



HAIVISION

Makito X4 Decoder
User's Guide v1.3.2

HVS-ID-UG-MX4D-132

Edition Notice

© 2015-2023 Haivision. All rights reserved.

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

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

Edition Notice	2
About Haivision	2
Trademarks	2
Disclaimer	2
Contents	3
About This Document	6
Conventions	6
Typographic Conventions and Elements	6
Action Alerts	6
Obtaining Documentation	7
Getting Service Support	7
Introduction	9
New Product Features	9
Version History	10
Product Overview	12
Chassis Styles	13
Secure Reliable Transport (SRT)	16
IPv4 and IPv6 Support	17
Physical Description	18
System Interfaces	18
Audio/Video Interfaces	18
LED Status Indicators	19
Getting Started with the Web Interface	22
Accessing the Decoder	23
Security Steps	23
Default Decoder IP Address	24
Role-based Authorization	25
Signing In to the Web Interface	26
Exploring the Web Interface	27
Donut Charts	28
Changing Your Password	30
Password Requirements	31
Signing Out	31
Managing the Decoder	32
Configuring Decoder Outputs	33
Decoder Settings	37
Decoder Statistics	41
Oversubscription of Decoder Channels	50
Configuring Streams	52
Stream Settings	54
Stream Statistics	58
System Administration	63
Viewing System Status Information	64
Status Settings	65
Rebooting the Decoder	66
Taking a System Snapshot	66
Saving and Loading Presets	68

Installing Firmware Upgrades.....	71
Configuring Network Settings.....	74
Network Settings	77
Configuring Date and Time	81
Date and Time Settings.....	82
NTP Statistics	82
Enabling and Disabling Network Services.....	83
Services Settings.....	85
Pairing the Decoder with Haivision EMS.....	86
Managing Licenses.....	88
License File Errors.....	90
Managing Users and Security	91
Managing User Accounts.....	92
Account Management.....	94
Account Settings	96
Managing Public Key Authentication	98
Managing Audits	99
Audit Settings	101
Managing Banners.....	102
Managing Certificates	104
Generating a Certificate.....	104
Importing a Certificate	106
Viewing Certificate Details.....	108
Certificate Settings	109
Managing Messages.....	112
Managing Security Policies	113
Policy Settings	114
Using SNMP to Configure A/V Services	117
Audience	117
SNMP Overview	118
Supported MIBs.....	118
SNMP Agent Components	120
snmpd.....	120
snmpd.conf.....	120
snmpd.local.conf	120
nmcfg.....	121
SNMPv3	123
Examples.....	123
SNMP Utilities.....	124
SNMP Syntax for Setting Up Streams	125
Examples.....	126
Resetting the Decoder	127
Default Network Settings.....	128
CLI Command Reference	129
Accessing the CLI.....	129
Syntax Conventions.....	129
Command Summary and Access Control.....	130
Operation Commands.....	133
dec	134
leds	139
mkstill	141
still.....	143
stream	144
temperature	149
Administration Commands	150
account	151
audit.....	153
banner	155
certificate.....	157
config.....	160

date	162
emspair	163
ethercfg	166
haiversion.....	168
ipconfig.....	169
ipv6config.....	172
license.....	174
messages.....	176
nmcfg.....	178
package	183
passwd	185
policy	186
pubkey	191
reboot.....	192
service.....	193
system_snapshot.sh	195

Technical Specifications 196

Audio/Video Interface Specifications	197
Video Decoding.....	198
Additional Video Decoding Specifications.....	198
Audio Decoding	199
Advanced Features.....	199
Metadata (Optional).....	199
Network and Management Interfaces	200
Chassis Options.....	201
Single-Height Appliance	201
MB6X - 6 Blade Chassis.....	201
MB21X (#F-MB21X-R)	203
Power Connector Pinouts (Single-Height Chassis).....	204
Single-Height - Power Connector	204
Regulatory/Compliance.....	205

Accessing the REST API 206

Multi-channel Synchronization 208

Multi-Sync Overview	209
Step 1: Configure NTP Settings	210
Step 2: Configure Encoder Settings.....	212
Step 3: Configure Decoder Settings (Decoder Pass 1).....	213
Step 4: Observe and Measure Delay Ranges (Decoder Pass 2)	215
Makito X Decoder.....	215
Makito X4 Decoder	215
Step 5: Configure MultiSync Delay (Decoder Pass 3).....	218

Warranties 219

1-Year Limited Hardware Warranty	219
EXCLUSIONS AND LIMITATIONS	219
OBTAINING WARRANTY SERVICE.....	220
APPLICABLE LAW	220
EULA - End User License Agreement.....	221
READ BEFORE USING	221
SLA - Service Level Agreement.....	221
1. Introduction.....	221
2. Definitions	221
3. Service Levels for the Video Content Management System.....	221
4. Exceptions to Availability for the VCMS	222
5. Credits for Downtime for the VCMS.....	223
6. Support Services for the VCMS	223
7. Service Levels for Haivision Streaming Media Service	224
8. Credits for Outages of Haivision Streaming Media Service.....	224
9. No Secondary End User Support	224

Getting Help 225

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.

Obtaining Documentation

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

Getting Service Support

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

This user's guide describes how to install, configure, and manage the Makito X4 decoder to receive audio, video, and data over an Ethernet-based IP network, using either the Web interface, the Command Line Interface (CLI), or an SNMP server.

For information on installing and connecting to the Makito X4 decoder, please refer to the [Makito X4 Decoder Quick Start Guide](#).

Important

Before using the decoder, please familiarize yourself with the [Safety Guidelines](#) in the [Makito X4 Decoder Quick Start Guide](#) and [Waste Electrical and Electronic Equipment \(WEEE\) Disposal](#) notice in the [Preface](#) (available at <https://doc.haivision.com>).

Note

Unless otherwise specified, references to the "Makito X Series" can be taken to include the Makito X, Makito X4, and Makito MX1 family of encoders and decoders.

Introduction

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

New Product Features

Makito X4 Decoder Version 1.3.2 introduces the following features and enhancements to existing capabilities:

- **FIPS 140-2 Support** - Implementation of FIPS 140-2 security improvements.
- **Configurable Minimum Password Lifetime** - A new option is available to restrict 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. The default is 0.

See [Managing Security Policies](#) and [policy](#).

- **Added Trusted Root CA Bundle** - In order to properly support future interactions with Haivision Hub over HTTPS, the Makito X4 firmware now includes a list of trusted root certificate authorities (`ca-certificates.crt` installed under `/etc/ssl/certs/`). This list may be used to validate certificates returned by remote servers.

Version History

Makito X4 Decoder Version 1.3.1 introduced the following new features and enhancements to existing capabilities:

- **Security Improvements** – Corrective action to resolve identified security issues affecting certification. Including:
 - Disabling accounts after a specified period of account inactivity
 - Limiting the number of invalid sign-in attempts by a user during a specified time period
 - Limiting the number of concurrent sign-in sessions per user

See [Managing Security Policies](#) or [policy](#).

Makito X4 Decoder Version 1.3 introduced the following new features and enhancements to existing capabilities:

Slice-based Decoding

The Makito X4 Decoder now supports slice-based streams from the Makito X4 Encoder (i.e., streams that use multiple slices per frame instead of the normal one slice per frame). Encoding latency is improved since encoded slices can be transmitted on the network without having to wait for the whole frame to be encoded.

There are no user interface changes on the decoder, only on the encoder interface.

Detection for HDR Transfer Function Signaling as per SMPTE 352

The Makito X4 Decoder now supports High Dynamic Range (HDR) and Wide Color Gamut (WCG), including both Hybrid Log Gamma (HLG) and Perceptual Quantizer (PQ) HDR transfer functions. When licensed and configured for HDR, the decoder detects the inbound transfer function signaling within the stream (transmitted from a remote Makito X4 Encoder or any other compliant 3rd party encoder) and forwards this information within the SDI output signal.

HDR is a licensed feature. If the unit is not licensed for HDR, the colorspace is Standard Dynamic Range (SDR)/BT.709 in the output stream.

The EMS agent has been updated to support HDR options.

See "Dynamic Range" in [Decoder Settings](#) and [dec](#).

Admin Security Web Pages

The following Security pages have been added to the Administrative section of the Web Interface:

- Account Management (add new accounts)
- Audit
- Banner
- Certificates
- Messages
- Policies

See [Managing Users and Security](#).

Addition of Control Center Preview Thumbnails

Preview Thumbnails have been added to the Control Center Decoder configuration panels to provide a visual reference of each video decoder's output. Preview Thumbnails can be enabled/disabled and the Preview capture interval configured from the Web Interface Admin Services page.

Preview settings persist through reboot. By default, previews are enabled and set to 10 second intervals.

See [Enabling and Disabling Network Services](#).

Certificates Page Improvements

The following improvements have been made to the Certificates page:

- Removed type "root-CA" in Identity import modal
- Removed type "Identity" and "ca-chain" in CA import modal
- Added confirmation notification when changing default certificate
- Added more custom error messages on certificate upload failure

Support Decoding of System Timecodes generated as per SMPTE 12M

There are no user interface changes on the decoder, only on the encoder interface.

Decoder and Stream Statistics

New statistics are available on the Web Interface, including enhanced statistics supporting multi-channel synchronization between Makito X Series encoders and decoders.

See [Decoder Statistics](#), [Stream Statistics](#) and [Multi-channel Synchronization](#).

Makito X4 Decoder Version 1.2 introduced the following new features and enhancements to existing capabilities:

- The Licensing page (Admin Settings Web Interface) now includes the license feature list (as found on the Makito X4 Encoder).
- EMS Agent has been updated for configuration and telemetry.
- Buffering has been improved to account for Video Codec Unit (VCU) performance variability, including Skip/replay under certain conditions and audio problems possibly aggravated by the presence of skip/replay.

Makito X4 Decoder Version 1.1 introduced the following new features and enhancements:

- The Certificates page was added to the Admin Security Web Interface.
- Audio issues from release 1.0 were resolved.

Product Overview



The Makito X4 decoder is a low latency, quad channel SDI video decoder for live sports coverage, news broadcasts, corporate video, and mission-critical ISR (Intelligence, Surveillance, Reconnaissance) deployments. It is designed to be used with the Makito X4 encoder in Broadcast, Defense, and Enterprise markets.

Features include the following:

- **4K UHD / Quad HD Video Decoding** – The Makito X4 is a versatile real-time HEVC/H.265 and AVC/H.264 video decoder that can receive up to four 1080p50/60 HD streams or a single full 2160p50/60 4K UHD (Ultra High Definition) stream over IP, along with 32 channels of digital audio. The Makito X4 can decode video streams with either 8- or 10-bit pixel depth and 4:2:0 or 4:2:2 chroma subsampling. Decoded streams can be output as 12G-SDI video for 4K content or in HD with up to four 3G-SDI outputs.
- **Ultra Low Latency End-to-End** – The Makito X4 decoder decodes HEVC and H.264 video with extremely low latency and is ideally suited for live broadcast interviews and remote production.
- **Remote Production with Stream Sync** – The Makito X4 decoder supports Haivision’s Stream Sync technology which automatically synchronizes multiple streams based on timecodes embedded by Makito X4 encoders. Stream Sync supports remote production of live video over IP by enabling synchronized switching between multiple video and audio sources.
- **High Density Form Factor** – The Makito X4 decoder is available as a compact standalone appliance or as a blade for Haivision rack-mountable enclosures. With the same single-height form factor as the Makito X4 encoder, the Makito X4 decoder offers high channel density for up to 84 HD or 21 UHD video encoding or decoding sources within a single 4RU rack module.
- **Secure Reliable Transport** – The Makito X4 decoder can decode video streams secured with AES 128- or 256-bit encryption using the SRT protocol. In order to reliably deliver streams over unmanaged networks, SRT adapts to changing network conditions and recovers lost packets in real-time.

Chassis Styles

The Makito X4 decoder is available in the following chassis styles:

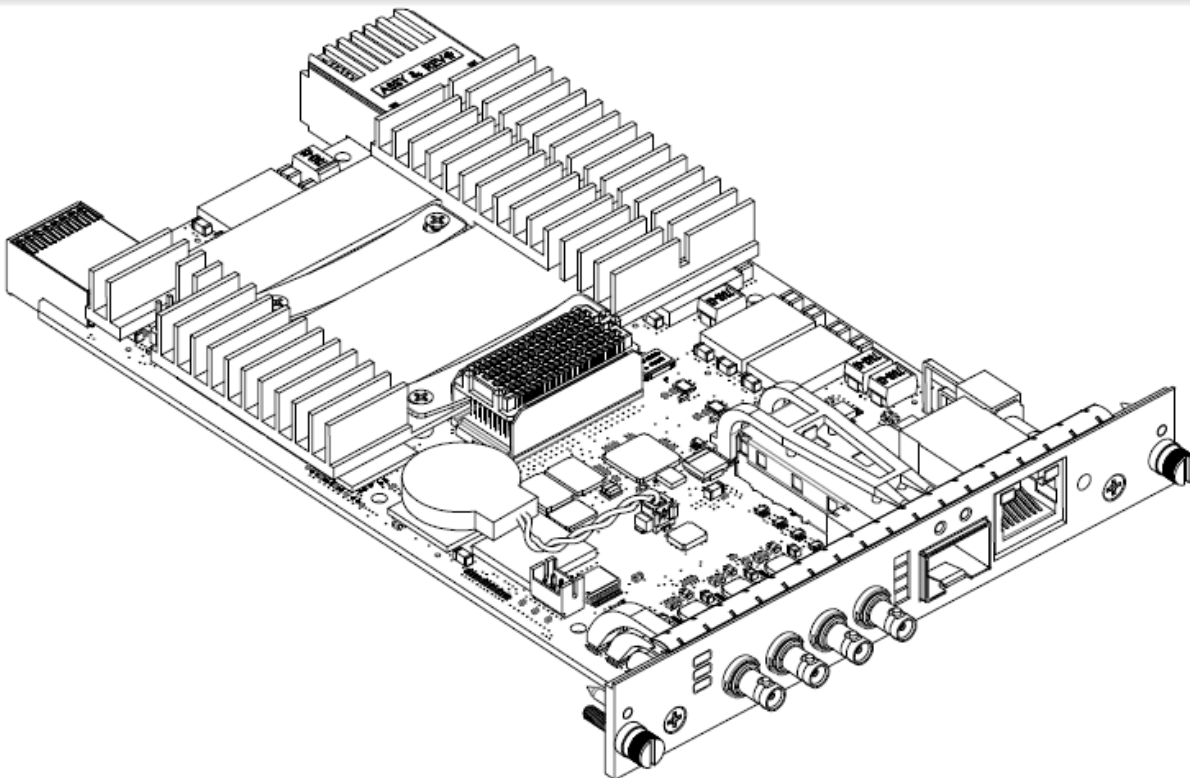
- as an ultra-compact appliance for single, dual or quad channel encoding.
- as a blade within a 1RU chassis (MB6X) that can contain up to six single-height or three dual-height Makito X Series or other Haivision encoder/decoder blades.
- as a blade within a 4RU chassis (MB21) that can contain up to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

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

Makito X4 Decoder (#S-MX4D-SDI4)



Makito X4 Decoder blade (#B-MX4D-SDI4)



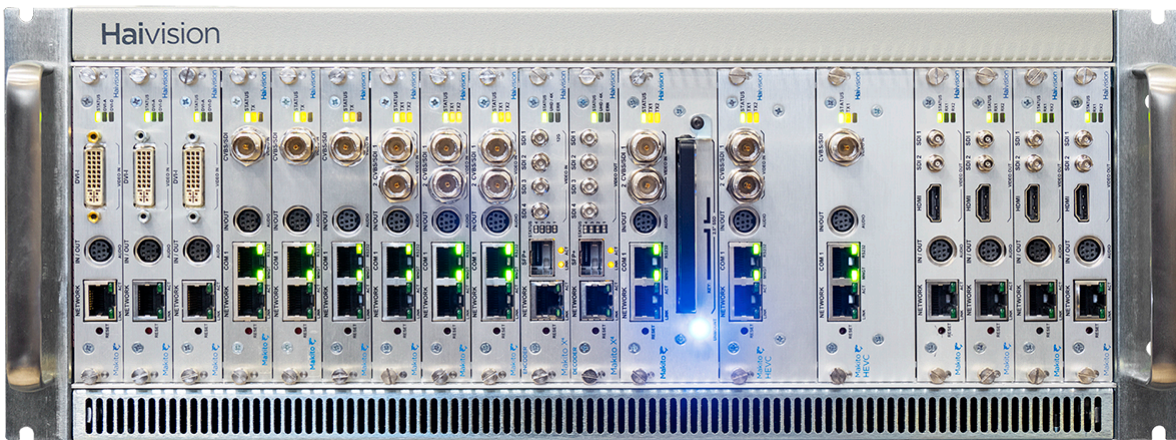
MB6X Multichannel Chassis (Front and Rear Views, #MB6X-RAC)



Note

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

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





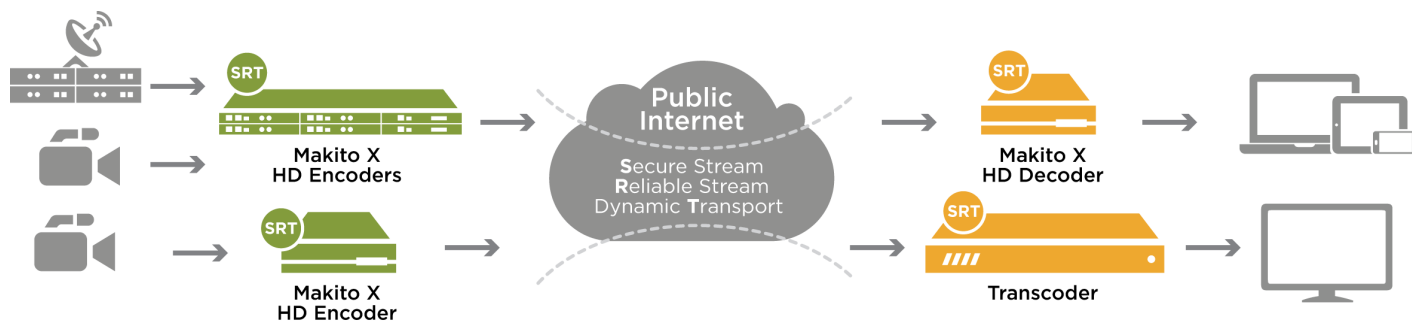
For information on the MB21 chassis, refer to the [MB21 Chassis Installation Guide](#).

Secure Reliable Transport (SRT)

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

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

Makito X SRT Workflow



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

IPv4 and IPv6 Support

The Makito X4 series and Makito FX devices support Internet Protocol Version 4 (IPv4-only) and Version 6 (IPv6-only) as well as dual-stack IPv4/IPv6 networks. You can install the Makito X4 or FX on an IPv4 network, an IPv6 network, or on a network supporting both IPv4 and IPv6. You will be able to access the Web Interface, CLI and SNMP via the IPv4 and/or IPv6 addresses assigned to the device.

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

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

Related Topics

- [Configuring Network Settings](#)
- [ipconfig](#) (CLI command)
- [ipv6config](#) (CLI command)

Physical Description

Following is a description of the Makito X4 decoder interfaces, connectors, and LED status indicators.

System Interfaces

The Makito X4 decoder comes equipped with the following interfaces:

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



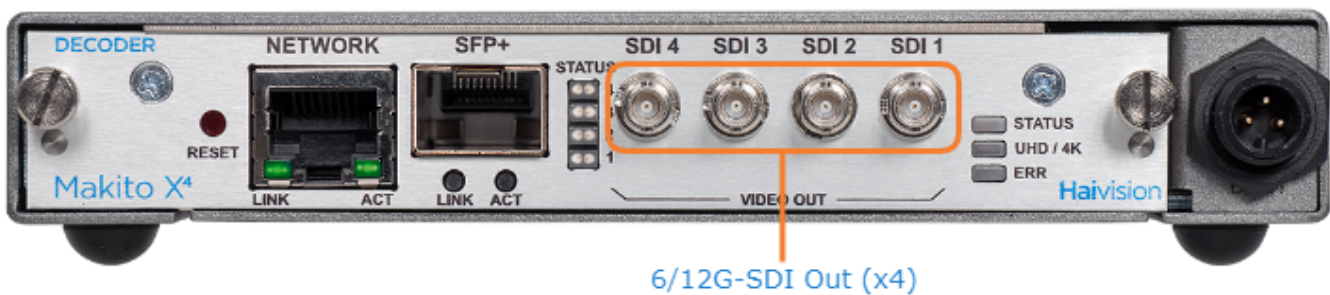
Related Topics:

- [Connect to the Network](#)

Audio/Video Interfaces

SDI Video and Embedded Digital Audio Interfaces

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



The HD-BNC connector(s) are used for SD-SDI (Serial Digital Interface), HD-SDI, 3G-SDI, 6G-SDI and 12G-SDI video output signals. All ports are 6/12G-SDI capable.

In addition, the HD-BNC connector(s) support auto-detection of the HD resolution and embedded digital audio.

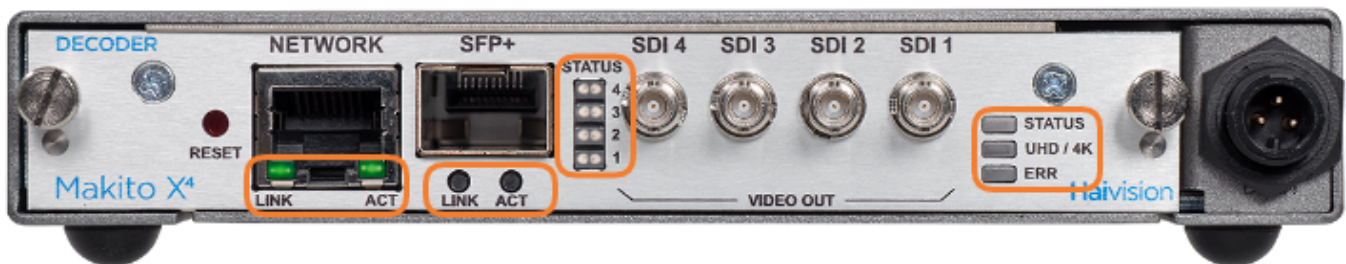
Related Topics:

- [Connect to A/V Displays](#)

LED Status Indicators

Front panel LED colors and flashing (blinking) speed indicate network traffic, Video Output status and output resolution modes of the decoder.

There are four SDI Status Output LEDs, one corresponding to each output. Each LED (1-4) reflects the state associated with the same HD-BNC output (SDI 1-4).



[Network Port](#) [SFP+ Port \(Future Use\)](#) [SDI Output Status](#) [General](#)

Network Port

Function	Description	Indication
LINK	Off	Not connected
	Green blinking once per second	Connected at 10 Mbps
	Green blinking twice per second	Connected at 100 Mbps
	Green blinking three times per second	Connected at 1000 Mbps
ACT	Off	No activity
	Green intermittent	Little activity (e.g., management). The LED should be lit when there is activity.
	Green solid	Intense activity (e.g., receiving video traffic)

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

SFP+ Port (Future Use)


Function	Description	Indication
LINK	Off	Not connected
	Green solid	Connected
ACT	Off	No activity
	Green intermittent	Little activity (e.g., management). The LED should be lit when there is activity.
	Green solid	Intense activity (e.g., receiving video traffic)

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

SDI Output Status

Function	Description	Indication
SDI1 / SDI2 / SDI3 / SDI4	Off	No data. Either the decoder is off, the stream is not flowing, or the stream does not contain any audio or video.
	Solid Amber	SDI is being driven by either audio or video, but not both.
	Solid Green	SDI is being driven by both audio and video.
	Blinking Amber	<div style="border: 1px solid #ffc107; padding: 5px;"> <p>Note</p> <p>The only error that currently triggers this is Oversubscription. For more information, see Oversubscription of Decoder Channels.</p> </div>

General

Function	Description	Indication
STATUS	Off	No power
	Green fast blinking	Reset button is pressed for less than four seconds. If the Reset button is not pressed, there is a power fault.
	Green slow blinking	Booting/Initialization
	Green solid	Booting/Initialization sequence is complete (No fault/Normal operation).
	Red fast blinking	Reset button is pressed for more than four seconds (Factory Reset enabled).
	Red slow blinking	Reset button is released after the Red fast blinking state (executing Factory Reset).
UHD/4K	Solid Green	<p>A valid 4K input stream is actively being processed.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note All SDI channels support 6G/12G (UHD/4K) video output.</p> </div>
ERR	Amber solid	The decoder has encountered an unrecoverable error.

Getting Started with the Web Interface

! Important

Before proceeding, make sure that the decoder is set up correctly and all necessary network and A/V connections are established. For information on installing and connecting to the Makito X4, please refer to the [Makito X4 Decoder Quick Start Guide](#).

All Makito X4 decoder interfaces and applications such as Audio/Video services and IP links may be configured, managed, and monitored through the Web Interface, the Command Line Interface (CLI), or an SNMP server. All methods require access to the decoder through its Ethernet LAN port.

Topics in This Chapter

- [Accessing the Decoder](#)
- [Signing In to the Web Interface](#)
- [Exploring the Web Interface](#)
- [Changing Your Password](#)
- [Signing Out](#)

Accessing the Decoder

Managing the Makito X4 decoder from the Web interface requires a connection from the unit's LAN port to your network. You must then connect a computer with a Web browser to the network to access the Web interface.

To access the Makito X4 decoder configuration Web page:

1.

Note

The Makito X4 decoder supports the latest production versions (as of this document date) of the Firefox, Safari, Chrome, and Edge browsers. Internet Explorer is not supported. 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 decoder's IP Address in the browser's address bar and press Enter.
3. Sign in. (See [Signing In to the Web Interface](#).)

Tip

For a list and description of the CLI commands to configure and manage the Makito X4 decoder, see [CLI Command Reference](#).
For information on SNMP management of the Makito X4 decoder, 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).

Note

The Makito X4 identity certificate and trusted root certificates are managed using the CLI `certificate` command. For details, see [certificate](#) (CLI).

Default Decoder 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 Decoder](#)

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.

