start audio encoder /apis/audenc/:id/start

PUT - set audio encoder /apis/audenc/:id

PUT - start audio encoder /apis/audenc/:id/start

PUT - start audio encoder /apis/audenc/:id/stop

Audit

GET - get audit server configuration /apis/audit

PUT - configure audit server /apis/audit

Authentication

GET - user session /apis/authentication

POST - login /apis/authentication

Banner

DELETE - remove banner /apis/identity

GET - get banner settings /apis/banner

POST - upload new ASCII banner /apis/identity

PUT - upload new ASCII banner /apis/identity

Certificates

DELETE - delete ca certificate /apis/ca/:id

Makito X1 Encoder

1.1.2

REST API doc

Audio Encoder

Audio Encoder - GET - get all audio encoder /apis/audenc

1.0.0

GET

```
/apis/audenc
```

Success 200

Field	Type	Description
stats	Object	Statistics
info	Object	Configurations
data	Object[]	Array of objects
name	String	Name of encoder
state	Number	Audio encoder state. Found in the "stats" object. 0 == stopped 3 == working 67 == muted 128 == failed
id	Number	ID of encoder
interface	Number	Input interface 1 == SDI 1 (1-2) 2 == SDI 1 (3-4) 3 == SDI 1 (5-6) 4 == SDI 1 (7-8) 5 == SDI 1 (9-10) 6 == SDI 1 (11-12) 7 == SDI 1 (13-14)

Getting Help

General Support	North America (Toll-Free) 1 (877) 224-5445 EMEA +33 2 56 56 50 18 International 1 (514) 334-5445
Managed Services	U.S. and International 1 (877) 224-5445
Support Portal	https://support.haivision.com
Product Information	info@haivision.com