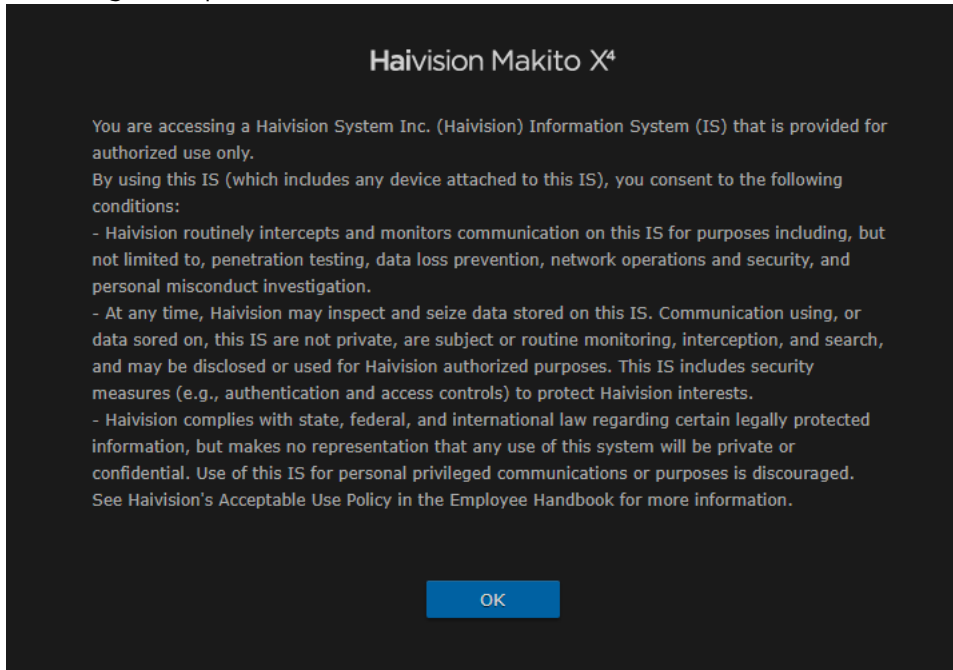
Related Topics

- [Command Summary and Access Control](#)

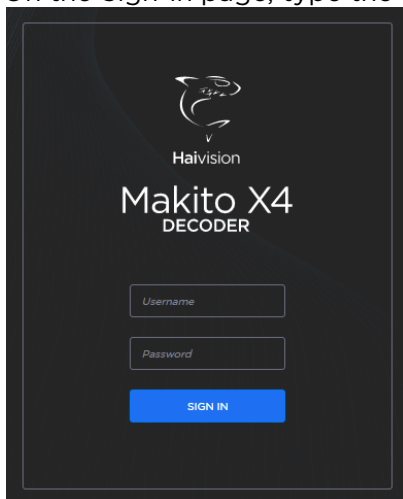
Signing In to the Web Interface

To sign in to the Makito X4 decoder Web interface:

1. From your Web browser, type the Makito X4's IP Address into the address field and press Enter. (Optional) On some systems, you will see an Advisory and Consent Banner, as shown in the following example.



2. Review the Advisory and Consent terms as required for your system and click **OK**.
3. On the Sign-in page, type the Username and Password and click **Sign In** (or press Enter).



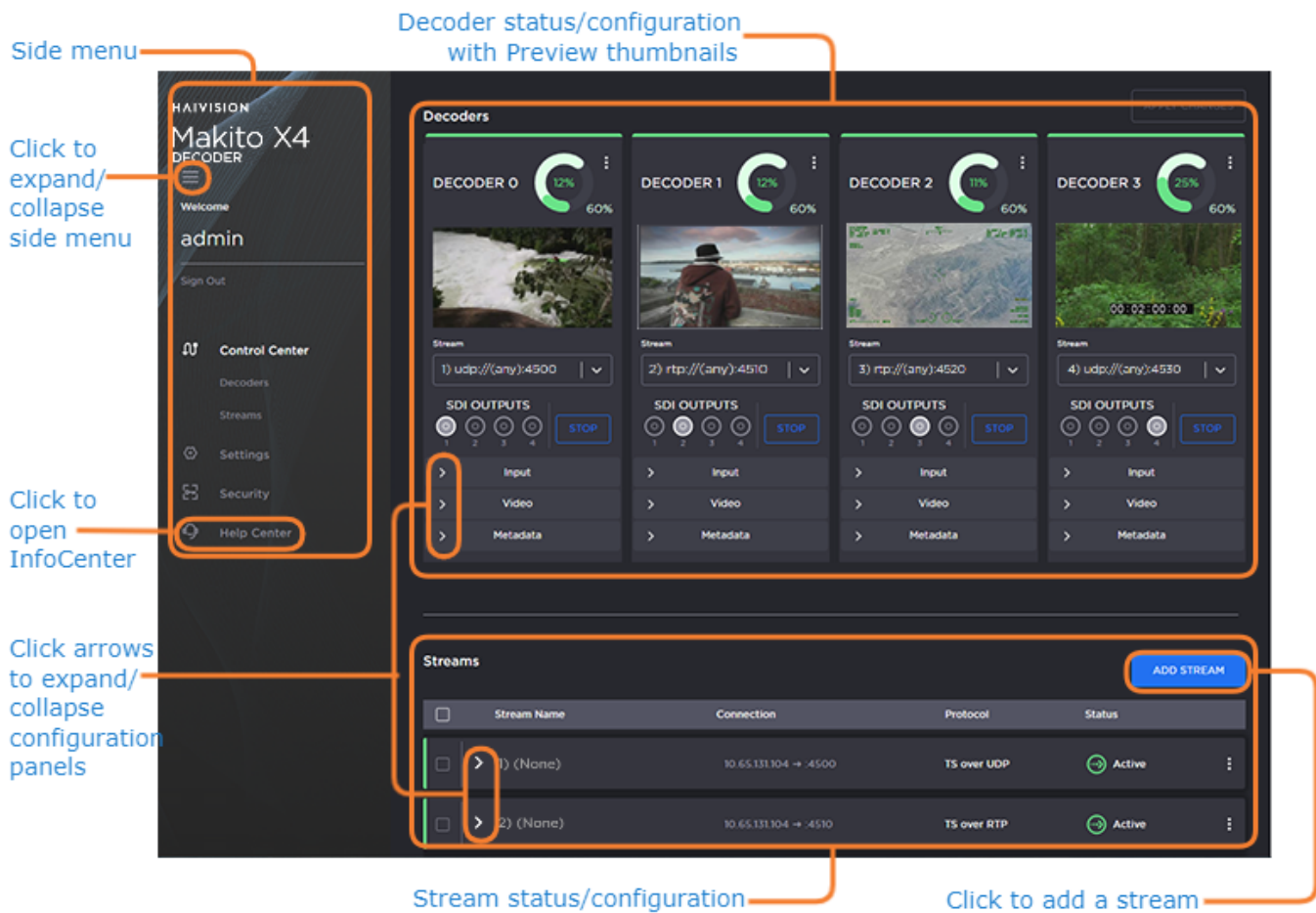
Please refer to the *Important Notice* (postcard shipped with the appliance or available from the [Download Center](#) on the Haivision Support Portal) for the default sign-in credentials.

Makito X4 provides three pre-defined user accounts. For information, see [Role-based Authorization](#).

Exploring the Web Interface

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

The Web interface opens to the Control Center, as shown in the following example. Your account information is displayed in the side menu. You can create streams and configure the decoders all on one page. Preview Thumbnails in the Decoder configuration panels provide a visual reference of each video decoder's output.

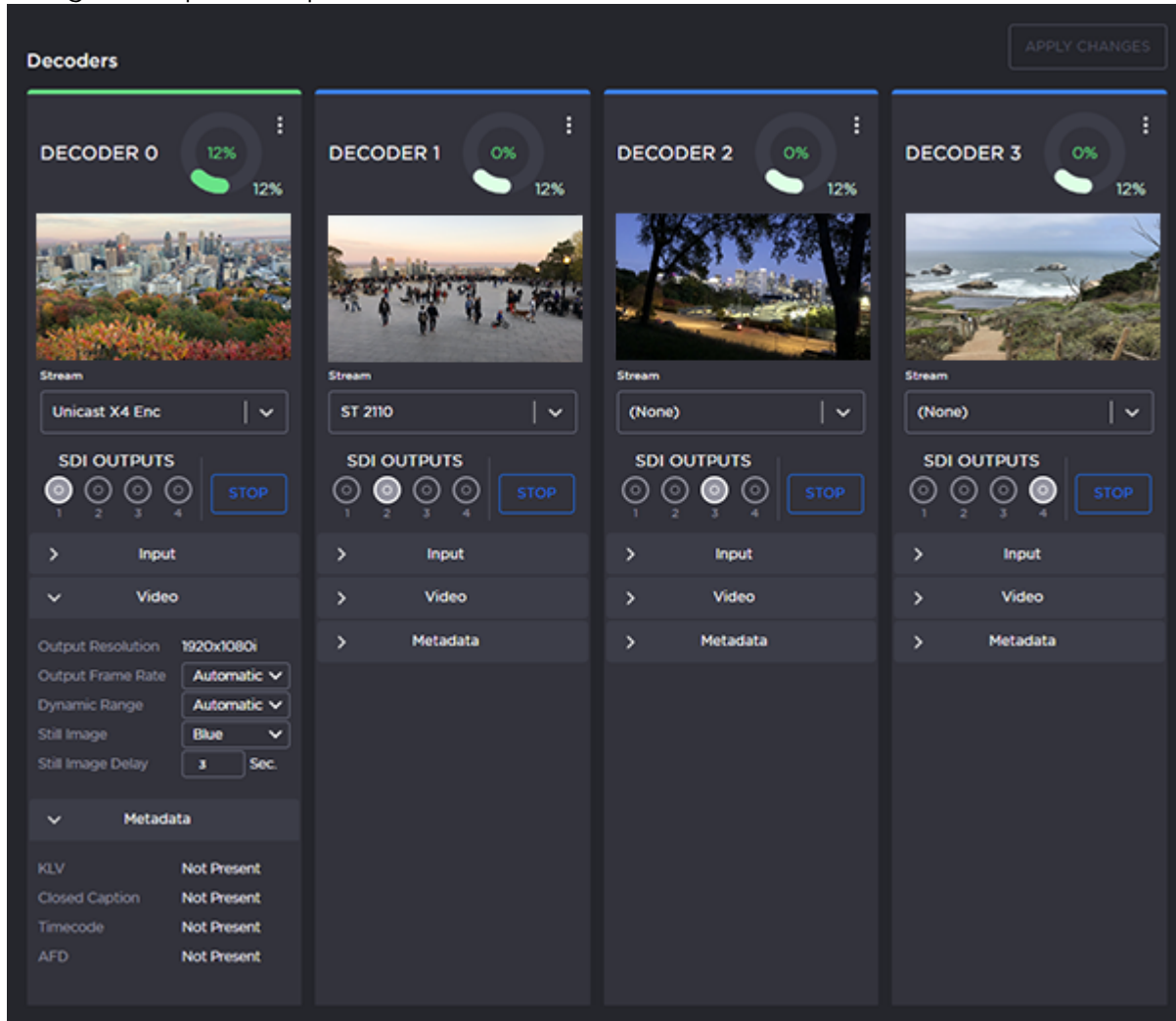


- To configure decoder settings, select **Decoders** from the side menu.
- To set up streaming, select **Streams** from the side menu.
- To access the administration or security settings, select **Settings** or **Security** from the side menu and then select the option from the tab bar, for example **Network** or **Accounts**.
- To access online **Help**, select **Help Center** from the side menu. This opens the **Haivision InfoCenter** website to the Makito X4 decoder documentation page.

Note

If no external internet connection is available, a local Makito X4 decoder online Help is opened in your Web browser. For the most up-to-date documentation, please visit the [Haivision InfoCenter](#).

- (Where applicable) Click the arrow (>) to expand or collapse the Decoders or Streams configuration panels. The following example shows the Decoder 0 Input, Video and Metadata configuration panels expanded.



Tip

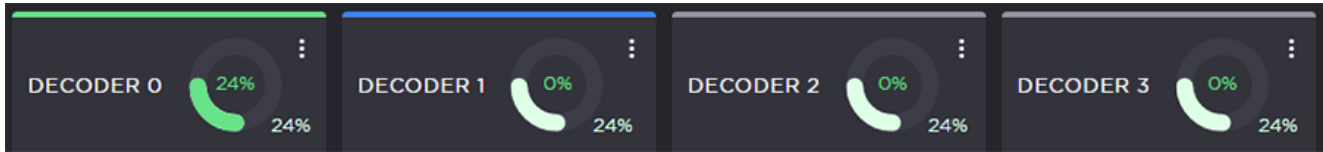
The donut charts on each Decoder panel show the resources used per decoder (darker green slice), as well as globally (lighter green slice). For more information, see [Donut Charts](#).

Related Topics

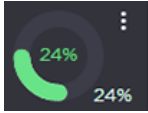
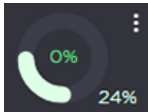
- [Donut Charts](#)

Donut Charts

The donut charts on the Control Center Decoder panels show the resources used per decoder, as well as globally.



The actual percent usage for the decoder is displayed as text within the ring, while the slice length gives a quick glance view of the percentage. The slice color also changes as follows:

	Darker green	Indicates the percentage of resources used for that decoder.
	Lighter green	Indicates overall percentage of resources used. It is the same value on all active decoders.

The color bar at the top of each Decoder panel indicates the status of the streams assigned to it (if any):

Color	Indication	Description
Blue	Listening	The decoder has started and is currently waiting for an input stream to be received / connected.
Green	Active	The decoder has started and is actively decoding a stream.
Gray	Inactive	The decoder is stopped.
Red	Error	The decoder has started but is unable to decode the incoming stream due to some errors. Please see the decoder statistics for more details on the error.

Changing Your Password

- Password Requirements

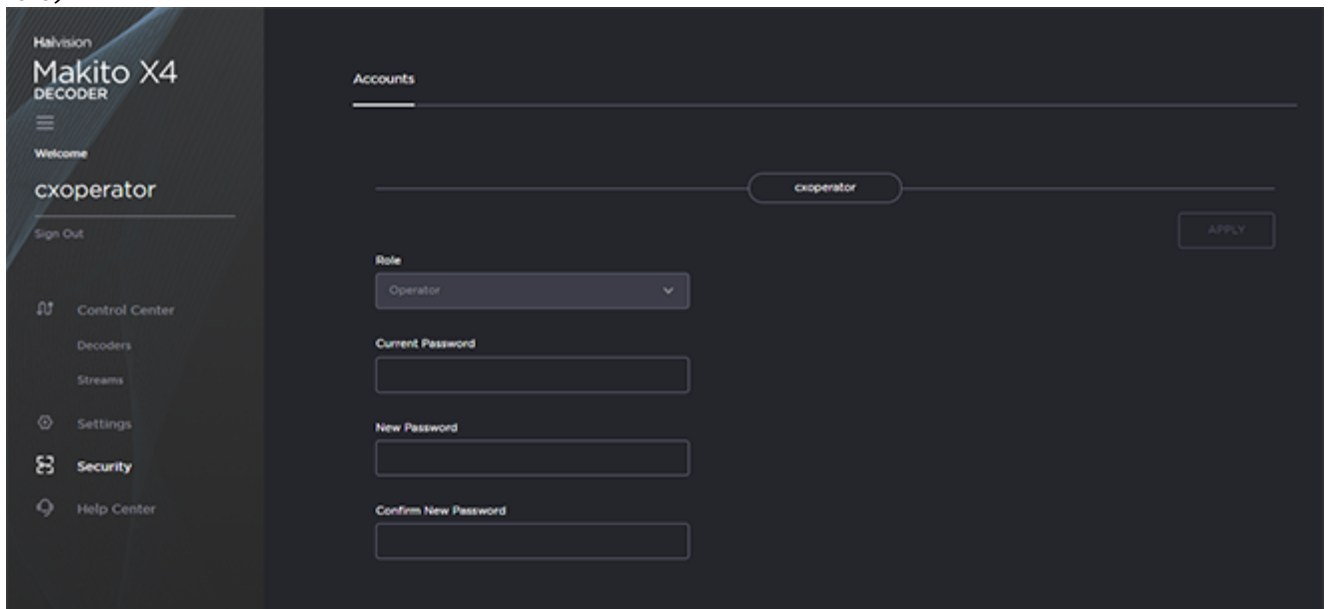
! Important

For security purposes, be sure to change the default password!

You can change your password from the Accounts page.

To change your password:

1. To navigate to the Accounts page, click **Security** on the side menu. The Accounts page opens. (The following example shows the Security privileges for the Operator role).



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

✓ 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 this only applies to SSH CLI access to the decoder. For more information, see [pubkey](#) (CLI command).

Password Requirements

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

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

⚠ Note

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

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

Signing Out

After you finish using the Makito X4, be sure to sign out. To do so, click **Sign out** from the side menu.

Signing out prevents misuse and unauthorized access to the decoder.

Managing the Decoder

Note

For a management overview of the Makito X4 Decoder as well as an overview of the Web interface, see [Getting Started with the Web Interface](#).

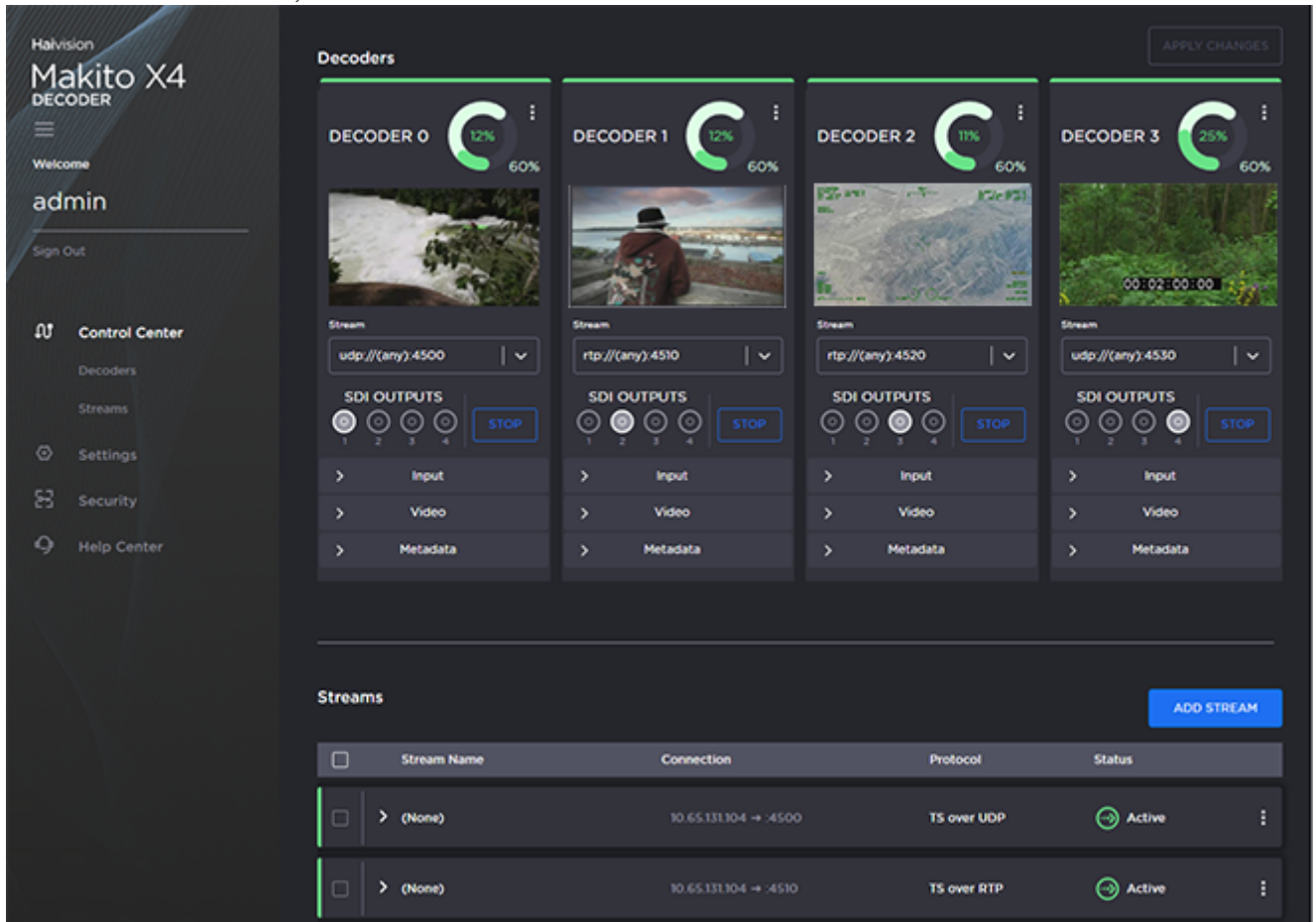
Topics in This Chapter

- [Configuring Decoder Outputs](#)
- [Configuring Streams](#)

Configuring Decoder Outputs

To configure decoder outputs:

1. On the Control Center, select **Decoders** from the side menu.



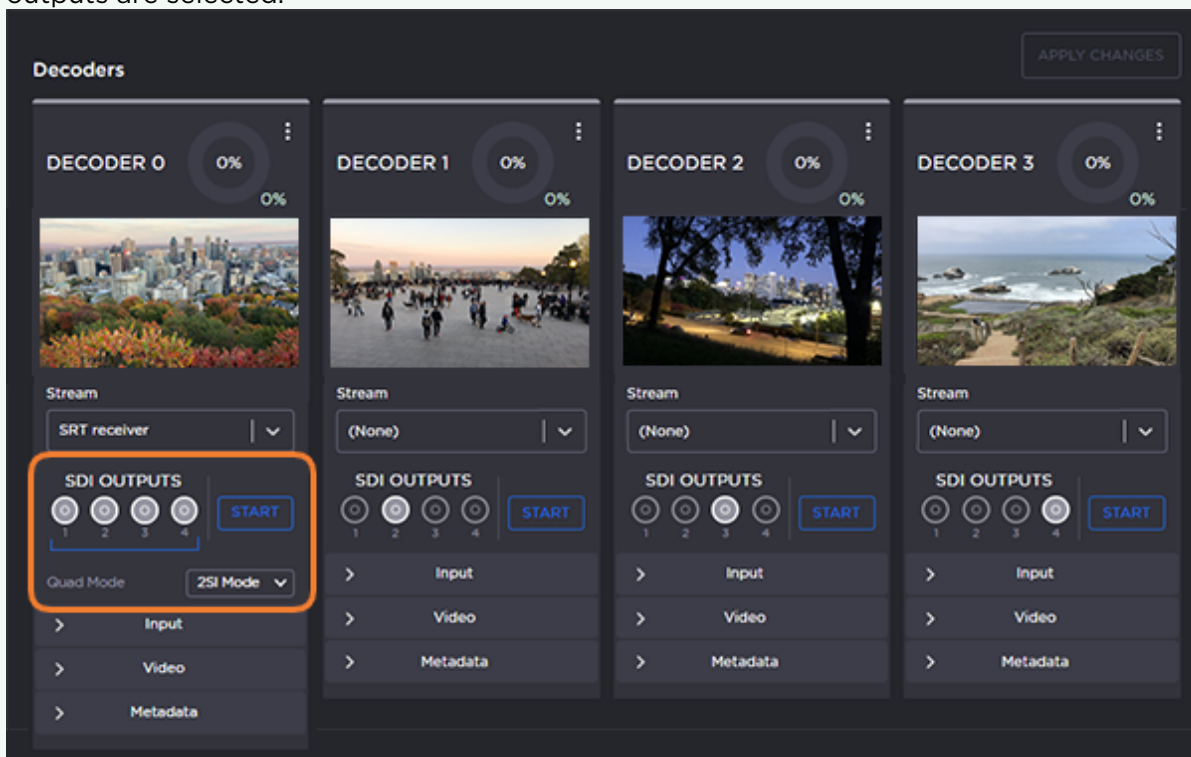
2. Select the decoder to configure, for example Decoder 0.
3. Select the Output port(s) for the decoder (if not using the default selection).
You can route the decoded video and audio to any set of physical outputs. This allows you to specify the interface(s) on which you want to see the video.


Important

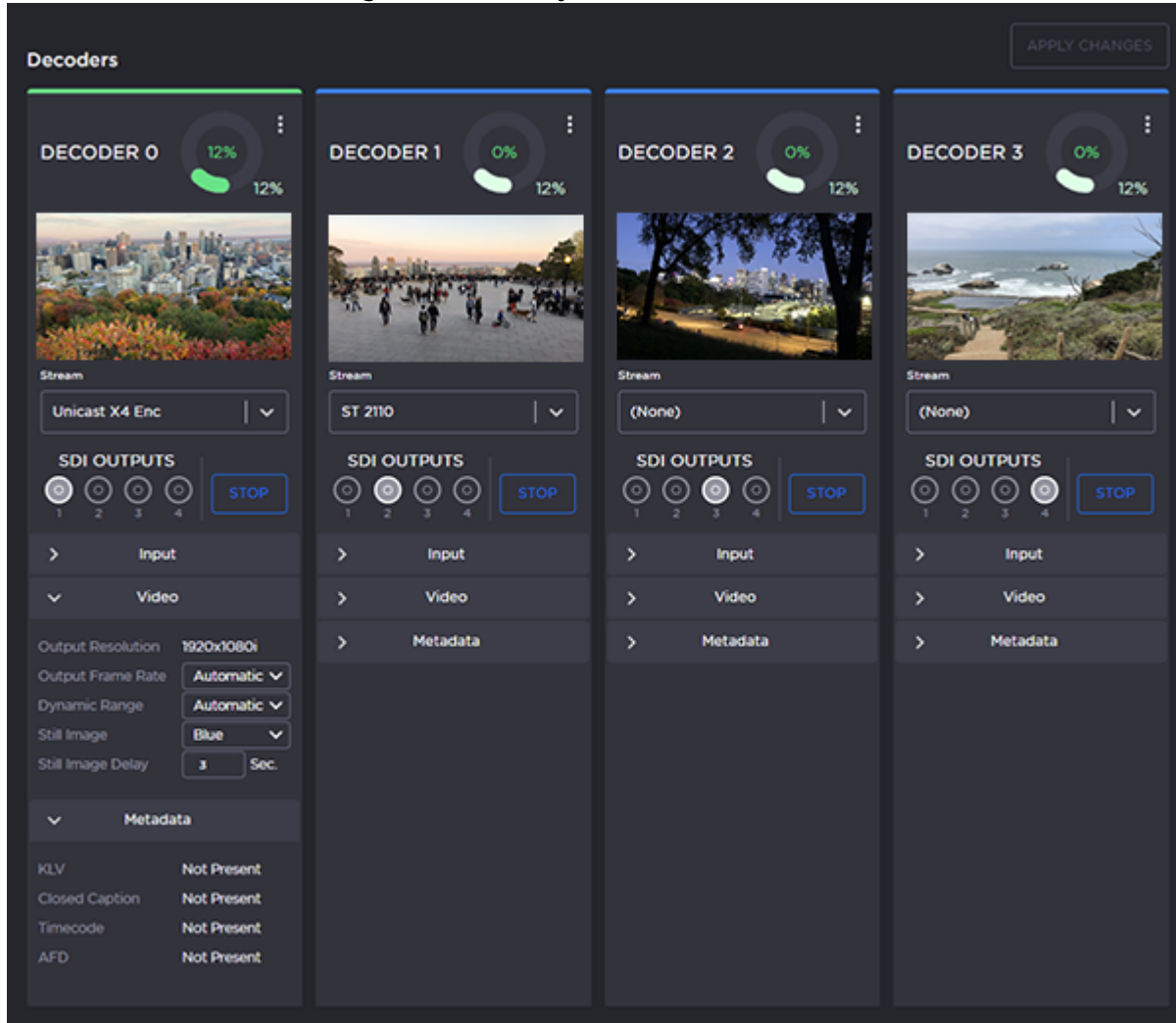
Decoder 0 has highest priority, and the video decoding resources are prioritized with the lower decoder numbers (i.e., 0, then 1, 2, and 3) having higher priority. For more information, see [Oversubscription of Decoder Channels](#).

Tip

To configure 2SI UHD output mode, select all four SDI outputs for the decoder channel. Then select 2SI Mode from the Quad Mode drop-down that becomes available when all four outputs are selected.



- Click the Input, Video and Metadata arrows () to expand the configuration panels. Some of the Decoder settings are read-only.



 **Tip**

The donut charts on each Decoder panel show the resources used per decoder (darker green slice), as well as globally (lighter green slice). For more information, see [Donut Charts](#).

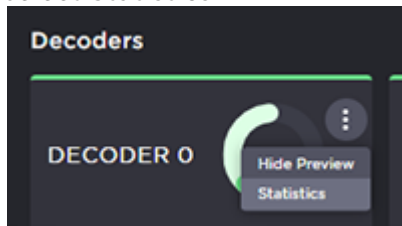
- Adjust settings where available. For example, you can change the Input Mode, Output Frame Rate, Still Image type, and Still Image Delay.

 **Note**

The decoder will display the Still Image if it is no longer receiving video (for example, if the encoder stream has stopped or the network connection is lost).

- Click **Start** to begin decoding the stream.

7. To view statistics for the decoder, click the More Options ("three dots") menu icon and select **Statistics**.



✓ **Tip**

For information on configuring multi-channel synchronization on the Makito X or Makito X4 encoder and decoder, see [Multi-channel Synchronization](#).

Topics Discussed

- [Decoder Settings](#)
- [Decoder Statistics](#)
- [Oversubscription of Decoder Channels](#)

Decoder Settings

The following table lists the decoder controls and settings for each decoder core:

[General](#) [Input](#) [Video](#)

General

Setting	Default	Description/Values
Stream	None	Select the stream from the drop-down list of available streams. See Configuring Streams .
SDI Outputs	Dec0 → SDI1 Dec1 → SDI2 Dec2 → SDI3 Dec3 → SDI4	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Note</p> <p>You can route the decoded video and audio to any set of physical outputs. This allows you to specify the interface(s) on which you want to see the video. A single decoder can output to one or more SDI outputs. See Configuring Decoder Outputs.</p> </div>
Quad Mode	Normal	<p>(All four SDI outputs must be selected for the decoder) Outputs a UHD (Ultra High Definition, 3840 x 2160) stream split into four 3G signals. Each of the four 3Gb/s HD-SDI links transmits a quarter of the video to be displayed as a full UHD image. These four signals are then combined to create a composite UHD resolution image that runs at 12Gb/s.</p> <p>Select the method to split the pixels:</p> <ul style="list-style-type: none"> • Normal - Outputs the video as individual outputs, i.e., outputs four times 4k. • 2SI Mode - Outputs the video using two sample interleaved (2SI) reduced resolution (as per SMPTE 435). Groups of two pixels are separated from the image and sent on four different links. 2SI puts the two first samples of the first line on link A, then the two next in link B and repeats this process over line 1. Then line 2 of the picture is divided exactly the same but put in links C and D, and identically for even and odd lines alternatively.

[General](#) [Input](#) [Video](#)

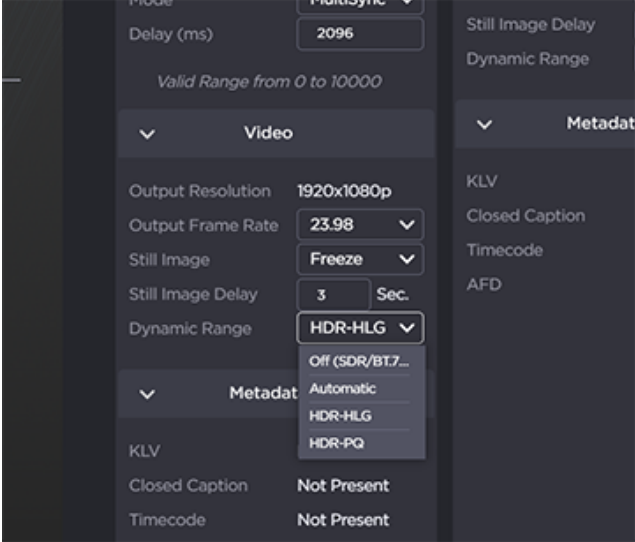
Input

Setting	Default	Description/Values
Resolution	N/A	(Read-only) The input signal detected from the incoming video stream. It includes the number of pixels per line, and whether the video is interlaced or progressively scanned (indicated by i or p).
Audio	N/A	(Read-only) The sampling rate of the incoming audio signal.

Setting	Default	Description/Values
Mode	Automatic	<p>The type of buffering to use. A jitter buffer temporarily stores arriving packets in order to remove the effects of jitter from the decoded stream.</p> <ul style="list-style-type: none"> Note The added delay will not decrease with time even if the video jitter disappears. <p>The added delay depends on the monitored video jitter. It also depends on the audio arrival time; if the audio is late, this delay will be added to the current calculated delay. For example, if the audio is late by 500 ms (vs Video), an additional 500 ms delay will be added to allow the Audio/Video synchronization.</p> <ul style="list-style-type: none"> Fixed: Fixed mode allows users to specify a delay to be added to the decode pipeline after the content is decoded. The amount of delay does not vary and artifacts may result if a too low value is used. (See "Delay (Fixed Mode)" below.) <ul style="list-style-type: none"> Note The decoder has a minimum buffer set based on the resolution and frame-rate of the stream content. In addition, users can add more delay if desired: (1) to achieve a specific decoding latency for inter-channel synchronization purposes; (2) to deal with unusually large amounts of jitter in the stream; or (3) to allow A/V sync to occur when the stream content is highly out of sync. MultiSync: Use to synchronize the content across multiple channels to within one frame period. This is designed to allow down-stream equipment to switch smoothly between video and audio sources. You need to set the "(MultiSync) Delay" on all of the decoder channels to the same value. For the steps to configure multi-channel sync on a Makito X or Makito X4 Series encoder and decoder, see Multi-channel Synchronization.
Delay (Fixed Mode)	0 ms	<p>The delay in ms when using buffering in Fixed mode. Range = 0...3000 ms</p> <ul style="list-style-type: none"> Note The maximum delay is 2000 ms. If for any reason the system requires more than this value to play smoothly, video or audio artifacts will be noticed.
Delay (MultiSync Mode)	1000 ms	<p>The delay in ms required to ensure that two or more decoder channels are synchronized. Range = 0...10000 ms</p> <ul style="list-style-type: none"> Note The difference in the values between the decoder channels cannot exceed 2000 ms.

Video

Setting	Default	Description/Values
Output Resolution	N/A	(Read-only) The dimensions of the frames (width and height) sent to the display, with an indicator (i or p) designating whether the video is interlaced or progressive.
Output Frame Rate	Automatic	<p>The frame rate per second generated for the displays:</p> <ul style="list-style-type: none"> Automatic: The decoder will select the best display frame rate based on the stream parameters and the connected display's capabilities. 75, 60, 59, 50, 30, 29, 25, 24 or 23 <div style="border: 1px solid #f0e68c; padding: 5px;"> <p>i Note</p> <p>If Automatic is selected, the actual frame rate generated will be the next highest valid frame rate supported by the SDI and HDMI interface, plus the one that gives the best decimation factor. For example, 30 Hz could be chosen instead of 29.970 Hz.</p> </div>
Still Image	Freeze	<p>This setting controls what the decode channel outputs when the decoder is not receiving a video stream (e.g., a stream is stopped (at the encoder) or the network connection fails). A still image is inserted on the output SDI interface having the same resolution and frame rate as the last decode picture of the last stream. The options available are:</p> <ul style="list-style-type: none"> Freeze: continues to display the last decoded video frame. Black Screen: displays a black screen. Blue Screen: displays a blue screen. Color Bars: displays a series of vertical color bars across the width of the display. Mute: disables the video output. <div style="border: 1px solid #f0e68c; padding: 5px;"> <p>i Note</p> <p>When the still image is substituted on the display outputs, the video frame rate and resolution will be maintained.</p> </div>
Still Image Delay	3	<p>The delay in seconds before the still image is displayed. Range = 1...1000 seconds</p> <div style="border: 1px solid #f0e68c; padding: 5px;"> <p>i Note</p> <p>Until the selected still image is displayed, the output will freeze.</p> </div>

Setting	Default	Description/Values
Dynamic Range	Automatic	<p>(10-bit Chroma Subsampling must be selected) Select to configure the decoder to detect the inbound High Dynamic Range (HDR) transfer function signaling and forward that information within the decoded stream.</p> <ul style="list-style-type: none"> • Off (Standard Dynamic Range (SDR)/BT.709) • Automatic: the decoder detects HDR transfer function from the encoder • 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 

Decoder Statistics

The following tables list the Decoder statistics:

- [General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)




General

Statistic	Description/Values
Decoder ID	ID Number of the decoder (Possible values are 0 to 3).
State	<p>Current state of the decoder engine. Possible values are:</p> <ul style="list-style-type: none"> • STOPPED - The decoder is currently stopped by the user. • STARTED - The decoder is currently started by the user. • ACTIVE - The decoder is processing an active stream. • NOT DECODING (reason) - The decoder is not decoding some or all of the stream. The “reason” can be one of the following: <ul style="list-style-type: none"> • Unsupported - The stream has content that is not supported by this platform. Most notably, H.264 1080i content is not supported. • Unlicensed - The stream has components that are not licensed to process. For example, this can be KLV, UHD resolutions, or HEVC. • Oversubscribed - The decoder is currently started by the user; however, there are insufficient processing resources to decode the video portion of the active stream. Higher priority decoders (those that have lower Decoder IDs) are consuming the resources. See Oversubscription of Decoder Channels. • No Memory - There was not enough memory in the system to decode the video stream. Audio and metadata are unaffected.
Up Time	Time elapsed since the decoder was first started.
Oversubscribed Frames	If the decoder was oversubscribed at any point, the number of frames that were rejected as a result.

- [General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Buffering Statistics

Statistic	Description/Values
Buffering State	<p>The state of the buffering module. Possible values are:</p> <ul style="list-style-type: none"> • IDLE - The buffering module is running, but not actively processing data. • ACTIVE - The buffering module is actively processing data. • MultiSync NO NTP CLIENT - MultiSync buffering was selected but NTP client is not active • MultiSync Timecode NOT PRESENT - MultiSync buffering was selected, but the stream does not contain the required timecode. • MultiSync Timecode INVALID - MultiSync buffering was selected, but the timecode in the stream is considered to be invalid. The embedded timecode is likely not close enough to the current system time or it may even be in the future.

Statistic	Description/Values
Buffering Mode	<p>The type of buffering used: Automatic, Fixed or MultiSync. See Decoder Settings Input>Mode.</p> <div style="border: 1px solid green; padding: 5px;"> <p> Tip If the mode is FIXED, advice on the minimum recommended delay setting is also provided.</p> </div>
Buffering Adjustments	<p>The number of times the buffering delay has been adjusted, based on streaming conditions and system jitter, and when the last adjustment was. For example: 4 (Last: 14h49m33s ago)</p>
Video Latency	<p>The delay from streaming receive time to the display of video frames with the current buffering scheme.</p>
PCR Updates	<p>The number of times the PCR (Program Clock Reference) was updated, and the length of time elapsed since the last one. The PCR is the clock reference that is contained in the MPEG transport stream.</p>
STC Updates	<p>The number of times the STC (System Time Clock) was updated, and the length of time elapsed since the last one.</p> <div style="border: 1px solid green; padding: 5px;"> <p> Tip For lower latency, the STC runs ahead of the PCR. For higher latency, the STC runs behind the PCR.</p> </div>
STC Lead Time Adjusts	<p>The number of times the lead time for video decoding and output was adjusted, and when the last adjustment was.</p>
STC to PCR Lead Time	<div style="border: 1px solid yellow; padding: 5px;"> <p> Note The PCR (Program Clock Reference) is the clock reference that is contained in the MPEG transport stream. The STC (System Time Clock) is the clock reference that the output of video, audio and KLV frames are scheduled against. For lower latency, the STC runs ahead of the PCR. For higher latency, the STC runs behind the PCR.</p> </div>
Packets Sent Late	<p>The number of packets sent internally through the decoder later than expected and when the last one was. If it does not appear, there weren't any.</p>
MultiSync Delay Set	<p>(MultiSync only) The delay set by the user and an indication of whether or not the delay is in range. Possible values include:</p> <ul style="list-style-type: none"> • X ms (Too Low) - The MultiSync delay setting is too low. See the MultiSync Delay Range below. • X ms (Too High) - The MultiSync delay setting is too high. See the MultiSync Delay Range below. • X ms (In Range) - The MultiSync delay setting is in the acceptable range.
MultiSync Delay Actual	<p>(MultiSync only) The measured delay of the actual data, for comparison against the set value.</p>
MultiSync Delay Range	<p>(MultiSync only) The range of acceptable values for "MultiSync Delay Set" based on streaming characteristics and system jitter.</p>
Max Input Jitter	<p>A measure of the input stream jitter (the variation of arrival time to the decoder). This contributes to the CBUF Delay (i.e., internal delay in the buffering module).</p>
Non-Video Late	<p>If non-video content (e.g., audio or KLV) is muxed later than the video, this statistic shows how much later it is. The video must be delayed by this much time to play in sync. Stream CBR content will typically have this, whereas VBR / low-latency content will not. This contributes to the CBUF Delay (i.e., internal delay in the buffering module).</p>

Statistic	Description/Values
Video Decoder Latency	A measure of input-to-output delay of the video decoder accelerator. Contributes to the STC Lead Time required for the video.
Video Decoder Jitter	A measure of the variability of the video decoder accelerator processing. Contributes to the STC Lead Time required for the video.
Hardware Delay	An additional delay applied for smooth playback. Contributes to the STC Lead Time required for the video.
Video STC Lead Time	A measurement of how far in advance of the time the frame needed to be played, the decoder output went out for display. A negative number here means the frame went out after it was time to play it.
Last Video Skip/Replay	How long ago the last video skip/replay event occurred.
Audio STC Lead Time	A measurement of how far in advance of the time the frame needed to be played, the decoder output went out for playback. A negative number here means the frame went out after it was time to play it.
Last Audio Skip	How long ago the last audio skip event occurred.

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Video Statistics

Statistic	Description/Values
Algorithm	The video compression standard in use. Possible values are H.264 and H.265.
Color	The color space encoding in the video stream. Possible values are: <ul style="list-style-type: none"> 4:2:0 8-bit 4:2:0 10-bit 4:2:2 8-bit 4:2:2 10-bit
Profile	The profile tier for the incoming video stream from the H.264 / H.265 standard: <ul style="list-style-type: none"> (AVC/H.264) Main, High, or Baseline (HEVC/H.265) Main or High, optionally with 4:2:2 and/or 10-bit <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>The profiles and levels are defined in the corresponding AVC/H.264 or HEVC/H.265 specifications.</p> </div>
Level	The level tier from the H.264 / H.265 standard (i.e., the required level of decoder performance to be able to process the incoming video stream): <ul style="list-style-type: none"> (AVC/H.264) 3, 3.2, 4, or 4.2 (HEVC/H.265) 1, 2, 2.1, 3, 3.1, 4, 4.1, 5, 5.1, 5.2, 6, 6.1 or 6.2
Format	The format of the video stream as it was encoded. This information includes resolution (Width x Height), picture structure (“p” for progressive, “i” for interlaced) and frame rate. Example: 1280x720p59.94.

Bit Rate	Measured rate of data transfer that is being received in the video stream.
Framing	The framing structure detected in the stream. Possible values are: <ul style="list-style-type: none"> • I - Only I frames are detected in the GOP • IP - Only I and P frames are detected in the GOP • IBP - I, P and one B-frame are detected in the GOP • IBBP - I, P and two B-frames are detected in the GOP • IBBBP - I, P and three B-frames are detected in the GOP • IBBBBP - I, P and four B-frames are detected in the GOP • I + N B-pictures - I and N B-frames are detected in the GOP (where N is the number of B-frames that were found). • IP + N B-pictures - I, P and N B-frames are detected in the GOP (where N is the number of B-frames that were found). • Intra Refresh - No I-frames have been detected in the GOP since the decoder was started.
GOP Interval	The distance between I-frames in the stream (measured in frames).
Slices per Frame	The number of H.264/H.265 NAL slices produced per video frame in the encoder.
Stream ID Changes	How many times the stream ID was changed in the decoder configuration (and when the last one occurred).
Format Changes	How many times the video format changed in the stream (and when the last one occurred).
Input Frame Rate	A measurement of how many video frames per second were received in the input stream. If this value is significantly less than the frame rate in the stream format, the decoder will need to produce replayed frames to compensate.
Still Image	Information about the still image. It can be ACTIVE or INACTIVE. This line also includes how many times the still image was presented, the maximum amount of time it was turned on, when it was last turned on and off. For example: FREEZE (INACTIVE) [Count=0, Max=0s, Last On=Never, Last Off=Never]
Output Pkt List Ovflws	Number of times the video preprocessor output packet list overflowed and when. Not present if it never occurred.
Video Decoder State	The state of the video decoder engine. Possible values include: <ul style="list-style-type: none"> • IDLE - The video decoder engine is not decoding frames. • ACTIVE - The video decoder engine is actively decoding frames.
Display Format	The currently configured display format. This information includes resolution, picture structure and frame rate. For example 1920x1080p60.
Video Decoder Load	How much of the system's total video decoding capacity that is taken up by the current stream. The total capacity is 3840x2160 at 60fps. For example, a stream encoded at 1920x1080p60 would consume 25% of the total video decoding capacity.
Preprocessor State	The current state of the video preprocessor. Possible values are: <ul style="list-style-type: none"> • IDLE - The video preprocessor is not actively receiving data. • ACTIVE - The video preprocessor is actively receiving data. • UNSUPPORTED - The video stream is not supported by our implementation. This includes interlaced H.264 streams and video larger than 3840x2160p. • UNLICENSED - The video stream contains features that are not permitted by the current license set. This can include 4:2:2 color space, 10-bit, and a higher resolution than is currently licensed (Tiers are SD, HD, Full-HD, and UHD).

Unlicensed Reason	If the Preprocessor State is UNLICENSED, this provides the reason. The reason is one of the following: <ul style="list-style-type: none"> • KLV - KLV is in the stream but is unlicensed. KLV output is disabled. • SRT - The stream is SRT but this feature is not licensed. Streaming is disabled.
Unsupported Reason	If the Preprocessor State is UNSUPPORTED, this provides the reason. The reason is one of the following: <ul style="list-style-type: none"> • H.264 Interlaced - This combination is not supported by the platform. • H.264 Intra Refresh - This combination is not supported by the platform. • Second 4k H.264 4:2:2 10-bit Video - Only of these is supported by the platform.
Video Input Packets	The number of video input packets recognized by the decoder.
Encoded Format	The format of the video stream as it was encoded. This information includes resolution (Width x Height), picture structure (“p” for progressive, “i” for interlaced) and frame rate. Example: 1280x720p59.94.
Hardware Counters	
Displayed Output Frames	Number of decoded output frames that were successfully displayed, and when the last one occurred.
Skipped Output Frames	Number of decoded output frames that were not displayed but instead were “skipped” and when the last one occurred. Skipped output frames can occur if the frame arrived too late at the display engine.
Replayed Output Frames	Number of times the last output frame had to be replayed because no new content was available to be displayed.

- [General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)

[Closed Caption](#)
[Timecode](#)

Audio Statistics

Statistic	Description/Values
Audio Decoder State	The state of the audio decoding engine. Possible values are: <ul style="list-style-type: none"> • IDLE - The audio decoder engine is running, but not decoding frames. • ACTIVE - The audio decoder engine is actively decoding frames. • STOPPED - The audio decoder engine is stopped.
Audio Sample Rate	The audio sampling rate of the incoming stream.
Number of Pairs	The number of audio pairs currently being decoded.
Decoded Frames	The number of decoded audio frames.
Played Output Frames	The number of output audio frames that were successfully played on time, and when the last one occurred.
Skipped Output Frames	The number of output audio frames that were not played because the content did not arrive at the playback engine in time.
Audio Pair #1/2/3/4	
Audio Mode	The number and type of audio channels being decoded, either Stereo, Mono-Left or Mono-Right.

Audio Compression	The compression standard used to encode the audio stream. Possible values include AAC-LATM, AAC-ADTS, MP1, MP2 or MP3.
Audio Bitrate	The measured bit rate of the data flowing in this audio channel.
AV Sync	How close audio and video are to being played in perfect sync.
(TS) Discontinuities	How many times a discontinuity (which is an unexpected jump in the audio time stamp) occurred and how long ago the last one was seen.
Decoder Errors	For this audio channel, how many times the decoder failed and returned an error code.
Output Errors	For this audio channel, how many times an audio frame was successfully decoded but could not be sent out.
Sample Rate In	The detected audio sample rate in the stream in Hz.
Sample Rate Out	The output audio sample rate in Hz.

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Metadata Statistics

Statistic	Description/Values
Metadata Decoder State	The state of the metadata decoding engine. Possible values are: <ul style="list-style-type: none"> • IDLE - The audio decoder engine is running, but not decoding frames. • ACTIVE - The audio decoder engine is actively decoding frames. • STOPPED - The audio decoder engine is stopped.
Active Metadata	The kinds of metadata currently active in the decoder. Possible values include: <ul style="list-style-type: none"> • TC - Timecode • CC - Closed captioning • AFD - Active Format Description • KLV - Key-Length-Value More than one may be present. In that case, they are all listed. For example, a stream with both CC and TC would show as "TC, CC".
Timecode	If present, the current value of the timecode in the stream.
Channel Stats	Up to four channels may be present. Each channel has its own unique set of the following stats:
Received Packets	Number of packets received for processing.
Output Packets	Number of packets sent to the SDI output vertical blanking.
Latency	The latency of the metadata as it is going out.

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Clock Recovery Statistics

Statistic	Description/Values
Tracking Mode	Whether or not clock recovery is ENABLED.
Status	The current status of clock recovery. Possible values are: <ul style="list-style-type: none"> LOCKED - The clock adjustment did not vary by more than 5 ppm in the last 2 minutes. UNLOCKED - The clock adjustment was over 5 ppm in the last 2 minutes.
ReSync Count	The number of times clock recovery needed to resynchronize.
PCR Update	The number of times the PCR needed to be updated and when the last one occurred.
Current STC	The current value of the System Time Clock, and how far away from the nominal frequency in PPM.
STC Avg (last 2 min)	Average value of the the STC clock for the last 2 minutes, plus the deviation in PPM.

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

High Dynamic Range (HDR) Statistics

Statistic	Description/Values
Dynamic Range in Stream	For HDR, the dynamic range that was detected in the stream. Possible values are SDR, HLG, PQ, UNSPECIFIED (not present) and CUSTOM (not recognized).
Dynamic Range Output	For HDR, the dynamic range that is being sent to the output SDI. Possible values are SDR, HLG and PQ.
Color Primaries	The value of color primaries present in the H.264 or H.265 video stream. Example: 1 (ITU-R BT.709-5)
Transfer Characteristics	The value of transfer characteristics present in the H.264 or H.265 video stream. Example: 1 (ITU-R BT.709-5)
Matrix Coefficients	The value of matrix coefficients present in the H.264 or H.265 video stream. Example: 1 (ITU-R BT.709-5)

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Closed Caption Statistics

Statistic	Description/Values
Received Packets	Number of packets received for processing.

Statistic	Description/Values
Output Packets	Number of packets sent to the SDI output vertical blanking.

[General](#)
[Buffering](#)
[Video](#)
[Audio](#)
[Metadata](#)
[Clock Recovery](#)
[High Dynamic Range \(HDR\)](#)
[Closed Caption](#)
[Timecode](#)

Timecode Statistics

Statistic	Description/Values
Received Packets	Number of packets received for processing.
Output Packets	Number of packets sent to the SDI output vertical blanking.
Timecode Value	If present, the current value of the timecode in the stream.

Related Topics:

- [Decoder Settings](#)

Decoder Statistics Example

Decoder 0
Refresh Every 2s ▼
RESET

Statistics

General

State	Active
Up Time	15h26m14s

Buffering

Buffering State	ACTIVE
Buffering Mode	AUTOMATIC
Buffering Adjustments	4 (Last: 15h25m43s ago)
Video Latency	141 ms
STC to PCR Lead Time	57 ms (STC is ahead of PCR by 57 ms)

Video

Algorithm	H.265
Profile	Main
Level	5.1
Framing	IP
Slices per Frame	1
Preprocessor State	ACTIVE
Video Input Packets	1665512
Video Decoder State	ACTIVE
Encoded Format	1920x1080p29.97
Display Format	1920x1080p29
Video Decoder Load	12%
Still Image	FREEZE (INACTIVE) [Count=0]
Displayed Frames	1,665,434 [99.99%] (Last: 0s ago)
Skipped Frames	47 [0.00%] (Last: 15h25m42s ago)
Replayed Frames	72 [0.00%] (Last: 15h25m42s ago)

Audio

Audio	
Audio Decoder State	ACTIVE
Audio Sample Rate	48 kHz
Number of Pairs	1
Decoded Frames	2,602,810 (Last: 0s ago)
Played Frames	2,602,569 [100.00%] (Last: 0s ago)
Skipped Frames	13 [0.00%] (Last: 15h25m7s ago)
Audio Pair #1	
Audio Mode	Stereo
Audio Compression	AAC-ADTS
Audio Bitrate	80.33 kbps
AV Sync	15 ms
Discontinuities	0
Decode Errors	0 (Last: Never)
Output Errors	0 (Last: Never)
Sample Rate In	48000 Hz
Sample Rate Out	48000 Hz
Clock Recovery	
Tracking Mode	ENABLE
Status	LOCKED (0.0PPM)
ReSync Count	2
Current STC	27,000,056Hz (2PPM from Nominal)
STC Avg (last 2 min)	27,000,055Hz (Deviation 0.0PPM)
High Dynamic Range (HDR)	
Dynamic Range In Stream	SDR
Dynamic Range Output	SDR
Color Primaries	1 (ITU-R BT.709-5)
Transfer Characteristics	1 (ITU-R BT.709-5)
Matrix Coefficients	1 (ITU-R BT.709-5)

Oversubscription of Decoder Channels

Oversubscription occurs when the sum of the streams being decoded exceeds the capabilities of the decoder. This can be due to bitrate (aggregate bitrate ingress limit) or resolution/frame-rate (limit is 1 x UHDp60 or equivalent). This topic explains the behavior of the decoder when streams are sent that overtax its capabilities.

The Makito X4 decoder can decode up to a single 3840x2160p60 stream. This represents 100% of the system's decoding capacity.

The video decoding resources are prioritized with the lower decoder numbers having higher priority, i.e.:

- Decoder 0 has highest priority
- Decoder 1 has 2nd highest priority
- Decoder 2 has 3rd highest priority
- Decoder 3 has lowest priority

This priority logic is only exercised if one of the active streams is UHD, because the Makito X4 can decode up to four 1920x1080p60 streams simultaneously without difficulty.

Oversubscription occurs when more than one 3840x2160p60 stream or more than two 3840x2160p30 streams are decoded. In this situation, Decoder 0 will always run, and Decoder 1 will run if there are enough resources remaining, then Decoder 2, then Decoder 3.

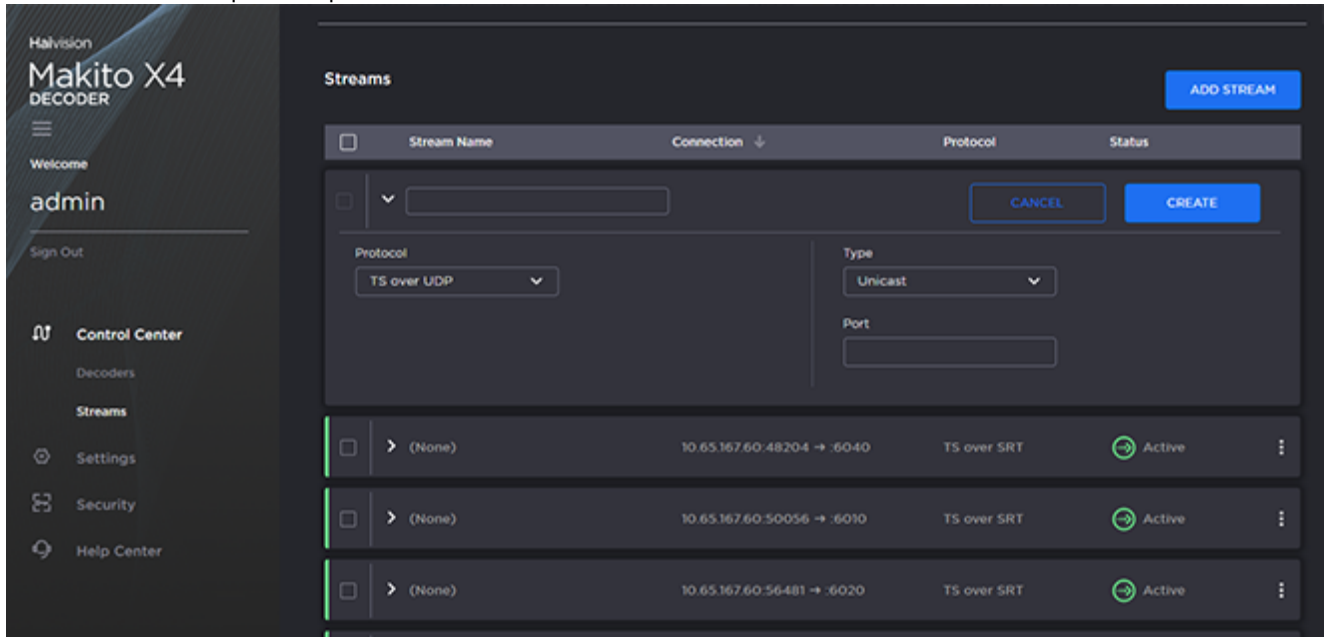
! Important

Any streams that are mission-critical and cannot be interrupted should always be decoded on Decoder 0. The lower-priority decoders that are running may be interrupted during decoding if the video decoding resources are required for a higher-priority decoder.

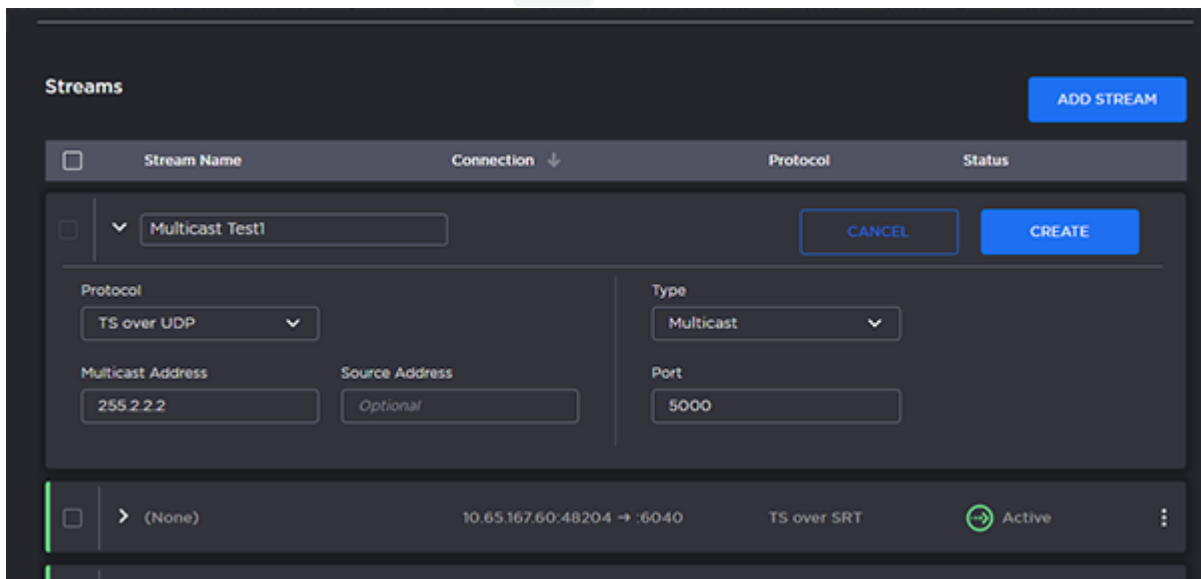
Configuring Streams

To add a stream:

1. On the Control Center, click **Add Stream** to add the first stream. The New Stream panel opens.



2. Type a name for the stream in the Name field.
3. Select the stream Protocol, for example, **TS over UDP**.
4. Select the stream Type, either Unicast or Multicast.
5. For Multicast streams, type in the Multicast Address, for example, **225.2.2.2**.
6. Type in the Port number, for example, **5000**.



7. Click **Create**. The new stream is active and is added to the Streams List. The stream status indicators are as

follows:

Statuses

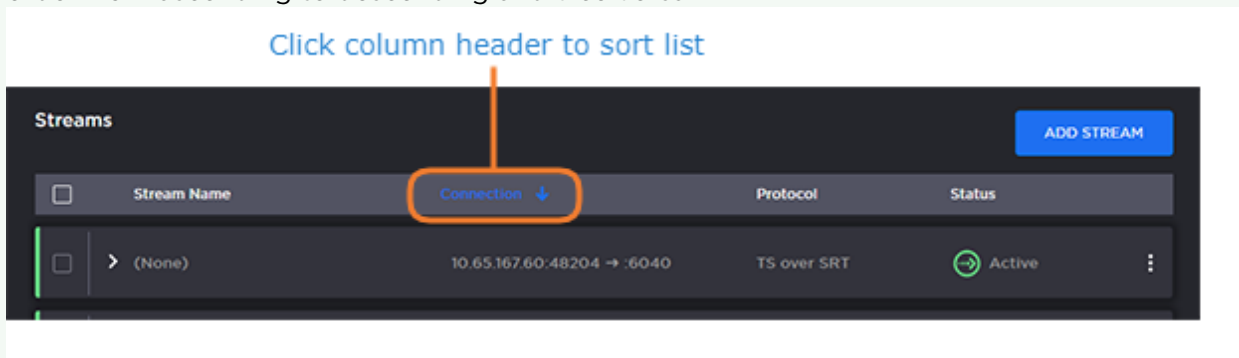
Streams will be either:

- Listening Blue
- Active Green
- Streaming Purple
- Inactive Gray
- Warning Amber
- Error Red

8. To add another stream, click **Add Stream** and follow the previous steps (Step #2 - #7) to configure the stream.

Tip

To sort the streams in the list by Stream Name, Connections, Protocol, or Status, simply click the column header to sort the list by. Clicking again changes the sort order from ascending to descending and vice versa.



Related Topics

- [Stream Settings](#)
- [Stream Statistics](#)

Stream Settings

The following table lists the stream controls and settings:

Stream Setting	Default	Description/Values
Name	N/A	Specify a name for the stream. 1 to 32 characters
Protocol	TS over UDP	Select the Encapsulation Protocol type for the decoded stream. <ul style="list-style-type: none"> • TS over UDP: MPEG transport stream over UDP (no RTP header) • TS over RTP: MPEG2 transport stream over RTP • TS over SRT: Haivision's Secure Reliable Transport (see Secure Reliable Transport (SRT))
Type	Unicast	Select the Stream Type for the decoded stream. <ul style="list-style-type: none"> • Unicast • Multicast
Multicast Address	N/A	(Multicast streams only) Enter the multicast IP address in dotted-decimal format.
Source Address	N/A	(Multicast streams only) The Source Address specifies where the multicast stream is coming from (i.e., what address is broadcasting). In cases where many devices are sending multicast streams on the same multicast address, specifying the source encoder address can reduce the amount of multicast traffic being forwarded on your network. Only the multicast traffic from that specific source to that address will be forwarded (instead of all of them).
Address	N/A	(TS over SRT only) Enter the source IP address in dotted-decimal format.
Port	N/A	Enter the source UDP port for the stream. Enter a number in the range 1025 . . 65,535 . Note that RTP streams use even numbers only within this range.
FEC	None	(Optional, TS over RTP only) Enable Forward Error Correction (FEC). Select either: <ul style="list-style-type: none"> • (None) • Pro-MPEG FEC (TS over RTP only) On the Encoder, you set all these parameters, whereas on the decoder they are detected from the stream, and are available in the stream stats.

Related Topics

- [SRT Stream Settings](#)

SRT Stream Settings

The following table lists the TS over SRT-specific parameters:

[Connection](#) [SRT Settings](#) [SRT to UDP Stream Conversion](#)

Connection

Setting	Default	Description/Values
Mode	Listener	Specifies the SRT Connection Mode (to simplify firewall traversal): <ul style="list-style-type: none"> • Caller: The decoder acts like an SRT caller and connects to a server listening and waiting for an incoming call. • Listener: The decoder acts like an SRT listener and listens for a server to connect to it. • Rendezvous: Allows calling and listening at the same time. To simplify firewall traversal, Rendezvous Mode allows the encoder and decoder to traverse a firewall without the need for IT to open a port.
Address	n/a	(Caller and Rendezvous Connection modes) Specifies the destination IP address for the SRT stream.
Source Port	Auto-Assign	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.</p> </div>
Destination Port	n/a	(Caller and Rendezvous Connection modes) Specifies the UDP destination port for the SRT stream.
Port	n/a	(Listener Connection mode only) Specifies the UDP local port for the SRT stream.

SRT Settings

Setting	Default	Description/Values
Latency	125	<p>Specifies how long the decoder will buffer received packets.</p> <div style="border: 1px solid #f0e68c; padding: 5px; margin: 5px 0;"> <p>Note</p> <p>The SRT buffer, configured as “Latency”, is the time reserved in the decoder to recover missing packets.</p> </div> <p>Because real-time video cannot be paused, restarted, slowed down, or accelerated, the buffer adds a fixed delay in the end-to-end latency. If a lost packet cannot be recovered, this may result in an A/V artifact. In this case, you should increase the SRT latency as it is likely too low. Please see the SRT Deployment Guide for tuning guidance.</p>
Encrypted	Off	Toggle to On to enable decryption of encrypted streams.
Passphrase	n/a	(Encrypted must be On; must match encoder passphrase) This parameter is required if the stream is encrypted and is used to retrieve the cryptographic key protecting the stream. Range = 10-79 UTF8 characters
Reject Unencrypted Callers	On	(Listener Connection mode only, and Encrypted must be On) For security reasons, when encryption is enabled in the decoder’s SRT Listener stream configuration, this option causes the decoder to reject all unencrypted SRT Caller streams.

SRT to UDP Stream Conversion

Setting	Default	Description/Values
Enable	Disabled	<p>Note</p> <p>The SRT input stream may be encrypted and includes error correction. Enable this to rebroadcast the SRT stream on the local LAN without the encryption and error correction elements over UDP. A single multicast or unicast destination TS/UDP stream is supported for re-streaming.</p>
Address	n/a	Specifies the destination IP address for the stream.
Destination Port	n/a	Specifies the UDP source port for the stream.
TTL	64	<p>(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.</p> <p>Range = 1..255</p>
ToS	184 or 0xB8	<p>(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.</p> <p>Range = 0..255 (decimal) or 0x00..0xFF (hex)</p> <p>Important</p> <p>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.</p> <p>Note</p> <p>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.</p>

Stream Statistics

The following table lists the Stream statistics:

[General](#) [SRT](#) [SRT Graph](#) [Video/Audio Stream \(Detailed\)](#) [Pro-MPEG FEC](#)

General

Statistic	Description/Values
Stream	
ID	ID number of the stream the statistics describe.
Name	Name of the stream (if provided by the user).
Decoder ID	ID Number of the decoder on which the stream is running. (Possible values are 0 to 3.)
Statistics	
Encapsulation	The Encapsulation Protocol type selected for the decoded stream, including: <ul style="list-style-type: none"> • TS over UDP • TS over RTP • TS over SRT
State	The current operating status of the stream. Possible values are: <ul style="list-style-type: none"> • STOPPED: Stream is currently stopped by the user. • LISTENING: Stream has been started by the user, but no data is currently being received. • ACTIVE: Stream is actively flowing into the decoder system. • UNLICENSED: The stream contains features that are not permitted by the current license set. This can include TS-SRT (although licensing will prevent the creation of SRT streams, so this protection may not trigger). • RESOLVING: For TS-SRT only, a FQDN host address is currently resolving. • CONNECTING: For TS-SRT and TS-RTP with FEC only, a connection is in the process of being established. • SCRAMBLED: For TS-SRT, stream is scrambled and cannot be decoded. I think this one may be deprecated in the SRT library in favor of stricter encryption to prevent a possible denial-of-service attack. • SECURING: For TS-SRT, encrypted but keying material not ready (wrong secret?) • FAILED: For TS-SRT and TS-RTP with FEC only, the streaming connection attempt failed.
Source Address	IP address and port of the remote streaming source (sender). For example, 10.66.131.62 port 37435 .
Bit Rate	Measured rate of data transfer that is being received in the stream (in kbps).
Connections	The number of times the streaming module attempted to connect to the stream. For example, 2 (Last: 19h57m54sec ago)
Received Packets	Total number of packets that have been received and processed. In parenthesis is how long ago the last one was received, e.g. "(Last One: 0s ago)".
Received Bytes	Total number of bytes that have been received and processed.
Last Received	How long ago the last packet was received.
Output Packets	Total number of packets that were output by the streamer into the decoder. In parenthesis is how long ago the last one was sent, e.g. "(Last One: 0s ago)".

Output Bytes	Total number of bytes that have been output by the streamer into the decoder.
Program Number	For MPEGTS streaming protocols only, the Program Number of the stream.
PCR PID	For MPEGTS streaming protocols only, the PID of the Program Clock Reference.
Stream Summary	A summary of the streams that have been recognized. This includes: <ul style="list-style-type: none"> • Video - H.264 or HEVC video streams (possible values are 0 or 1) • Audio - recognized audio streams (possible values are from 0 to 8) • KLV - recognized KLV streams (possible values are 0 or 1) • Filtered - When PID filtering is used, the number of streams that were rejected because of the filter. Video, Audio and KLV could all be filtered and counted here.
Errors	
Unlicensed Packets	When present, the number of packets that were flagged as UNLICENSED (See “State” description above).
Dropped Packets	When present, the number of packets that were dropped. A packet could be dropped for various reasons, including: <ul style="list-style-type: none"> • Corrupted frame • PID filtering (not supported in 1.0) • Demuxing error
Dropped Bytes	When present, the number of bytes that were dropped, corresponding to “Dropped Packets”.
Last PID Dropped	When present, the MPEGTS PID number of the last packet that was dropped.
Errors	When present, the number of errors encountered in the streaming module. Also includes when the last one occurred.
Last Error	The most recently encountered error with a brief description.
Corrupted Frames	When present, the number of frames that had missing or bad MPEGTS continuity counters.
Timestamp Rollovers	When present, the number of times the timestamp “rolled over” from a high value to a much lower value.
PES Size Mismatches	When present, the number of times the PES Size Mismatch error occurred.
New Stream Flags	The number of times the decoder’s stream ID was switched without restarting.
Resumed Stream Flags	The number of times a break in the stream was detected. For example, a resumed stream would be detected if the encoder stream were stopped and then started again.
PCR PID	For MPEGTS streaming protocols only, the PID of the Program Clock Reference.
Reset	Click to reset the Stream statistics.

[General](#)
[SRT](#)
[SRT Graph](#)
[Video/Audio Stream \(Detailed\)](#)
[Pro-MPEG FEC](#)

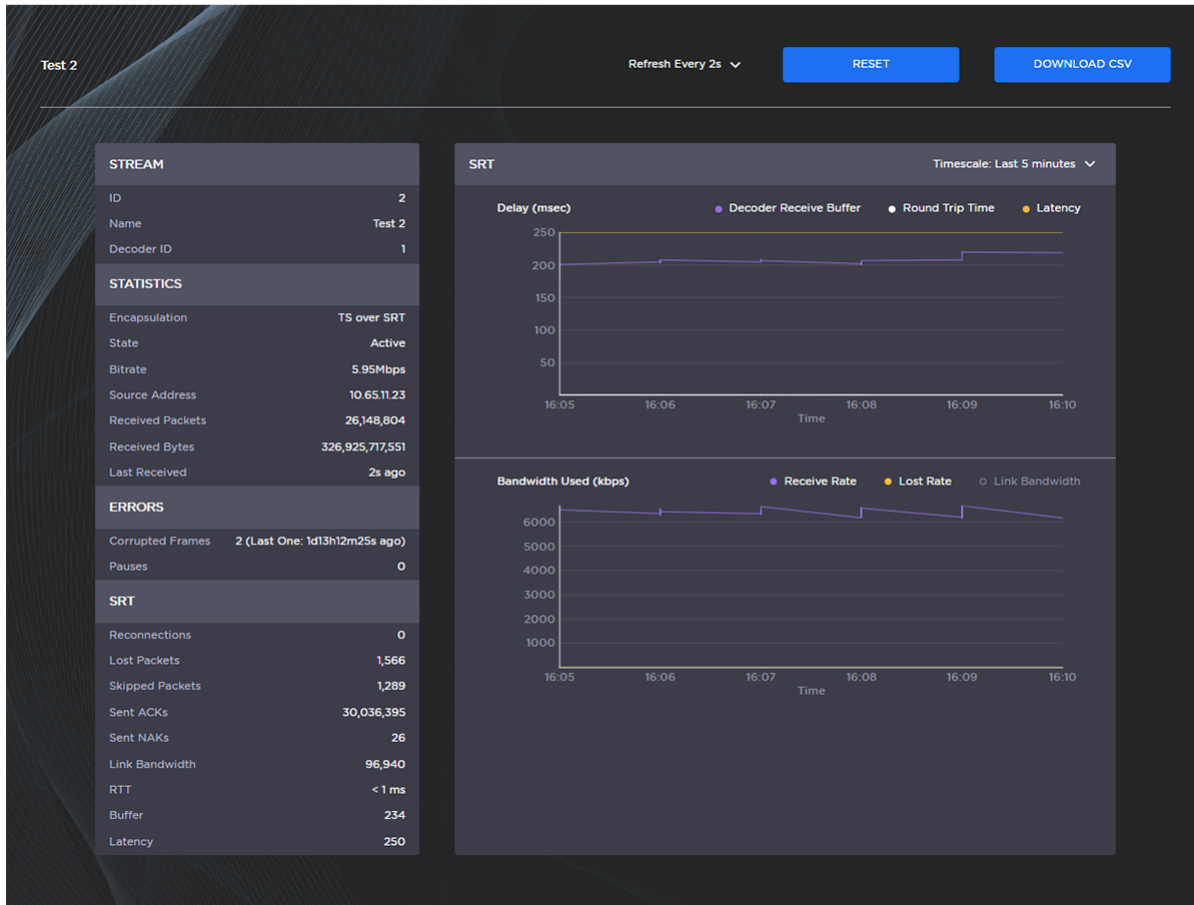
SRT Statistics

Statistic	Description/Values
Local Version	Version of the SRT Library implementation on the decoder.
Peer Version	Version of the SRT Library implementation on the remote streamer.

Statistic	Description/Values
Connections	Number of connection attempts. Severe network congestion may cause the connection to drop and automatically reconnect.
Local Port	Port number being used on the decoder.
Remote Port	Port number being used on the remote streamer.
AES Encryption	Indicates whether AES encryption has been enabled. Either On or Off.
Key Length	(AES encryption must be enabled) The key length for AES encryption. Either None, AES-128 or AES-256.
Decryption	(AES encryption must be enabled) Indicates whether the decoder can decrypt the stream/State of the decryption. Possible values are: <ul style="list-style-type: none"> Active Initializing Inactive (no passphrase) Inactive (invalid passphrase)
Lost Packets	<p>Note</p> <p>This is the raw number of packets dropped by the network. Most are recovered by retransmission at the source and so do not necessarily result in any artifacts.</p>
Dropped Packets	The number of SRT packets that were ultimately dropped. These are packets that have arrived at the destination device too late, or that never arrive at all. The time to play the packet has arrived and the lost packet was not recovered, so the decoder/receiver will continue playing. Some type of video artifact may result (i.e., a replayed frame or video blocking artifacts).
Dropped Bytes	The number of bytes corresponding to “Dropped Packets”.
Sent ACKs	Transmission progress acknowledgment and feedback sent.
Sent NAKs	Lost packet reports sent.
Link Bandwidth	An estimate of the actual link bandwidth.
RTT	Measured Round Trip Time.
Local Buffer Level	SRT decoder buffers are the received stream packets waiting to be decoded. This statistic shows the portion of the decoder buffers up to the first missing packet. In other words, the remaining time to transmit the missing packet before it's too late. The level of the decoder buffer in absence of packet lost is just below the latency value. In presence of packets lost, it is between 0 and the latency value.
Latency	Maximum of the decoder and encoder configured Latency. For example: <ul style="list-style-type: none"> Encoder Configured SRT Latency = 750 ms Decoder Configured SRT Latency = 20 ms The SRT Stats Latency (which is the current SRT connection applied Buffering Latency) = 750 (largest of the two). At startup, handshake exchanges the value configured on both sides, and the largest one is selected.

SRT Graph

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



Note

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

Tip

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

Video Stream/Audio Stream# (Detailed)

Statistic	Description/Values
Compression	The name of the compression standard used for the media. <ul style="list-style-type: none"> For video, it could be H.264 or H.265. For audio, it could be AAC-ADTS, AAC-LATM, MP1, MP2 or MP3. For KLV, it will be UNCOMPRESSED.
Bit Rate	The measured average bit rate of the elementary stream.
Program ID	In the MPEG2 Transport Stream, this is the Program ID (PID) of that elementary stream.
Received Packets	The number of packets received for this elementary stream.
Received Bytes	The number of bytes received for this elementary stream.
PTS	The most recently encountered Presentation Time Stamp in this elementary stream.
DTS	The most recently encountered Decode Time Stamp in this elementary stream.

Pro-MPEG FEC

Statistic	Description/Values
Level	The level of FEC protection: <ul style="list-style-type: none"> A (Column only): uses the column FEC stream. B (Row and Column): uses both column and row FEC streams.
Number of Columns/Rows	The number of columns and rows in the FEC matrix.
Block Aligned	The type of FEC matrix scheme: <ul style="list-style-type: none"> Yes: Sequential columns within a group start on the same row. No: Each column starts on the row below the row on which the previous column started.
Dropped Packets	The number of packets that were detected as missing by FEC.
Recovered Packets	The number of packets that were recovered by FEC. Tracking Mode
Lost Packets	The number of packets that could not be recovered by FEC.

System Administration

Note

Unless otherwise indicated, the Administration Settings pages are only accessible to administrators. The exceptions are as follows:

- Status is accessible to all users.
- Presets is accessible to Operators as well as Administrators.

Topics in This Chapter

- [Viewing System Status Information](#)
- [Saving and Loading Presets](#)
- [Installing Firmware Upgrades](#)
- [Configuring Network Settings](#)
- [Configuring Date and Time](#)
- [Enabling and Disabling Network Services](#)
- [Managing Licenses](#)

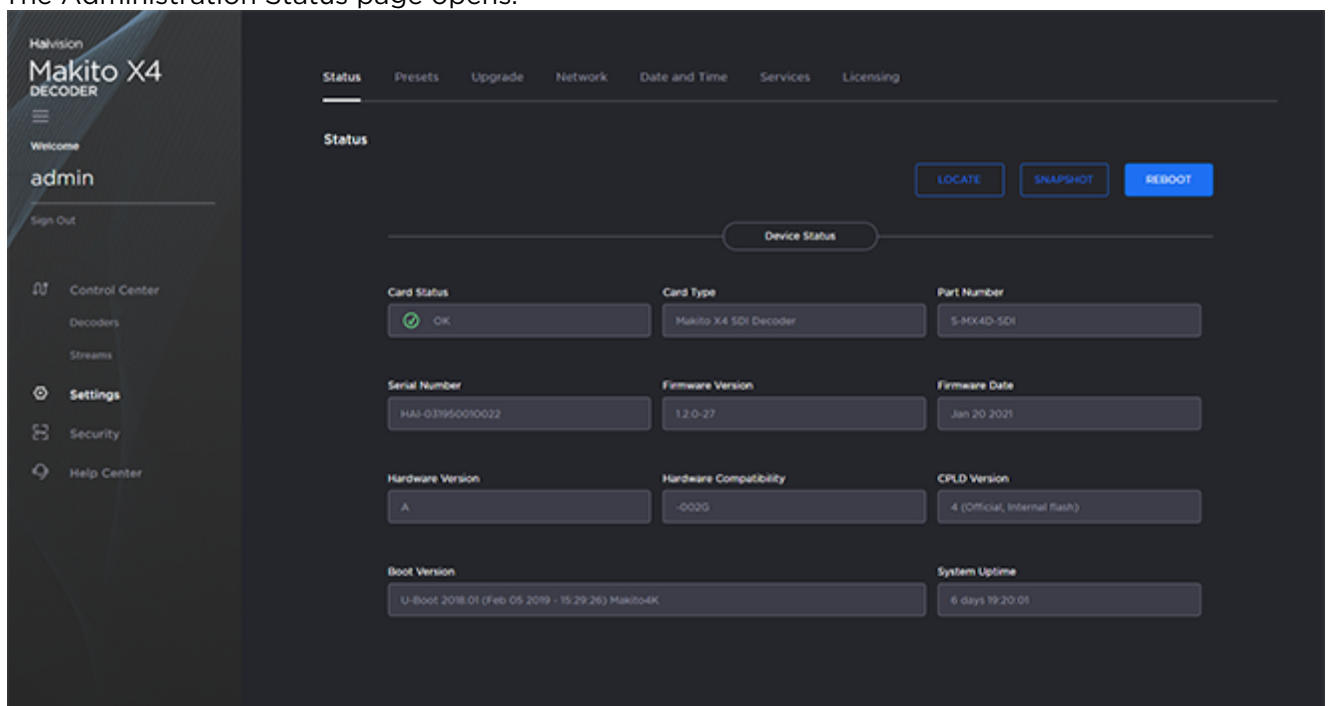
Viewing System Status Information

From the Status page, you can view status information about the Makito X4 decoder, such as the operating system uptime, along with information about the hardware and software components. You can also initiate blinking of the Status and TX LEDs (to help locate particular decoders in a lab or rack), as well as take a system snapshot and reboot the decoder.

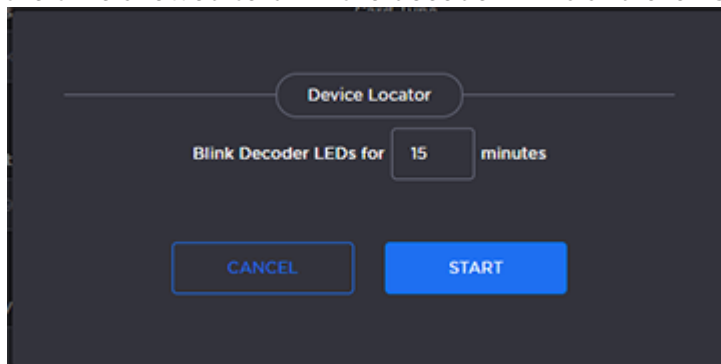
The Status page is available to Operator and Guest users as well as Administrators.

To view status information:

1. Click **Settings** on the side menu.
The Administration Status page opens.



2. The Status settings are read-only. For details, see [Status Settings](#).
3. To display a snapshot of system information, see [Taking a System Snapshot](#).
4. To initiate blinking of the Status and TX LEDs, click **Locate**. On the Device Locator dialog, adjust the time allowed to blink the decoder LEDs and click **Start**.



Note

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

- To reboot the decoder, see [Rebooting the Decoder](#).

Status Settings

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

Status Setting	Description/Values
Personality	Select between SDI, SQD (version 1.6 and later), DEFENSE (version 1.7 and later) and SMPTE 2110 (version 1.4 and later). This setting will take effect upon the next reboot.
Card Status	OK (or error message if applicable).
Card Type	The type of device, e.g., Makito X4 SDI Encoder.
Part Number	The Haivision part number for the encoder or decoder, e.g., B-MX4E-SDI4 or S-MX4D-SDI.
Serial Number	The serial number for this appliance or card.
Firmware Version	The firmware version of the device, e.g., 1.0.0-23.
Firmware Date	The firmware release date.
Hardware Version	The hardware version of the device.
Hardware Compatibility	-001G or -002G (basic card assembly).
Carrier Type	(Makito X4 Rugged Encoder only) The interface carrier board. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>In Release 1.2, the number of CVBS inputs supported depends on the Carrier Type. "Makito 4KR" indicates the three-input variant, whereas "Makito 4KR 12G" indicates the four-input variant.</p> </div>
CPLD Version	The CPLD version of the device.
Boot Version	The Boot version of the device.
System Uptime	The length of time the encoder or decoder has been "up" and running (e.g., 4 days 17:42:03).
Encoding Chipset Load	(Encoder only) The combined video encoding processor usage in percentage% (combining both Hi and Lo streams).
Temperature	The current board temperature in degrees Celsius.

Rebooting the Decoder

To reboot the decoder:

1. Click **Settings** on the side menu.
2. On the Status page, click **Reboot**.



Tip

You can also reboot the decoder from the Network Settings page. See [Configuring Network Settings](#).

Taking a System Snapshot

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

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

To take a system snapshot:

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

following example:

```

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

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

Local Time:
-----
Thu Jun  4 16:41:13 EDT 2020
-----

Universal Time:
-----
Thu Jun  4 20:41:13 UTC 2020
-----

System UP Time:
-----
16:41:13 up  3:09,  1 user,  load average: 1.43, 1.42, 1.44
-----

Manufacturing Information:
-----
MAC Address   : 5c:77:57:00:e0:be
Serial Number : HAI-031950010016
Boot Revision : U-Boot 2018.01 (May 28 2020 - 19:11:18 -0400) Xilinx ZynqMP MakitoX4D
-----

Card Temperature:
-----

Temperature Status:
  Current Temperature   : 35 Celsius measured 1s ago
  Maximum Temperature  : 35 Celsius measured 3h8m35s ago
  Minimum Temperature  : 34 Celsius measured 3h8m41s ago
Debug Statistics:
  Invalid Readings     : 0
  Discarded Deltas    : 0
-----

System Information:
-----
Card Type           : "Makito X4 SDI Decoder"
Part Number         : S-MX4D-SDI
Serial Number       : HAI-031950010016
MAC Address         : 5c:77:57:00:e0:be
Firmware Version    : 1.0.0-34
Firmware Date       : "Jun  4 2020"
Firmware Time       : "11:36:11"
Hardware Version    : A
Hardware Compatibility : -002G
CPLD Version        : 4 (Official, Internal flash)
Boot Version        : "U-Boot 2018.01 (Feb 05 2019 - 15:29:26) Makito4K"
-----

Installed Debian Packages:
-----
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version          Description
+---+

```

2. Save the file.

 **Tip**

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

Saving and Loading Presets

Each Makito X Series device is configured by users' selecting and setting values of applicable encoder or decoder settings, such as Video and Audio Encoder, Streaming Output, and (if licensed) Metadata settings; or Decoder Output and Stream settings. Presets provide a way for you to save groups of settings and recall these configurations settings to apply to other streams.

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

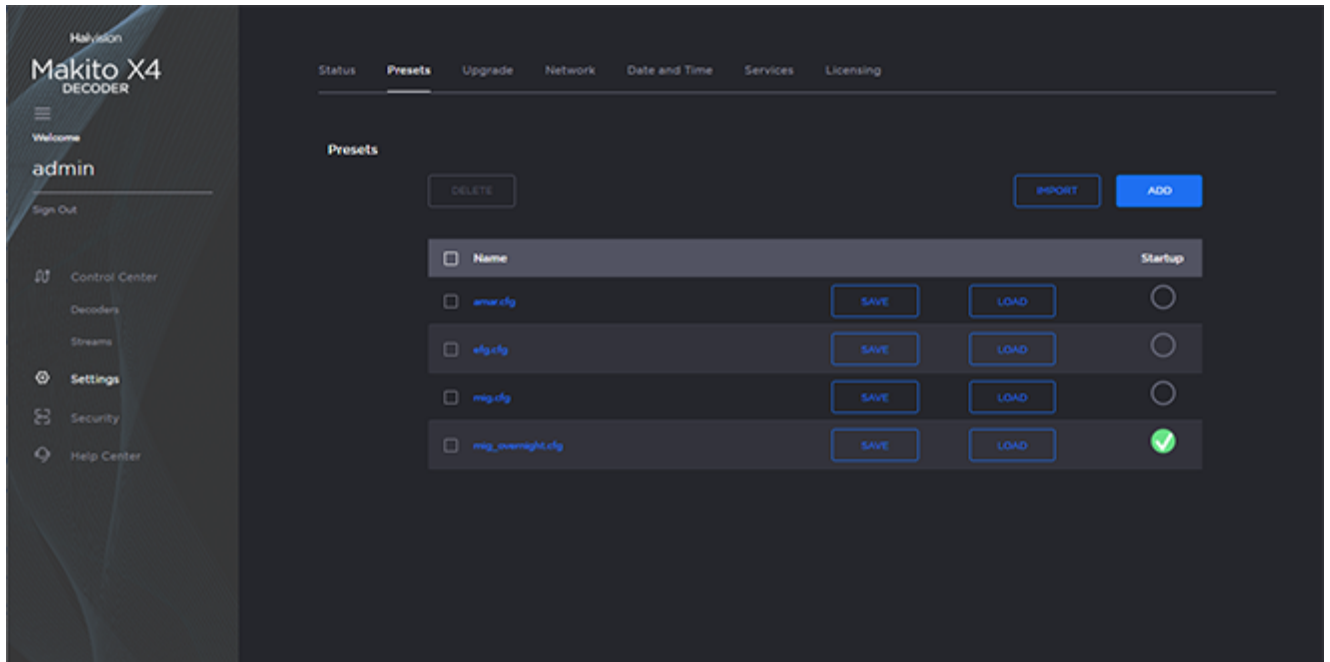
 **Note**

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

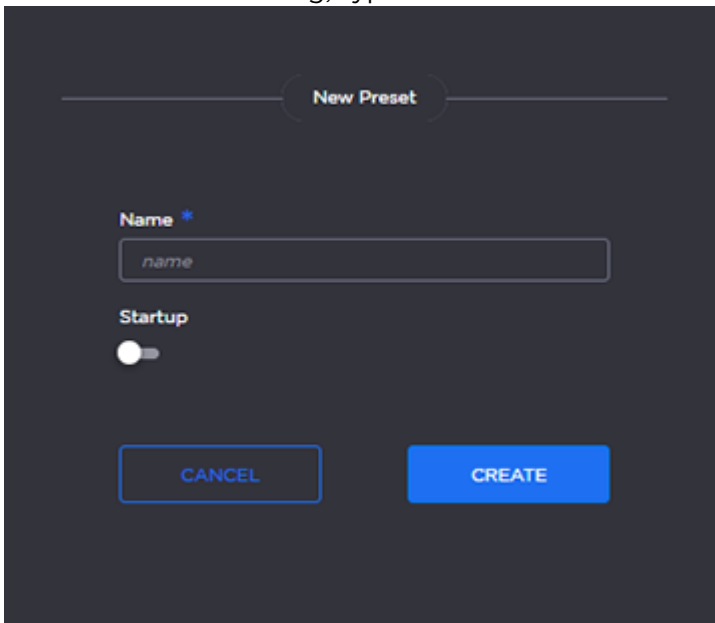
The Preset Manager displays a list of saved presets. From here you can load, rename, duplicate, or delete a saved preset, as well as view the contents of a preset file and select a preset to load at startup.

To view and manage presets:

1. Click **Settings** on the side menu and **Presets** on the navigation bar.
The Presets page opens displaying the list of saved presets for the decoder. The startup preset is indicated with a green check mark.

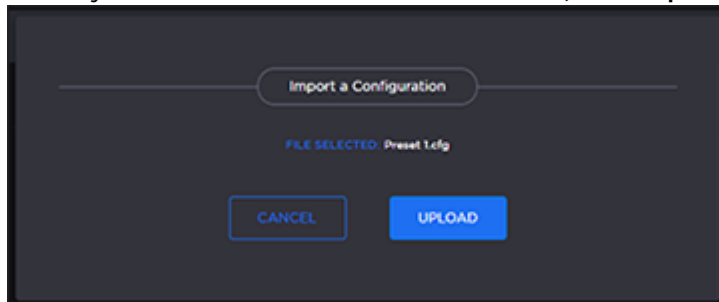


2. To load an existing preset into the current session, hover over the preset name or anywhere in the row and click **Load**.
3. To select an existing preset to load at startup, hover over the preset row and click the (empty) circle under **Startup**.
4. To save the current settings as a new preset, click **Add**.
 - a. In the New Preset dialog, type a new filename in the Name text box.



- b. To select this preset to load at startup, turn on the **Startup** toggle.
 - c. Click **Create**.
5. To save the current settings as an existing preset, hover over the preset row and click **Save**. You can (optionally) select **Startup**.
6. To import a preset, for example, from another Makito X4 decoder, click **Import** and drag the preset file to the drop area or click **Browse** or **Choose a file** to select the file.

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



✓ **Tip**

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

i **Note**

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

Installing Firmware Upgrades

Note

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

When you first receive 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.

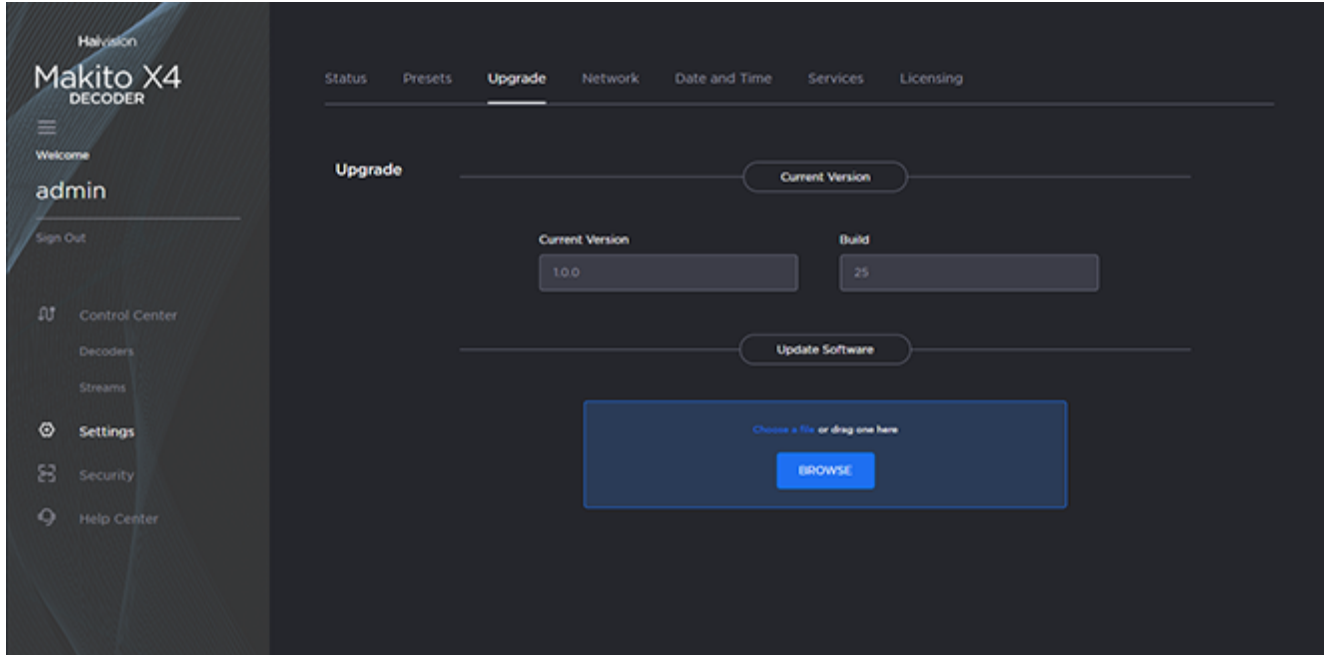
This section provides instructions to install a firmware upgrade from the Web interface.

Tip

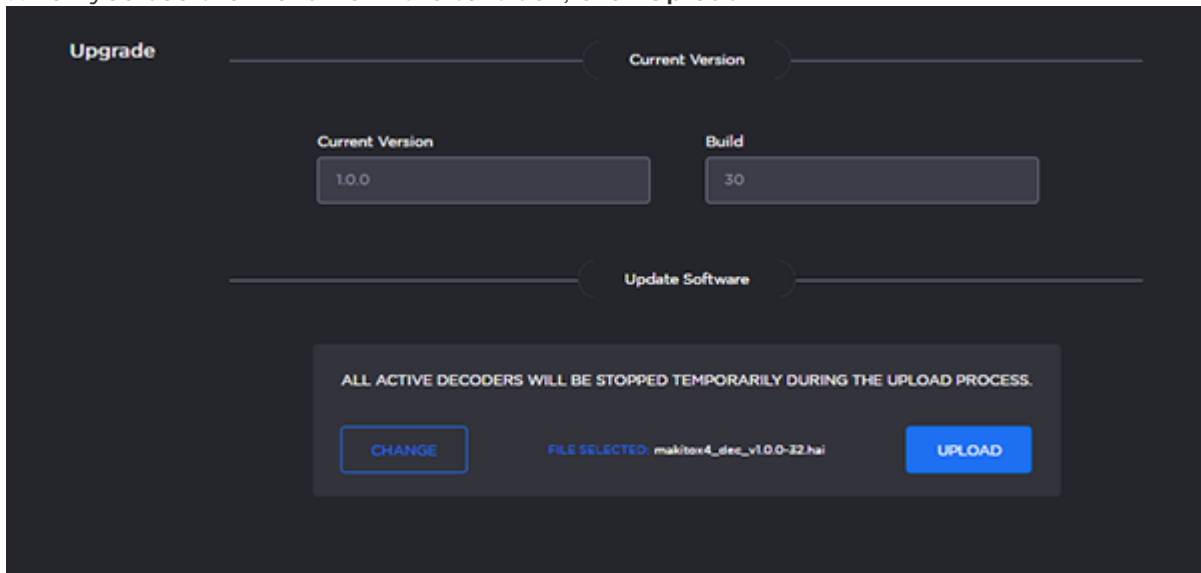
Do not delete existing licenses before uploading the new license when upgrading to a new release.

To install a firmware upgrade:

1. Click **Settings** on the side menu and **Upgrade** on the navigation bar. The Upgrade page opens.



2. Drag the upgrade file to the drop area or click **Browse** or **Choose a file** to select the file.
3. When you see the filename in the text box, click **Upload**.



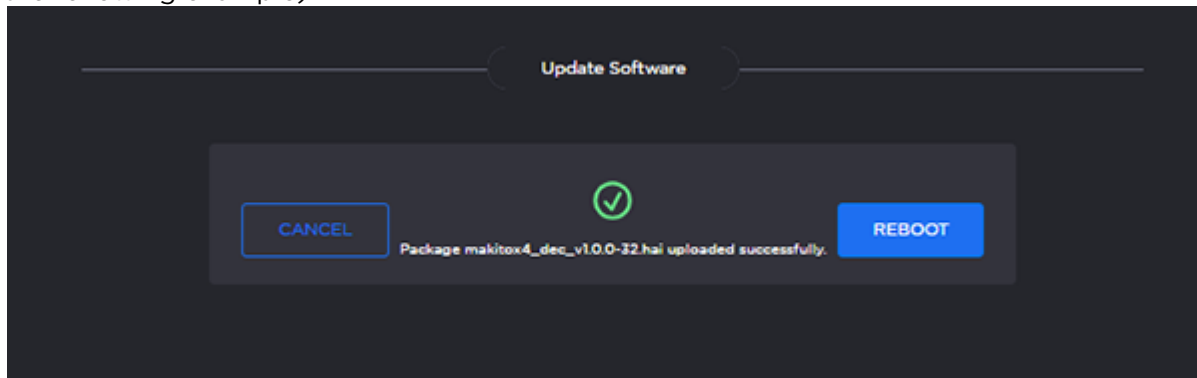
4. Wait for the file to be uploaded and verified and the file system synced.

! Important

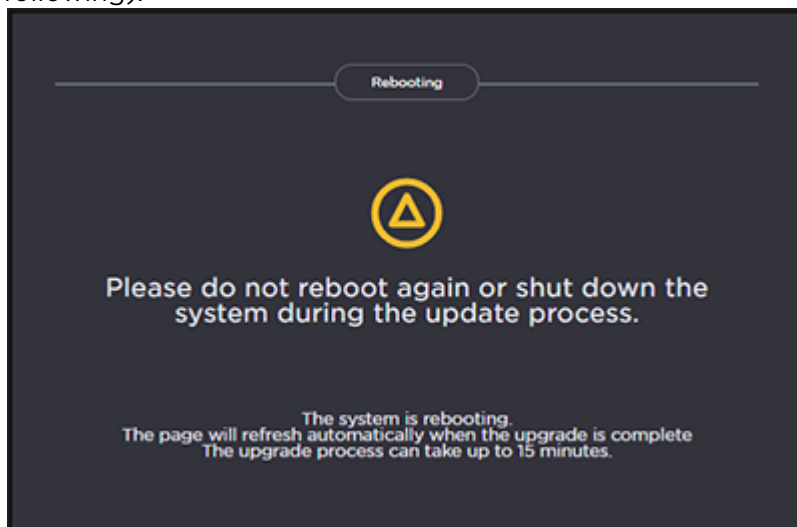
Remain on this page and do not click anything else in the Makito X4 Web interface during the upload.

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

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



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



Caution

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

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

- Clear your browser cache after the firmware upgrade.
- Sign in again in order to access the decoder. For more information, see [Signing In to the Web Interface](#).

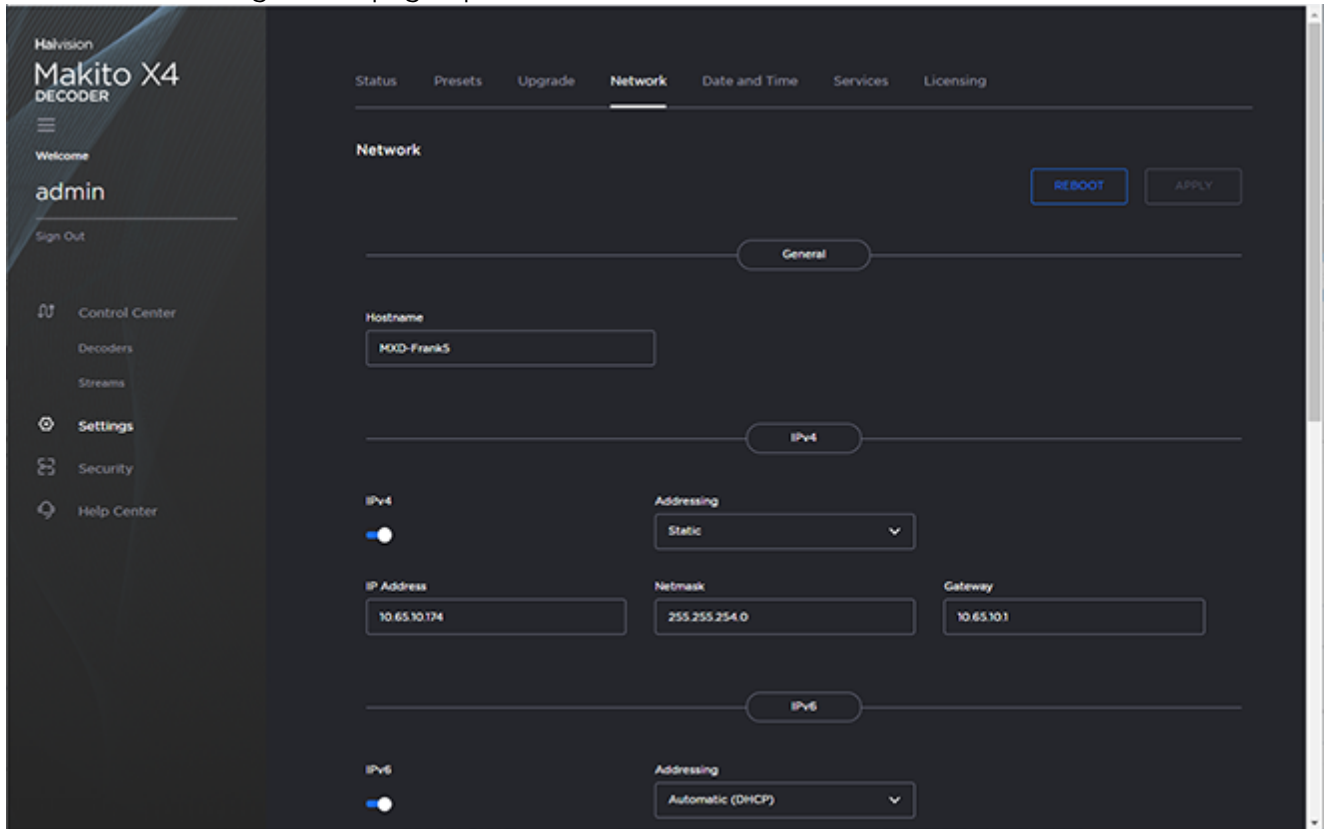
Configuring Network Settings

Caution

When you make changes to the Network settings, be sure to write down the new decoder IP Address or label the chassis. After you apply your changes and reboot, you will have to redirect the browser to the new IP address and sign in again in order to access the decoder. If you are connecting to the decoder 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:

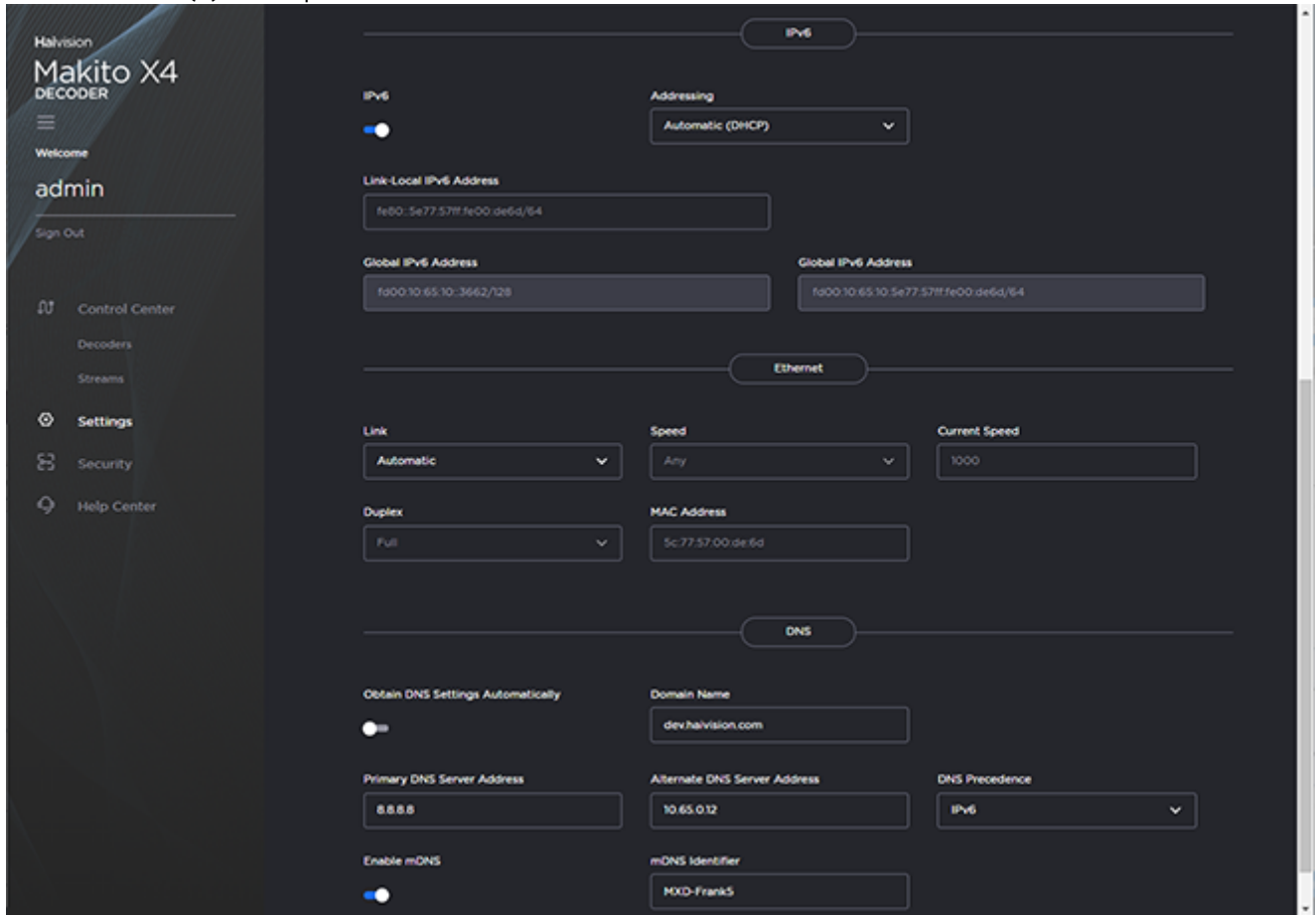
1. Click **Settings** on the side menu and **Network** on the navigation bar. The Network Configuration page opens.



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

IPv6:

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



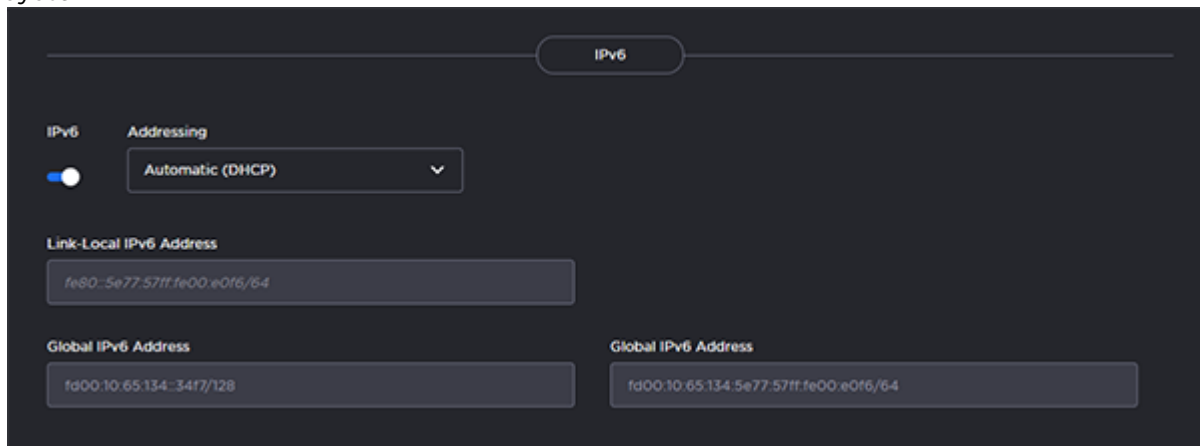
- Click **Apply**.
- Click **Reboot**.

Note

You must reboot the system for the changes to take effect.

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

system.



Network Settings

The following table lists the Decoder Network settings:

[General](#) [IPv4](#) [IPv6](#) [Ethernet](#) [DNS Settings](#)

General

Network Setting	Description/Values
Hostname	Enter a unique name for the Makito X4 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.

[General](#) [IPv4](#) [IPv6](#) [Ethernet](#) [DNS Settings](#)

IPv4

Network Setting	Description/Values
Addressing	<div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>When DHCP is enabled, the Makito X4 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.</p> </div>
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 X4 devices on their networks. The default Device Identification value is "Haivision Makito X4 Decoder".
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 X4 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 X4. 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 X4. 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.

Network Setting	Description/Values
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.

General IPv4 IPv6 Ethernet DNS Settings

IPv6

Network Setting	Description/Values
Addressing	Select one of the following options to obtain an IPv6 address for the unit: <ul style="list-style-type: none"> • 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 X4. 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.

General IPv4 IPv6 Ethernet DNS Settings

Ethernet


Network Setting	Description/Values
Link	Determines whether the Ethernet link settings will be negotiated automatically or configured manually: <ul style="list-style-type: none"> • 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.

Network Setting	Description/Values
Speed	<p>Select the Ethernet Speed (in Mbps):</p> <ul style="list-style-type: none"> • Any (default) • 1000 • 100 • 10 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>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.</p> </div>
Current Speed	(Read-only) Displays the actual Ethernet Speed.
Duplex	<p>If Link is Auto, displays the actual value for the Duplex Mode (read-only).</p> <p>If Link is Manual, select the Duplex Mode:</p> <ul style="list-style-type: none"> • Full • Half
MAC Address	(Read-only) The Media Access Control address assigned to the Makito X4.

General IPv4 IPv6 Ethernet DNS Settings

DNS Settings

Network Setting	Description/Values
Domain Name	Enter the domain for the Makito X4.
Obtain DNS Settings Automatically	<p>(Addressing cannot be Static) Check this checkbox to obtain DNS settings from DHCP.</p> <p>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).</p>
Primary DNS Server Address	(Obtain DNS Settings Automatically must be disabled) Enter the primary DNS server address for your network.
Alternate DNS Server Address	<p>(Obtain DNS Settings Automatically must be disabled) Enter an alternate DNS server address for your network.</p> <p>The alternate DNS server is used only if the primary server is not responding.</p>
DNS Precedence	<p>Select either IPv4 or IPv6 to specify the priority for DNS resolution.</p> <p>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.</p>

Network Setting	Description/Values
Enable mDNS	<div style="border: 1px solid #c8e6c9; padding: 10px;"> <p> Tip</p> <p>Enabling mDNS allows an mDNS application to automatically find the Makito X4. mDNS is enabled on units shipped from the factory or reset to factory defaults to allow them to advertise their existence. A user can then click Locate (Status page) to start the Status and TX or RX LEDs flashing in order to discover the location of the device, for example, within a large server room.</p> </div>
mDNS Identifier	(Optional) Enter a unique name for the Makito X4. By default, the system creates a unique name “MakitoXD (%HOSTNAME%)” for the device.

Related Topics

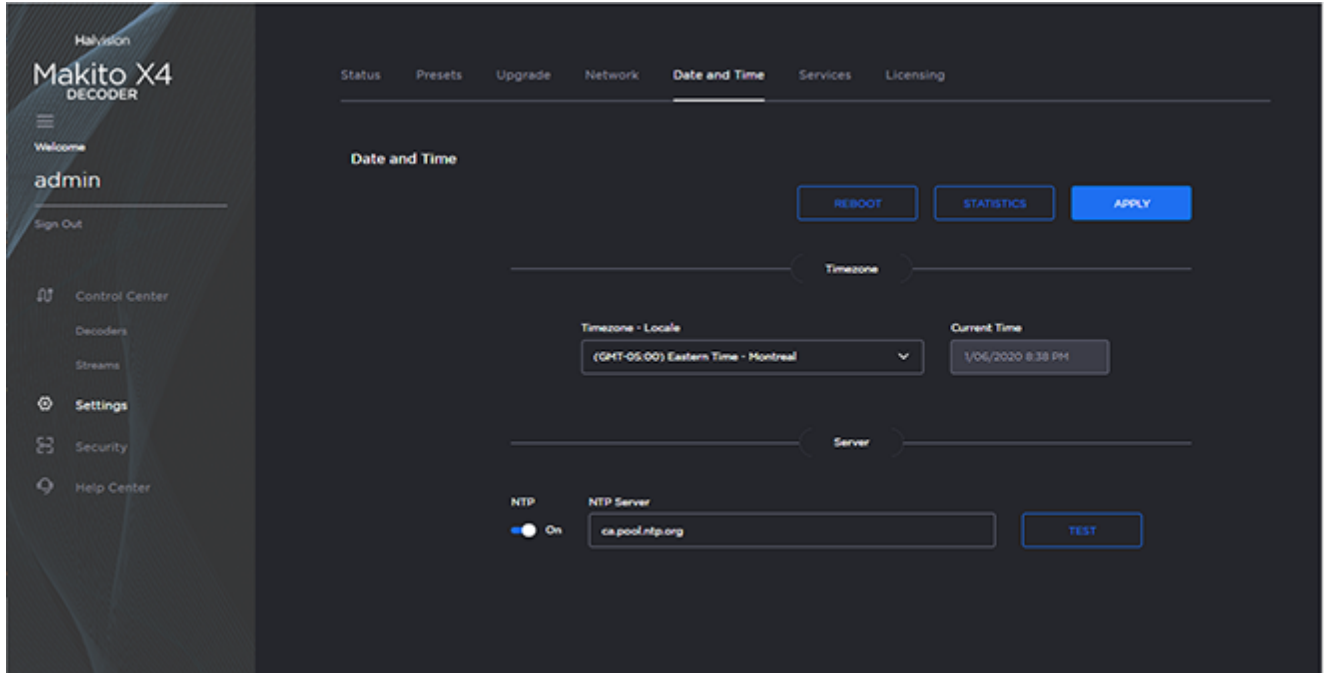
- [Configuring Network Settings](#)
- [Viewing System Status Information](#)

Configuring Date and Time

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

To view and configure the date and time:

1. Click **Settings** on the side menu and **Date and Time** on the navigation bar. The Date and Time page opens.



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

Topics Discussed

- [Date and Time Settings](#)
- [NTP Statistics](#)

Date and Time Settings

The following table lists the Date and Time settings:

Date and Time Setting	Description/Values
Timezone	
Time Zone	Select the desired time zone and corresponding city. <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> ⚠ Note The times are based on hours added to or subtracted from Greenwich Mean Time (GMT). </div>
Current Time	(Read-only) The current local date and time.
Server	
Use NTP	Toggle on to connect to a Network Time Protocol (NTP) server to synchronize the encoder or decoder clock.
NTP Server	If NTP is enabled, enter the IP address of the NTP server.
Manually Set Date & Time	If NTP is disabled, select the date and time from the calendar.
Test	If NTP is enabled, click to validate that the NTP server is reachable.
Statistics	If NTP is enabled, click to display tracking and source information, and source statistics for the NTP server.
Reboot	If changes have been made to the date and time settings, click to apply changes.

Related Topics

- [NTP Statistics](#)

NTP Statistics

Following is an example of the NTP Statistics:

NTP Statistics

Tracking

```

Reference ID      : 8AC599C8 (138.197.153.200)
Stratum          : 3
Ref time (UTC)   : Fri Jul 30 22:41:22 2021
System time      : 0.000091164 seconds slow of NTP time
Last offset      : -0.000022530 seconds
RMS offset       : 0.000043131 seconds
Frequency        : 13.079 ppm slow
Residual freq    : -0.000 ppm
Skew             : 0.017 ppm
Root delay       : 0.008856932 seconds
Root dispersion  : 0.000857683 seconds
Update interval  : 1027.7 seconds
Leap status      : Normal
    
```

Sources

210 Number of sources = 4

MS Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
A* 138.197.153.200	2	10	377	767	-294us[-317us] +/- 4505us
A- 216.6.2.70	2	10	377	31	+222ns[+222ns] +/- 66ms
A+ 162.159.200.1	3	10	377	577	+393us[+393us] +/- 8893us
A- 216.232.132.102	1	10	377	999	+191us[+169us] +/- 234ms

Source Stats

210 Number of sources = 4

Name/IP Address	NP	NR	Span	Frequency	Freq skew	offset	Std Dev
138.197.153.200	12	10	190m	+0.001	0.031	-214us	71us
216.6.2.70	6	5	86m	+0.015	0.064	-16us	33us
162.159.200.1	12	8	207m	-0.002	0.015	+414us	46us
216.232.132.102	9	6	137m	+0.005	0.020	+68us	29us

CLOSE

Enabling and Disabling Network Services

For security purposes, an administrator may need to stop one or more network services from accessing the Makito X4 decoder. From the Services page, you can enable and disable network services, including HTTP, SSH, Telnet, and SNMP. You can also enable or disable Haivision EMS as well as the Control Center Thumbnail Previews.

! Important

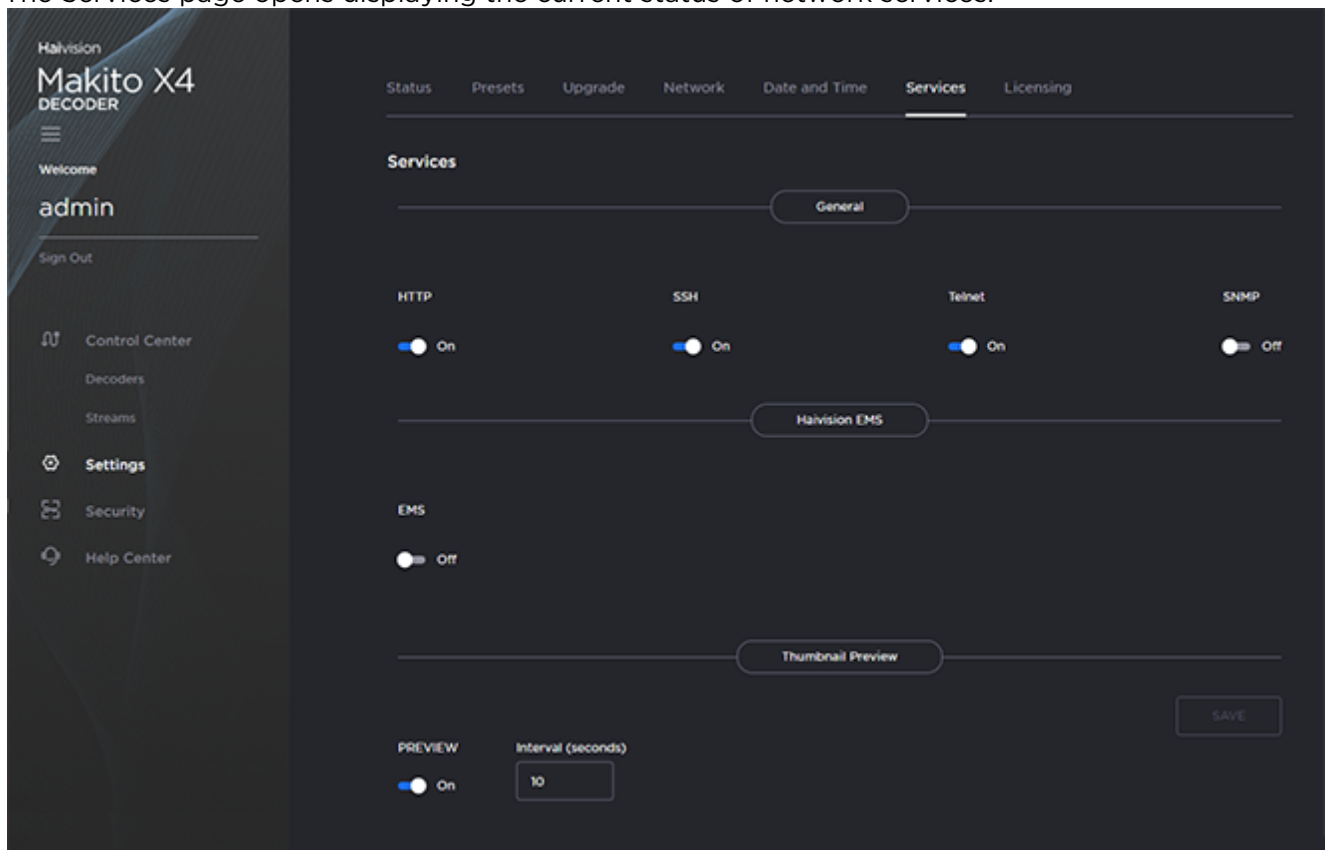
In order to optimize your decoder's performance, it is recommended that *only* the required network services be enabled. Please review the network services to make sure services used for your application are enabled or disabled as appropriate.

⚠ 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 Decoder](#)).

To enable or disable network services:

1. Click **Settings** on the side menu and **Services** on the navigation bar. The Services page opens displaying the current status of network services.



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

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





Tip

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

Services Settings

The configurable decoder Services are as follows:

Network Services

Service	Description/Values
General	
HTTP	Hypertext Transfer Protocol, used for Web browsers acting as a client. <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 5px;">  Note Only secured HTTP (HTTPS) is supported. </div>
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.
Haivision EMS	
EMS	Toggle to On to enable Haivision EMS.
Thumbnail Preview	
Preview	Toggle to On to enable Control Center Thumbnail Previews.
Interval	Enter the Preview capture interval in seconds and click Save . 1...600 (default is 10 seconds) <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 5px;">  Note A lower interval may affect performance. We recommend that you verify that the chosen value does not affect your system performance. The Preview settings will continue to be used after a reboot, or when the unit is turned off and on. </div>

Related Topics

- [Pairing the Decoder with Haivision EMS](#)
- [Managing Certificates](#) (to manage HTTP TLS certificates)

Pairing the Decoder 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 X4 decoder and then pair the decoder with Haivision-EMS. This allows the EMS to communicate with the decoder, for example, to monitor the connection status.

To manage a Makito X4 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 X4 devices you wish to pair.

To pair the Makito X4 decoder with Haivision-EMS:

1. On the Services page, toggle the **EMS** button to **On** .
The EMS settings now appear:

The screenshot displays the 'Haivision EMS' configuration screen. At the top, there is a 'Passcode (Copy from Haivision EMS)' input field. Below this, the settings are organized into four columns: 'Connection Status' (showing 'Unpaired' with a blue square icon), 'EMS Address' (containing 'ems.demo.haiv'), 'EMS Port' (containing '8883'), and 'Keep Alive (seconds)' (containing '3'). A prominent blue 'PAIR' button is located on the right side of the interface.

2. Enter the passcode (copied and pasted from Haivision EMS).

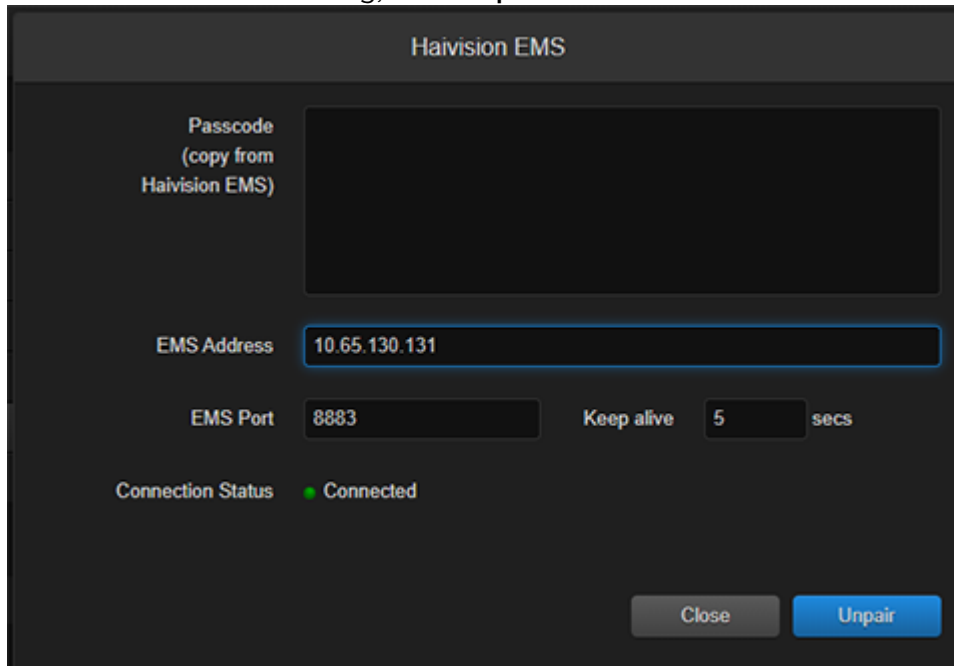
Note

On a new system, the EMS Address and Port are blank. When a pairing code is pasted in, the address and port are automatically filled in to reflect the IP address and port contained in the pairing code.
(Optional) You may change the EMS Address and Port in order to override the defaults extracted from the pairing code, for example, to accommodate network security requirements.

3. (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.
4. Click **Pair**.
This initiates the pairing and communication with the EMS server.

To unpair the Makito X device from Haivision-EMS:

1. On the Haivision EMS dialog, click **Unpair**.



The unpairing takes effect immediately.

Managing Licenses

- [License File Errors](#)

Feature licensing allows you to view the licensed capabilities of your Makito X4 decoder 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.

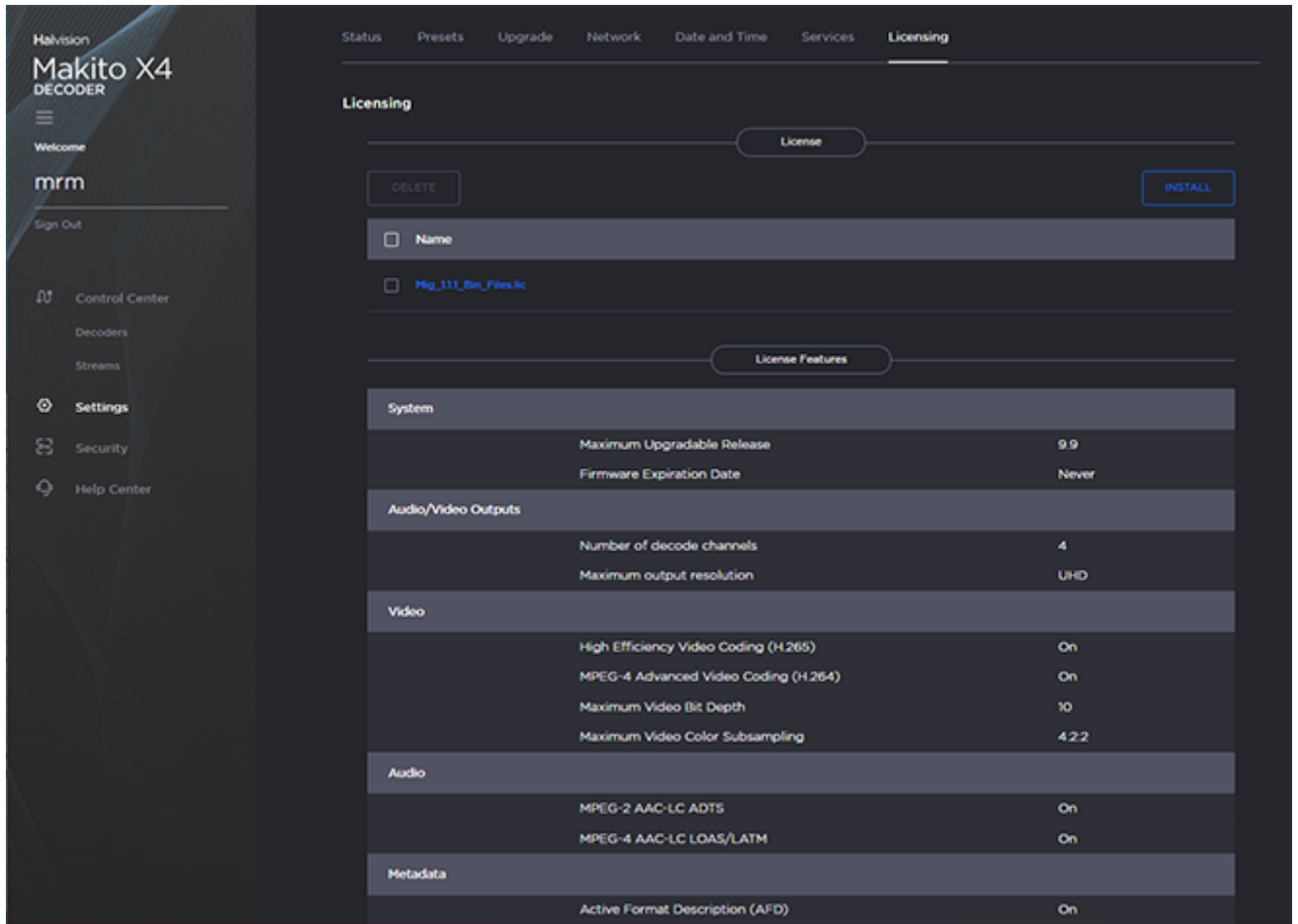
This section provides instructions to install a license from the Web interface as well as view current licenses on your system.

Caution

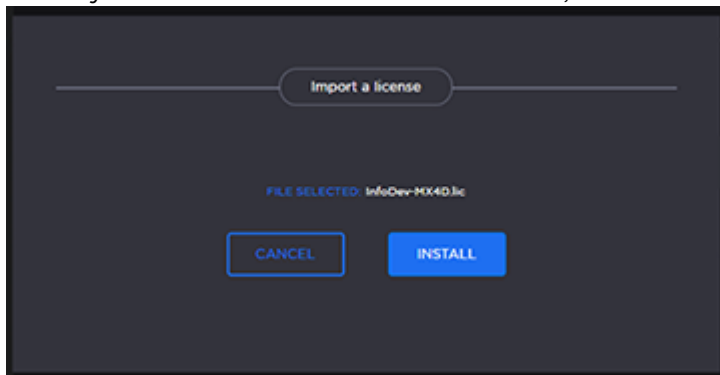
Do not delete existing licenses before uploading the new license. New licenses are typically add-ons to complement the base license. You should only delete existing licenses if *instructed* to do so by Haivision.

To install a license file:

1. Click **Settings** on the side menu and **Licensing** on the navigation bar. The Licensing page opens, displaying the list of currently installed licenses and the associated features, including System, Audio/Video Outputs, Video, Audio, **Metadata**, and Stream capabilities.



2. To select the license file to install, click **Install**.
3. Drag the license file to the drop area or click **Browse** or **Choose a file** to select the file.
4. When you see the filename in the text box, click **Install**.



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

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 Users and Security

Note

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

Topics in This Chapter

- [Managing User Accounts](#)
- [Managing Audits](#)
- [Managing Banners](#)
- [Managing Certificates](#)
- [Managing Messages](#)
- [Managing Security Policies](#)

Managing User Accounts

Note

The Accounts pages are available to administrators only (i.e., users assigned `Administrator` role). From here, administrators can create and manage user accounts for the Makito X4 (including their own accounts).

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

Important

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

From the Accounts pages, administrators can create, delete and modify user accounts for the Makito X4.

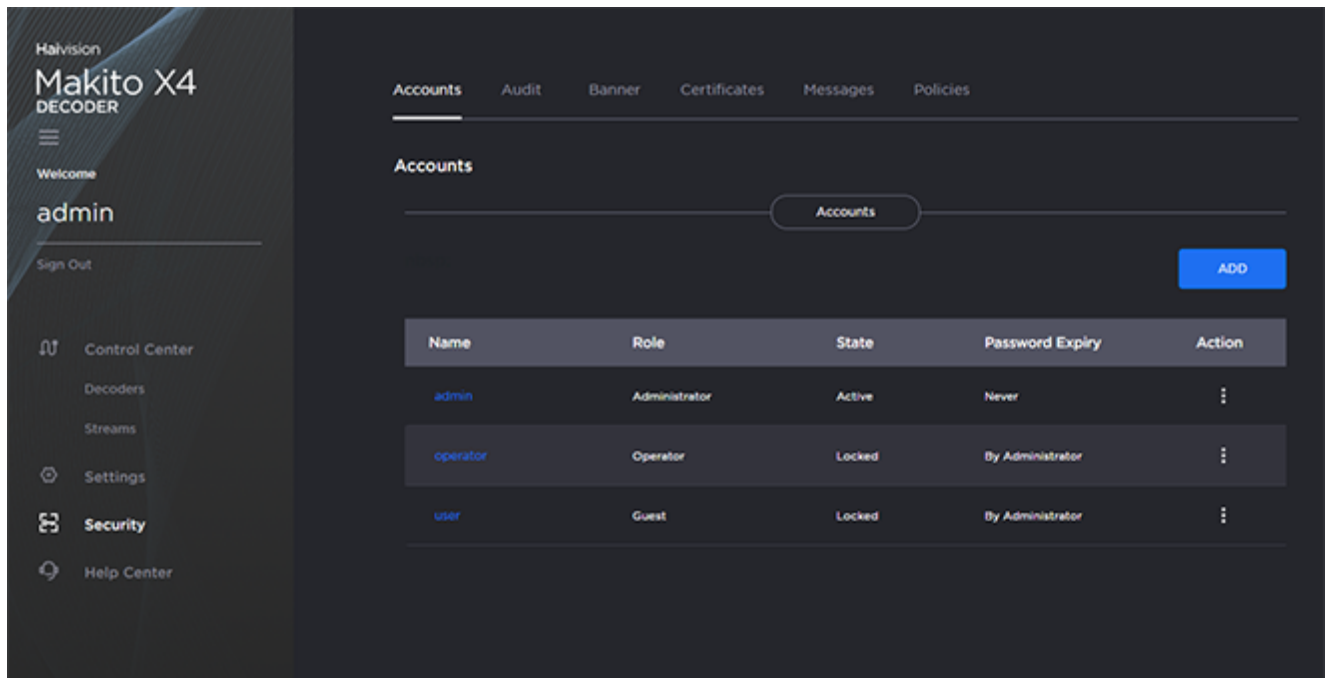
An account can be allocated to each user of the system so that the identity of the user can be uniquely determined. The Makito X4 provides three defined account roles to assign privileges to users: Administrator, Operator and Guest. For details, see [Role-based Authorization](#).

Using system-wide parameters, administrators can configure the allowable password strength and composition (i.e., to force the selection of strong passwords), as well as the periodic change of passwords. The Makito X4 can also be configured for Web interface and CLI account sessions to log out after an idle session timeout period. The session timeout period is selectable via a system-wide parameter. For details, see [Managing Security Policies](#).

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

To open the Accounts List View:

1. Click **Security** on the side menu.
The Accounts List opens, displaying the list of defined user accounts for the decoder, as shown in the following example.



The Accounts List displays the Name, Role, State (Enabled or Locked), and Password Expiry status for each account. It also provides options to lock/unlock or delete an account, as well as re-enable a disabled account.

2. To view or modify user account details, click the account link in the table to open the Account Settings page. For details, see [Account Management](#).
3. To add a new account, click **Add**. For details, see [Account Management](#).
4. To lock, unlock or re-enable an account, click the drop-down list under **Action** and select either:
 - Lock (if the current State is Enabled)
 - Unlock (if the current State is Locked) or
 - Enable (if the account has previously been disabled for inactivity).
5. To apply your changes, click **Apply**.

Tip

To delete an account, click the More Options icon under **Actions** and select Delete.

Topics Discussed

- [Account Management](#)
- [Account Settings](#)
- [Managing Public Key Authentication](#)

Account Management

✓ **Tip**

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

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

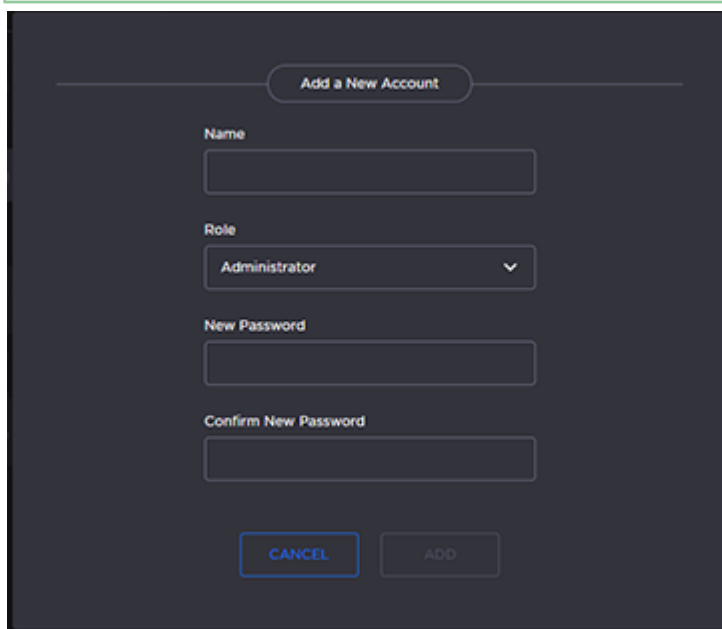
To add a new account:

1. From the Accounts List View, click the **+** **Add** button.

2.

✓ **Tip**

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



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

To manage existing accounts:

1. From the Accounts List View, click a link in the table for an existing account. The Account Settings page opens for the selected account (as shown in the following example).

The screenshot shows the 'Accounts' settings page for an account named 'operator'. The page has a dark theme and a navigation bar at the top with tabs: Accounts, Audit, Banner, Certificates, Messages, and Policies. The 'Accounts' tab is selected. Below the navigation bar is a back arrow and the account name 'operator'. There is an 'APPLY' button on the right. The main content area has three sections: 'Role' with a dropdown menu set to 'Operator', 'New Password' with an empty text input field, and 'Confirm New Password' with another empty text input field. Below these is a section for 'Public Keys' with an 'ADD' button. At the bottom, there is a table header with columns: Name, Fingerprint, and Action.

2. For security purposes, you cannot modify the Name or Role for an existing account.
3. To reset the password of an existing account, type the password in the Password field and again in the Confirmation Password field. For the allowed characters, see "Password Requirements" in [Changing Your Password](#).

4. **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.

5. To upload a public key for the account, follow the steps in [Managing Public Key Authentication](#).
6. To get the fingerprint for a public key, select the public key in the list. For more information, see [Account Settings](#).
7. To apply your changes, click **Apply**.

Account Settings

The following table lists the Accounts controls and settings:

Account Setting	Default	Description/Values
Name	n/a	(Read-only for existing accounts) The user name for the account. (New account) Type in a unique name for the account, meeting the following requirements: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Administrator • Operator • Guest
Old Password	n/a	(Your own account only) Type in your current password. <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>This is not required for other accounts since an administrator is frequently asked to change the password by users who have forgotten their passwords.</p> </div>
Password	n/a	Type in the new password.
Confirmation password	n/a	Re-type the new password.
Public Keys	n/a	Lists any public key files that have been uploaded for this account. <ul style="list-style-type: none"> • To add a public key, click Upload. • To delete a public key, click the More Options icon next it on 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). <div style="border: 1px solid #28a745; padding: 5px; margin-top: 10px;"> <p>Tip</p> <p>A public key fingerprint is a short sequence of bytes which you can copy and use to identify or look for a public key.</p> </div>

Related Topics

- [Role-based Authorization](#)
- "Password Requirements" in [Changing Your Password](#)

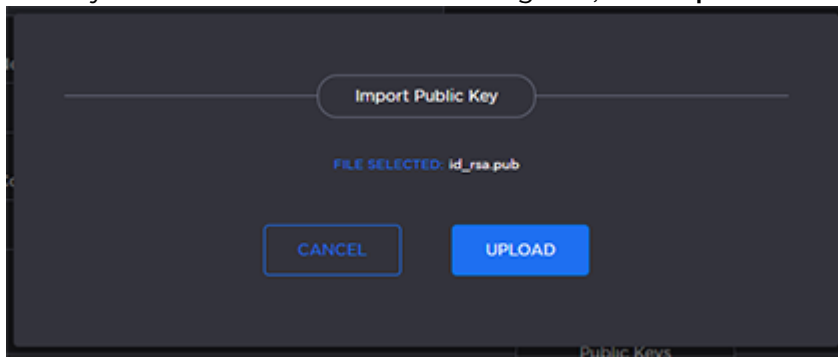
- **Managing Public Key Authentication**

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 Series.

To upload a public key file for an account:

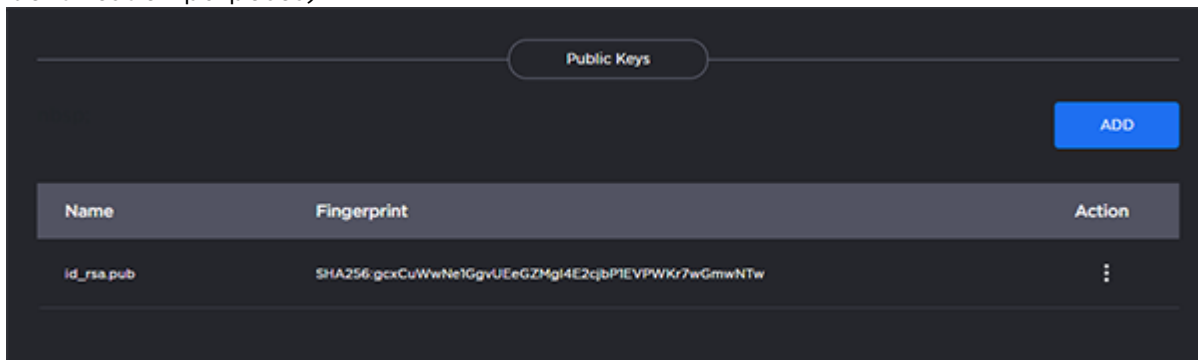
1. From the Accounts List View, click a link in the table for an existing account.
2. On the Account Settings page, under Public Keys, click **Add** and select the file in the Open File dialog box.
The public key file must have a `.pub` extension.
3. When you see the filename in the dialog box, click **Upload**.



Tip

To select a different public key file, click **Cancel**.

The file is then added to the Public Keys list 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

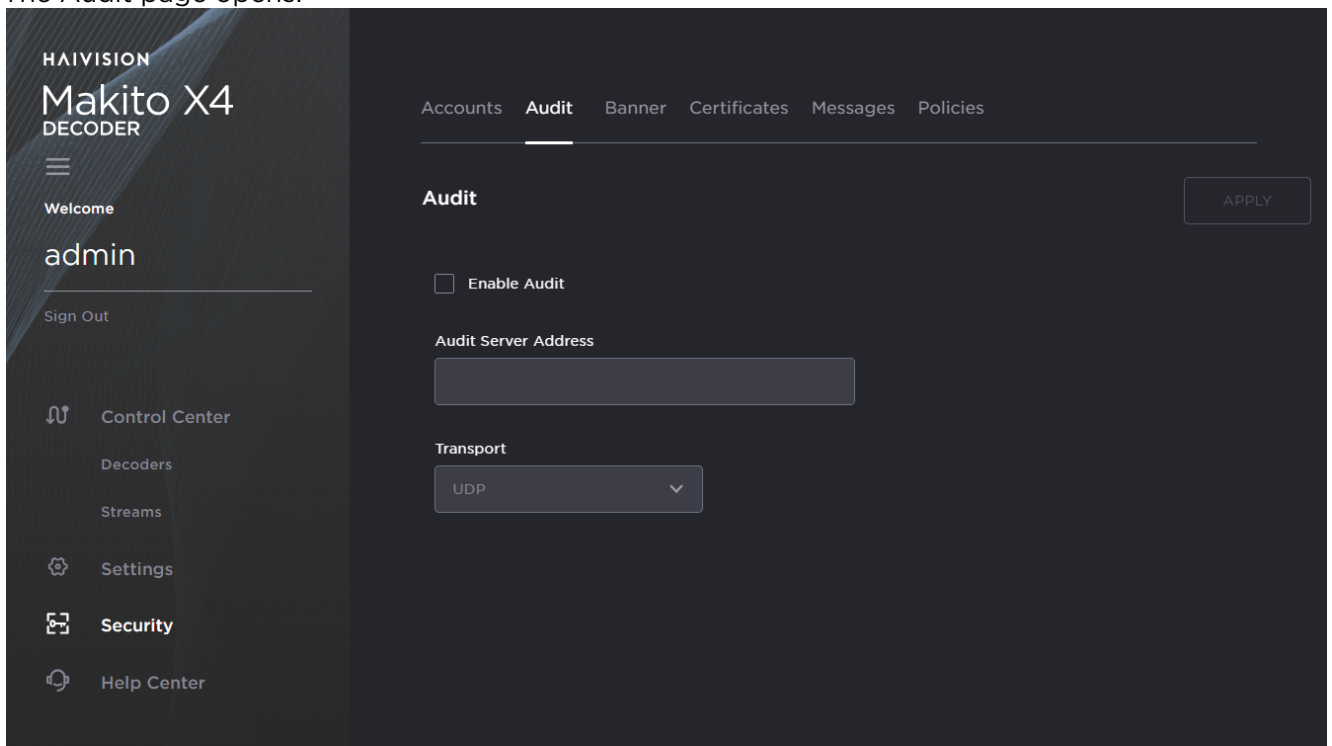
To delete a previously uploaded public key file from the list, click the More Options icon next to the filenames and click **Delete**.

Managing Audits

From the Audits page, administrators can set up logging to an Audit server for Makito X4 devices.

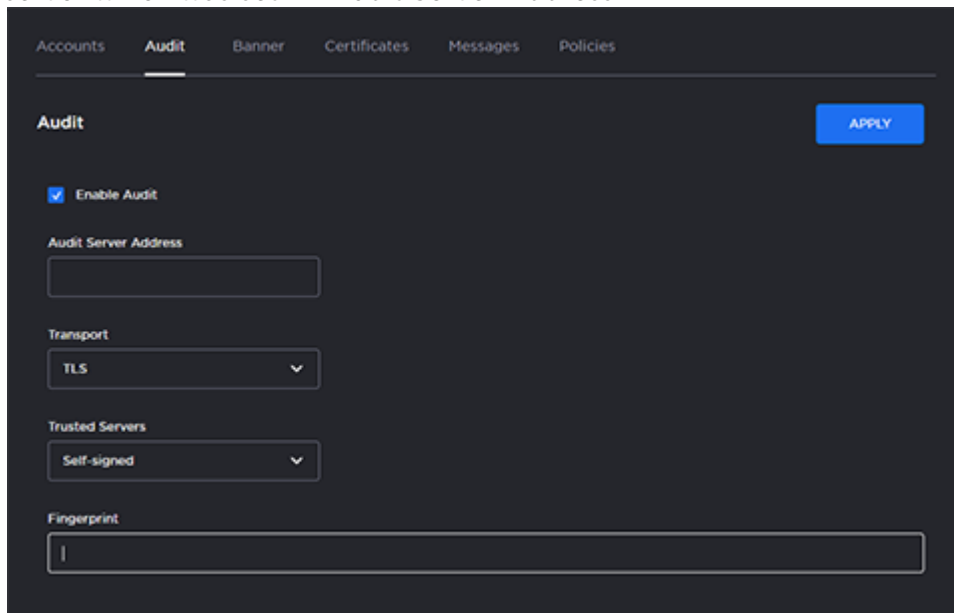
To configure an Audit server:

1. Click **Security** on the on the side menu and **Audit** on the navigation bar. The Audit page opens.



2. Check the **Enable Audit** checkbox to start logging to the audit server.
3. Type the audit server address and port in the Audit Server Address field. See "Audit Settings" (link below) for more details.
The server address must be the Common Name or one of the Subject Alternative Names in the server's certificate for successful authentication if Transport is set to TLS and Trusted Server is set to CA-Signed.
4. Set the type of transport protocol that will be used to send the logs to the audit server.
5. If TLS is selected as Transport, choose the type of audit server to be accepted as a trusted server: either All (no server authentication), CA-signed, or Self-signed. If Trusted Servers is set to CA-signed, the root-CA certificate of the audit server certificate chain must be imported in the encoder (see "Managing Certificates") for the TLS connection to succeed.
6. If Trusted Servers is set to Self-signed, copy the Fingerprint string from the Audit server's certificate and paste it in the Fingerprint field under Audit Settings to identify the certificate trusted for this TLS connection. The fingerprint should be that of the certificate that belongs to the audit

server which was set in "Audit Server Address".



The screenshot shows the 'Audit' configuration page in the HAIVISION interface. At the top, there is a navigation bar with tabs for 'Accounts', 'Audit', 'Banner', 'Certificates', 'Messages', and 'Policies'. The 'Audit' tab is selected. Below the navigation bar, the 'Audit' section is displayed. It includes a blue 'APPLY' button in the top right corner. The settings are as follows: 'Enable Audit' is checked; 'Audit Server Address' is an empty text input field; 'Transport' is a dropdown menu set to 'TLS'; 'Trusted Servers' is a dropdown menu set to 'Self-signed'; and 'Fingerprint' is a long, empty text input field.

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
Enable Audit	disabled	Check or clear this checkbox to enable or disable audits for the system.
Audit Server Address	n/a	Type in the address and port of the remote server, in one of the following formats: <ul style="list-style-type: none"> fqdn[:port] ipv4_addr[:port] ipv6_addr[:port] hostname[:port] If the port is not provided, the default port for the chosen Transport will be used:
Transport	UDP	Select the Transport Type from the drop-down list: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

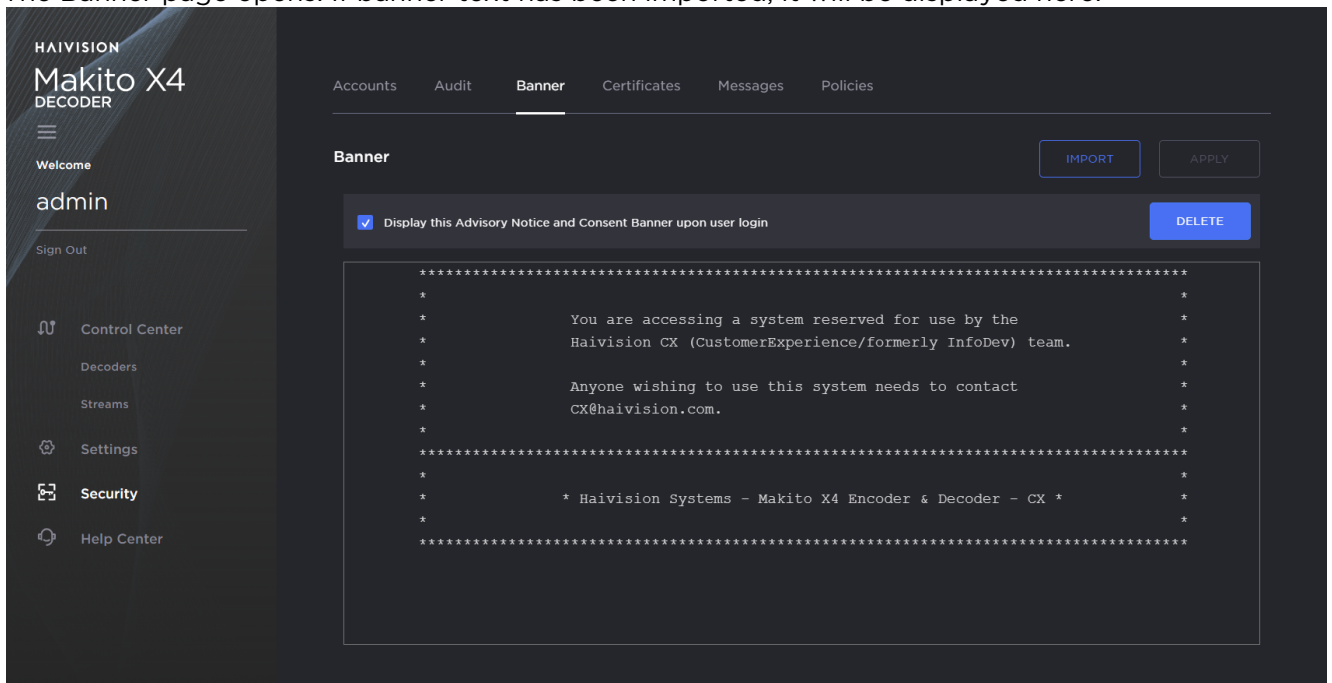
Managing Banners

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.

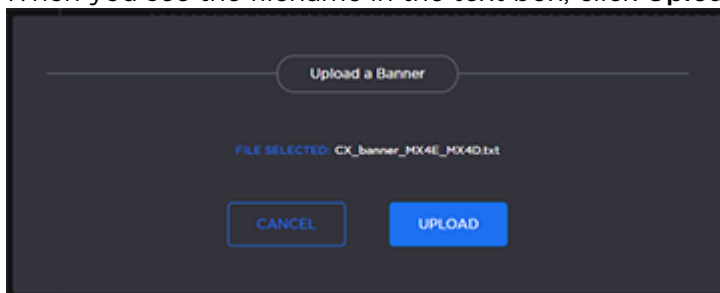
Only ASCII file format is supported for the banner file; the banner is a single text file with a maximum file size of 4KB.

To upload a text file for the Banner page:

1. Click **Security** on the side menu and **Banner** on the navigation bar.
The Banner page opens. If banner text has been imported, it will be displayed here.



2. Click **Import**.
3. Drag the banner file to the drop area or click **Browse** or **Choose a file** to select the file.
4. When you see the filename in the text box, click **Upload**.



Tip
To select a different banner file, click **Cancel**.

The banner text is now displayed in the pane.

5. To display the banner upon user sign-in, check the checkbox.

Note

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

Important

IP display is enabled on the serial port login prompt by default and takes precedence over a banner. If both Banner and IP display are enabled, users will see the IP, not the banner on the serial port.

You can disable and re-enable IP display using the CLI commands

`disable_ip_display_on_serial_port` and `enable_ip_display_on_serial_port`. If you disable IP display with this CLI command, the banner works.

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

Tip

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

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

Related Topics

- [banner](#)

Managing Certificates

The Certificates page shows the list of Identity and CA Certificates installed on Makito X4 devices.

- **Identity Certificates:** An Identity Certificate identifies the Makito X4 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 X4 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 X4 identity certificate (if you have one).

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

To manage Certificates:

1. To generate a Self-signed Certificate or a Certificate Signing Request (CSR), see [Generating a Certificate](#).
2. To import an Identity or Ca Certificate, see [Importing a Certificate](#).
3. To view the details of a certificate, click the certificate name from the list of Identity or CA Certificates. (See [Viewing Certificate Details](#).)
4. To set the default Identity Certificate (i.e., the Identity Certificate that will be used to represent the device during Audit and HTTPS authentication), hover over the certificate row and click the (grayed out) check mark under **Default**.

The selected certificate will be set as the default certificate. It will be immediately applied to communications with the Audit server, but will not apply to HTTP communications until the next service restart or system reboot.

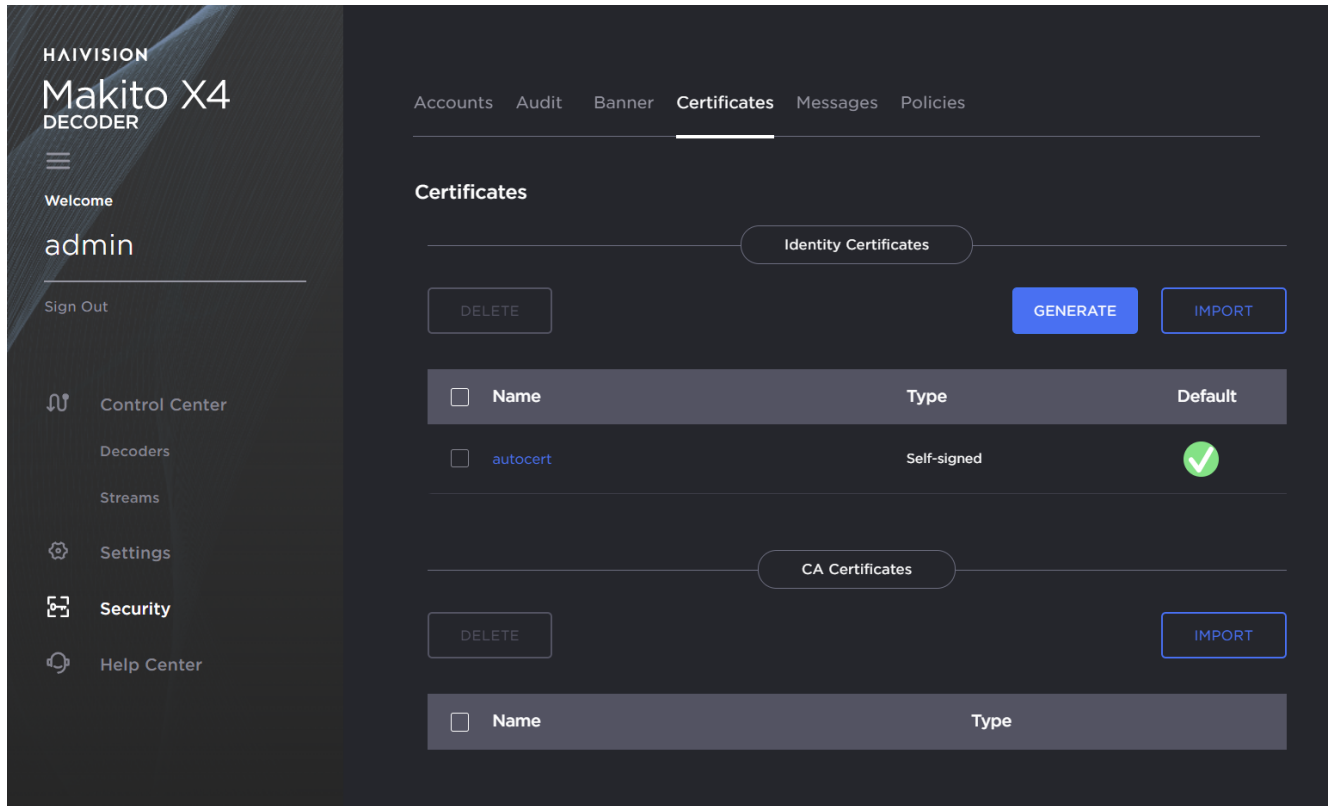
✓ Tip

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

Generating a Certificate

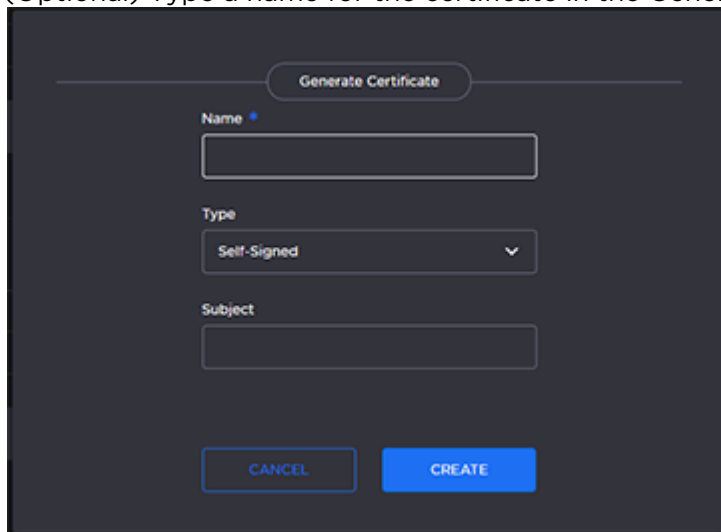
To generate a Self-signed Certificate or a Certificate Signing Request (CSR):

1. Click **Security** on the side menu and **Certificates** on the navigation bar.
The Certificates page opens.



The default Identity Certificate is indicated with a green check.

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



4. For the Type, 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 **Create**.

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 a Makito X Series device and exported for signing. For details, see "Certificate Name" in "Certificate Settings".

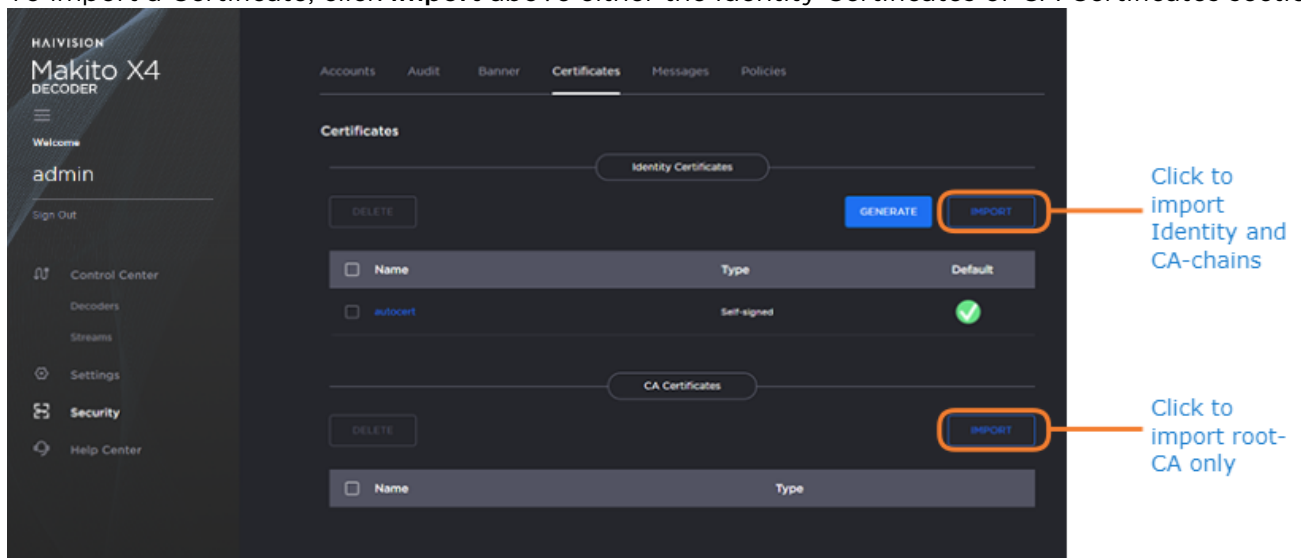
Related Topics:

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

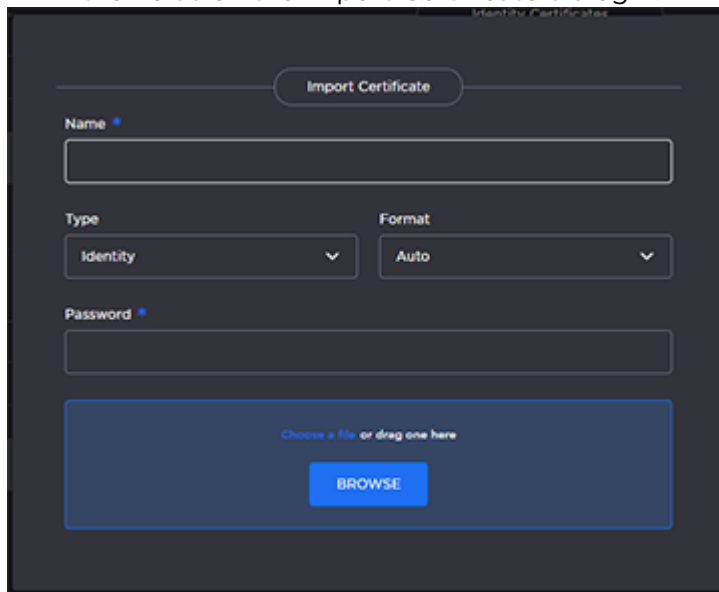
Importing a Certificate

To manage Certificates:

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



2. Fill in the fields on the Import Certificate dialog:



The screenshot shows a dark-themed dialog box titled "Import Certificate". At the top center is a button labeled "Import Certificate". Below it are several input fields: a "Name" text field, a "Type" dropdown menu currently showing "Identity", a "Format" dropdown menu currently showing "Auto", and a "Password" text field. At the bottom of the dialog is a large blue rectangular area containing the text "Choose a file or drag one here" and a smaller blue button labeled "BROWSE".

3. Type in the Certificate Name.

4. Select or enter the new value(s) in the remaining field(s). See "Import Identity or CA Certificate dialog" in "Certificate Settings" (link below).

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

```
Certificate Fingerprints:
MD5: 68:D5:F5:09:6E:88:EA:FF:8C:64:A3:47:E3:19:0A:09
SHA1: AF:1A:2E:F3:4F:CE:C9:4D:D9:63:DD:40:42:1C:B6:C8:68:14:0A:62
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    f4:d7:2f:8c:d6:74:2d:05
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=US, ST=Illinois, L=Lake Forest, O=Haivision Network Video, Inc., OU=PRODUCT DEVELOPMENT, CN=localhost.localdomain/emailAddress=support@haivision.com
  Validity
    Not Before: Oct 30 13:52:25 2020 GMT
    Not After : Feb  2 13:52:25 2023 GMT
  Subject: C=US, ST=Illinois, L=Lake Forest, O=Haivision Network Video, Inc., OU=PRODUCT DEVELOPMENT,
  CN=localhost.localdomain/emailAddress=support@haivision.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:e5:9e:41:a9:34:1b:0c:03:75:1b:cf:86:8e:06:
      b5:d6:96:7d:f2:62:8b:76:a7:3f:87:3e:fc:04:a3:
      31:35:d5:e2:61:ae:77:28:74:a7:6a:62:b0:7b:c6:
      ee:7f:6b:ce:d3:ba:f1:90:ec:dc:f6:50:2a:5a:1b:
      c4:19:1e:c1:91:30:c4:72:9a:5e:bf:7f:98:89:76:
      6b:36:87:ea:21:25:3c:5c:88:b1:0c:01:c7:db:29:
      0f:5e:a7:f4:ed:7e:07:d2:83:89:a6:c1:5e:82:e8:
      72:3e:6f:31:8e:7b:5e:d7:86:96:f2:bc:07:eb:b3:
      59:65:8a:50:72:ac:53:a8:dd:15:77:89:40:68:16:
      7d:9d:41:ad:8f:d5:79:20:38:4c:8e:ed:df:39:06:
      58:15:b2:6d:bf:d1:13:cd:24:00:59:6b:e8:82:d9:
      3d:94:2e:2a:1a:e9:76:cf:4a:3a:e4:12:fl:64:08:
      c4:11:4f:c5:ba:ef:f1:2f:04:a7:9b:6d:e0:cc:3c:
      fc:34:94:26:3f:a0:66:fb:b5:ac:6f:48:e4:45:91:
      92:cf:47:aa:ca:fb:14:b6:dc:94:43:11:3b:c9:f8:
      ae:de:89:d8:b4:21:13:5d:6d:1b:db:18:ae:bc:3b:
      bc:50:f9:58:9e:94:d8:15:e6:97:b0:8b:8b:ee:a9:
      c1:f9
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      E1:3B:03:33:BE:23:99:23:93:5C:DE:54:CA:87:CC:CB:D7:12:04
    X509v3 Authority Key Identifier:
      keyid:E1:3B:03:33:BE:23:99:23:93:5C:DE:54:CA:87:CC:CB:D7:12:04

    X509v3 Basic Constraints:
      CA:TRUE
    X509v3 Extended Key Usage:
      TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Alternative Name:
      DNS:MXD-Franks, IP Address:10.65.10.174
  Signature Algorithm: sha256WithRSAEncryption
  df:6b:9e:ca:43:69:f2:6c:72:01:0e:de:21:67:af:16:af:ae:
  12:30:d7:16:70:9a:e5:60:dd:7a:e3:b1:79:36:f1:a5:c5:dc:
  a0:4f:dc:c3:1b:a1:3a:9c:37:b4:7d:9e:f3:77:04:a3:e2:64:
  5d:9f:d6:be:1e:85:61:ac:80:9a:73:65:1d:bd:86:a4:f8:4b:
  75:b8:03:d5:e0:c3:d9:4b:53:53:5e:b0:0f:66:c1:87:fd:be:
  2a:1c:01:15:b2:3d:2c:a8:77:5d:35:2d:c3:3d:74:9d:7d:bb:
  d3:bd:a0:d5:36:f7:c0:c8:27:9d:d7:75:92:8a:f0:56:da:2a:
  51:76:88:e8:ed:5c:4b:f3:9b:f1:8e:1a:82:c9:96:bf:a1:00:
  f3:53:63:ad:ad:50:16:78:8b:af:9b:0d:eb:ca:b2:01:c7:0e:
  83:d5:67:c8:6b:c2:59:6e:db:ce:76:51:08:ef:ae:c3:b2:36:
  cc:8c:f6:61:03:cf:f1:15:8d:b1:b0:2c:19:03:c3:90:d8:4c:
  da:39:96:53:c3:94:d6:bf:28:38:32:69:4a:3a:dd:0c:ad:6c:
  6d:cd:8d:24:0c:2e:db:94:37:dc:a3:bf:3b:38:3f:02:a7:7c:
  1d:1c:3d:10:0b:1d:e0:7e:c5:d7:c7:9f:e5:90:57:81:f4:f6:
```

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 X4 as well as listed on the Certificate page.
Type	Self-signed	<p>Select the Signature Type:</p> <ul style="list-style-type: none"> • 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	<p>The Subject identifies the device being secured, in this case, the Makito X4.</p> <p>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).</p> <p>Type in the subject in the form: <code>"/C=US/ST=Maine..."</code></p> <p>where the most common attributes are:</p> <ul style="list-style-type: none"> • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name <p>Note that parameters with spaces should be enclosed in quotation marks.</p>

Import Certificate dialog

Setting	Default	Description/Values
Certificate Name	n/a	<p>The Certificate Name is the name under which the certificate will be stored on the device.</p> <ul style="list-style-type: none"> If the certificate is a new certificate generated outside of the Makito X4, 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)	<ul style="list-style-type: none"> Identity: If you are importing an identity certificate. CA-Chain: If the import is a chain of certificate authorities leading to the root certificate authority. The imported CA-chain can contain one or more certificates linking its associated identity certificate to the root-CA and may or may not include the root-CA itself (that will only be trusted if imported as a root-CA). <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p>⚠ Note</p> <p>Even though you can see the Type buttons, clicking Import in either the ID or CA sections may cause error messages to be displayed, i.e.:</p> <ul style="list-style-type: none"> If you select CA-root in the import from the ID. If you select Identity or CA-chain in the import from the ca-root. </div>
	root-CA (CA Certificates)	<ul style="list-style-type: none"> 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	<p>Select the file format for the Certificate (the formats differ in the way the file is encrypted):</p> <ul style="list-style-type: none"> 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	<p>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.</p>

Setting	Default	Description/Values
Import File	n/a	Drag the import file to the drop area or click Browse to select the file.

Related Topics:

- [Generating a Certificate](#)
- [Importing a Certificate](#)

Managing Messages

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

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

The log of the actions recorded includes the following:

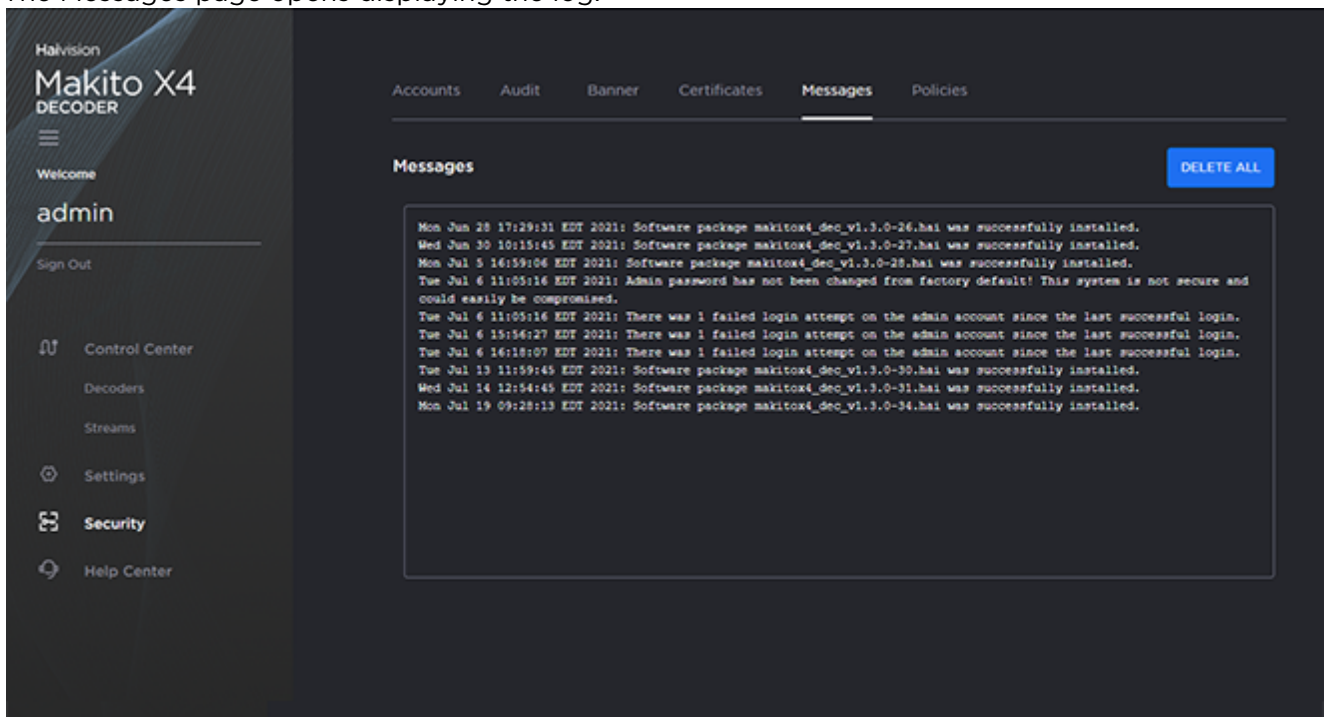
- The user initiating the action and the action being initiated.
- The time of the action.
- The results of the action (success/failure).

Note

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

To view the messages:

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



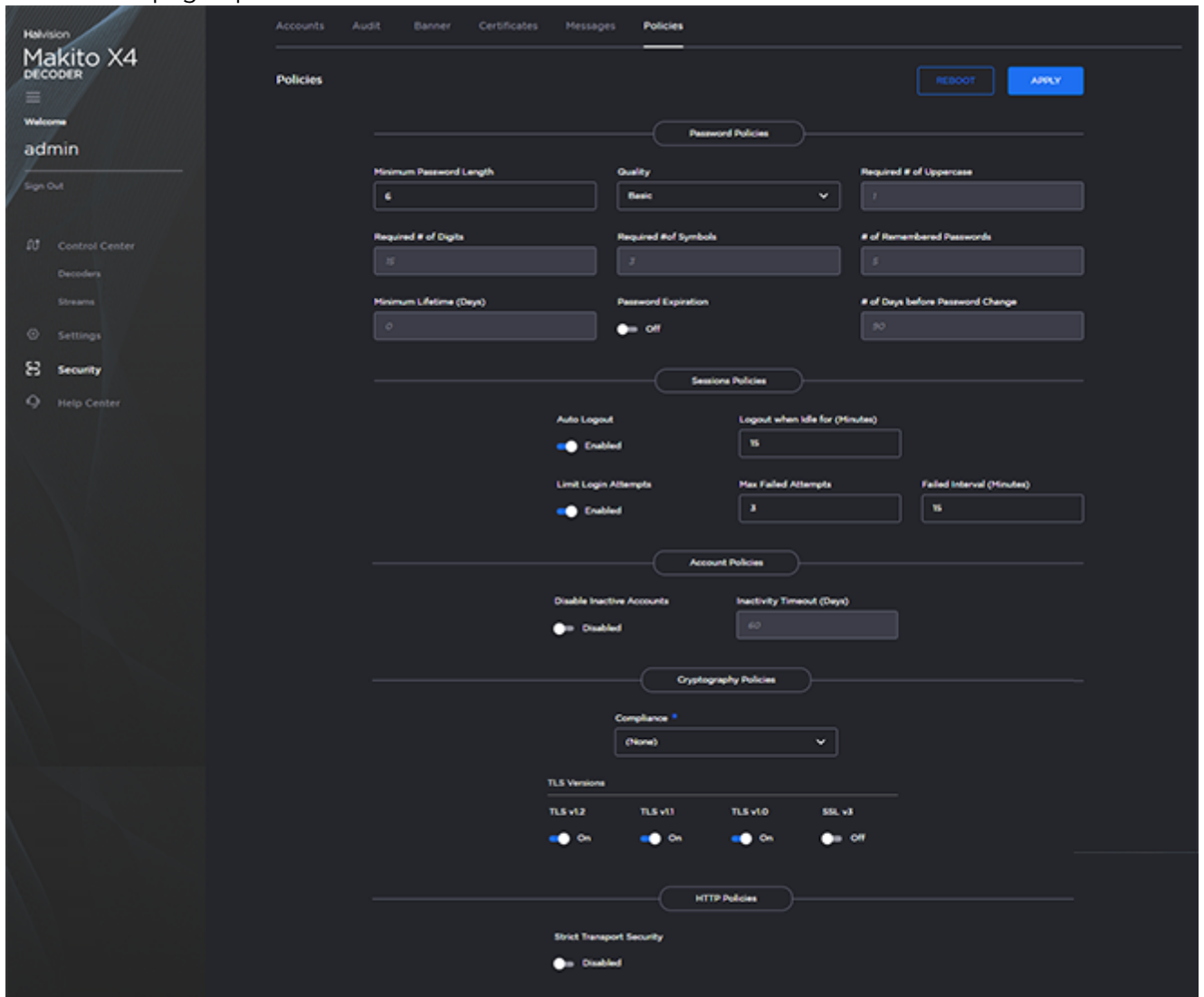
2. To delete the messages, click **Delete All**. The messages will be deleted immediately.

Managing 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.

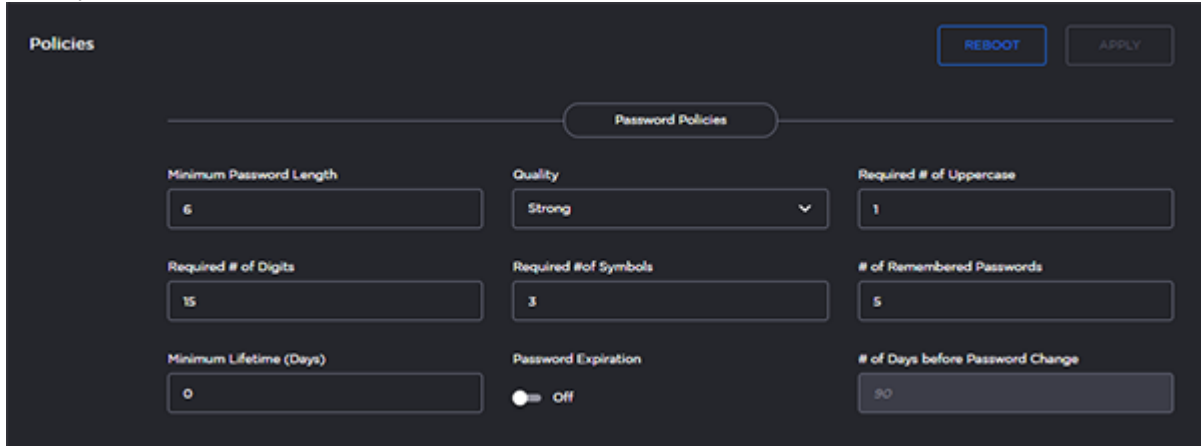
To view and manage the Security policies for the Makito X Series:

1. Click **Security** on the side menu and **Policies** on the navigation bar. The Policies page opens.



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

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



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

Policy Settings

The following table lists the Policy settings for the Makito X4 decoder:

Password Policies

Policy Setting	Default	Description/Values
Minimum Length	6 characters	Type in the minimum password length (from 6-40 characters). <div style="border: 1px solid #ffc107; padding: 5px;"> <p>Note Passwords can be up to 80 characters.</p> </div>
Quality	Basic	Select the required password quality; works in conjunction with Password requires at least below: <ul style="list-style-type: none"> 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.
Strong Requirements	0	(Password quality must be Strong) Specify the minimum required number of: <ul style="list-style-type: none"> 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	<p>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.</p> <div style="border: 1px solid #ffc107; padding: 5px;"> <p>Note Enabling the Auto-Logout Session policy also limits the number of concurrent sign-ins per account to 4.</p> </div>
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
Failed Interval (Minutes)	N/A if Disabled ----- 15 minutes if Enabled	<p>(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</p> <div style="border: 1px solid #ffc107; padding: 5px;"> <p>Note If a user fails the “Max Failed Attempts” within the “Failed interval”, the account will be locked for 10 minutes.</p> </div>

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	<p>(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.</p> <div style="border: 1px solid #28a745; padding: 5px;"> <p>Tip The system adds one (1) day (or 24hour grace period) to the setting configured by the user.</p> </div>

Cryptography Policies

Policy Setting	Default	Description/Values
Compliance	None	<p>Specifies the required cryptographic compliance, either:</p> <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>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.</p> </div>
TLS Versions	TLSv1.2, TLSv1.1, TLSv1.0	<p>Specifies which TLS (Transport Layer Security) versions are accepted from the HTTPS client.</p> <ul style="list-style-type: none"> • TLSv1.2 • TLSv1.1 • TLSv1.0 • SSLv3 <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>SSLv3 can be enabled only if Compliance is set to None. At least one TLS version must be enabled.</p> </div> <div style="border: 1px solid #c8e6c9; padding: 5px; margin-top: 10px;"> <p>Tip</p> <p>For backward compatibility considerations, you may choose to disable the older TLS versions not needed by the organization's TLS peers (i.e., browsers, syslog server) and plan the upgrade of those not supporting the latest TLS version with the objective of enabling only the latest TLS version.</p> </div>

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.

Using SNMP to Configure A/V Services

This section provides information required to manage the Makito X4 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 X4 through the exchange of SNMP messages.

Audience

This content is intended for users who are familiar with SNMP-based management and who will be developing applications such as provisioning services, or creating and modifying existing network management systems to manage the Makito X4.

**Tip**

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

Topics in This Chapter

- [SNMP Overview](#)
- [Supported MIBs](#)
- [SNMP Agent Components](#)
- [SNMPv3](#)
- [SNMP Utilities](#)
- [SNMP Syntax for Setting Up Streams](#)

SNMP Overview

To support management of Makito X devices by third party Network Management Stations (NMSs), the system includes an SNMP agent that may be used to configure and control the system's Audio/Video services and streams.

Note

The Makito X Series uses Net-SNMP Version 5.7.3 and support SNMP v1, v2c, and v3.

The Makito X Series supports a number of SNMP commands used to set or get Management Information Base (MIB) objects on the local host or on other SNMP agents reachable over IP networks.

Supported MIBs

The Makito X4 SNMP agent supports the MIB-II (RFC 1213) standard and its updates, SNMPv3 MIBs, as well as the Haivision proprietary Enterprise MIB. The following table lists the supported MIBs:

Supported MIBs	Standard	Description
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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).
<ul style="list-style-type: none"> • IPV6-MIB.txt 	RFC-2465	Management Information Base for IP Version 6.
<ul style="list-style-type: none"> • HAI-VISION-MIB.txt • HAI-AVT-STREAM-MIB.txt • HAI-HDC-MIB.txt 	Haivision Enterprise	Supports configuration, status, and statistics.

Encoder-only		
<ul style="list-style-type: none"> HAI-MAKITO-X4-ENC-CAPS.txt 	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X4 (encoder) SNMP AGENT. It specifies which object groups from the listed MIB files are implemented, and furthermore, it specifies implementation constraints and deviations from the MIB OBJECT specification such as differences in ranges.
Decoder-specific		
<ul style="list-style-type: none"> HAI-MAKITO-X4-DEC-CAPS.txt 	Haivision Enterprise	This MIB formally specifies the capabilities of the Makito X4 (decoder) SNMP AGENT. It specifies which object groups from the listed MIB files are implemented, and furthermore, it specifies implementation constraints and deviations from the MIB OBJECT specification such as differences in ranges.

Note

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

SNMP Agent Components

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

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

snmpd

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

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

snmpd.conf

`snmpd.conf` is the configuration file that defines how the SNMP agent works. You may need to edit this file to specify the location of the Network Management System (NMS). However, for most settings, it is preferable to use the `nmcfg` configuration script.

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

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

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

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

snmpd.local.conf

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

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

SNMP Community Names

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

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

nmcfg

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

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

Following is an example of the nmcfg configuration script output:

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

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

auth protocol      priv protocol      user
-----
MD5                DES                admin
MD5                nopriv             guest
SHA                AES                johndoe

# nmcfg help
usage: nmcfg
nmcfg help
nmcfg access help
nmcfg access usm permit <uname> {<group>|ro|rw} [{noauh|auth|priv}]
nmcfg access usm delete <uname>
nmcfg community help
nmcfg community permit <community> {<group>|ro|rw} [<host>]
```

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

SNMPv3

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

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

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

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

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

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

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

Examples

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

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

```
# snmpget -v3 -u johndoe -a MD5 -A "password" -l authNoPriv localhost sysName.0
SNMPv2-MIB::sysName.0 = STRING: razor #
```

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

```
# snmpget -v3 -u johndoe -l noAuthNoPriv localhost sysName.0

Error in packet
Reason: authorizationError (access denied to that object) #
```

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

```
# snmpset -v3 -u johndoe -a MD5 -A "password" -x DES -X "pass phrase" -l authPriv localhost
haiAvtStreamEncapsulation.1 i directRtp
```


```
HAI-AVT-STREAM-MIB::haiAvtStreamEncapsulation.1 = INTEGER:
directRtp(1)
```

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

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

SNMP Utilities

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

To do this...	Use this command ...
To retrieve the value of an object from a network entity.	<code>snmpget</code>
To set information on a network entity.	<code>snmpset</code>
To retrieve management information from a network entity.	<code>snmpstat</code> <code>us</code>
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.	<code>snmpwalk</code>
<p> Note The retrieval of a complete subtree is referred to as "walking the MIB."</p>	

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

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

SNMP Syntax for Setting Up Streams

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

Table	Index	Description
haiAvtStreamNewID.0	none	Next available stream ID
haiAvtStreamInverseTable	IP address type IP address Port	Table to retrieve the stream ID from the IP address and port
haiAvtStreamTable	Stream ID	Stream configuration and status
haiAvtStreamStatsTable	Stream ID	Stream statistics
haiAvtStreamPgmTable	Stream ID Program Index	Transport Stream programs. Only SPTS (Single Program Transport Stream) supported. Not present for non Transport Streams (directRTP, QuickTime).
haiAvtStreamContentTable	Stream ID Program Index Content Index	Contents (video, audio, ad insertion, and/or metadata). Elementary Streams (ES) for Transport Stream. Only one entry for non-TS in which case Program Index is 1. One to three entries exist for Transport Streams.

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

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

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

Examples

The following example, using `netsnmp` CLI commands on the Makito X Series encoder, creates a streaming session to IP Address `198.51.100.106` at port `2000`, and starts streaming immediately. The Stream ID `0` (`haiAvtStreamTable` index) is used to create a stream; this value will be set to the first available Stream ID ($>=1$) on `createAndGo` or when set to active after `createAndWait`:

```
>snmpset -v2c -c admin localhost haiAvtStreamAddrType.0 = ipv4 haiAvtStreamAddr.0 d 198.51.100.106
haiAvtStreamPort.0 u 2000 haiAvtStreamRowStatus.0 i createAndGo
```

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

```
>snmpset -v2c -c admin -IS haiAvtStream -Is .0 localhost AddrType = ipv4 Addr d 198.51.100.106 Port u
2000 RowStatus i createAndGo
```

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

```
>snmpget -v2c -c admin localhost haiAvtStreamInverseID.ipv4.4.198.51.100.106.2000
HAI-AVT-STREAM-MIB::haiAvtStreamInverseID.ipv4."198.51.100.106".2000 = HaiAvtStreamID: 5
```

To create a Stream with a known ID, the `haiAvtStreamNewID.0` object reports the next available Stream ID. In the example below, the Transport Stream Program number is set to `7` and the video encoder `1` is selected for the video content. Note that `createAndWait` is used so the program and content table can be set after stream creation.

```
>snmpget -v2c -c admin localhost haiAvtStreamNewID.0
HAI-AVT-STREAM-MIB::haiAvtStreamNewID.0 = HaiAvtStreamID: 5
>snmpset -v2c -c admin -IS haiAvtStream -Is .5 localhost AddrType = ipv4 Addr d 198.51.100.106
Port u 2000 Encapsulation i tsUdp RowStatus i createAndWait
>snmpset -v2c -c admin -IS haiAvtStream localhost PgmNumber.5.1 i 7 PgmNbContents.5.1 i 2 ContentType.5.1.1
i video ContentToolID.5.1.1 i 1 ContentType.5.1.2 i audio ContentToolID.5.1.2 i 0
>snmpset -v2c -c admin localhost haiAvtStreamRowStatus.5 i active
```

Resetting the Decoder

- **Default Network Settings**

This section describes the steps to perform a hardware reset on the Makito X4 decoder. The Reset button is used either to reset the system or to restore the factory default settings.

- **System Reset:** In some cases, if your decoder is experiencing a problem, resetting the system can return the decoder to normal operation.
- **Factory Reset:** If the problem remains after performing a reset, it may help to restore the decoder to its factory default settings. A factory reset returns the decoder 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.

Use one of the following methods to either reset or restore the Makito X4 decoder settings:

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



2. **System Reset:** Press the recessed micro switch (you will feel the button depress) for at least one second and release. Be sure to release the button in less than five (5) seconds.
-or-
Factory Reset: Press and hold the recessed micro switch for five (5) seconds.
3. Wait for the decoder to reboot. As soon as the lights stop blinking and the Status LED is solid green, the decoder is ready.

Default Network Settings

After a factory reset, the Network settings should be:

IP Address	Subnet Mask	Gateway
10.5.1.2	255.255.0.0	10.5.0.1

Related Topics:

- [Default Decoder IP Address](#)

CLI Command Reference

Management via the CLI is possible through a telnet session, SSH, or (if applicable) RS-232. This alphabetical command reference lists and describes the available Command Line Interface (CLI) commands to configure and manage the Makito X4 decoder.

Accessing the CLI

To access the decoder CLI:

1. Open a telnet session to the decoder (for the default encoder IP address, see [Accessing the Decoder](#)).
2. At the login prompt, type the username and password (see [Role-based Authorization](#)).

Syntax Conventions

The following syntax conventions are used in this appendix:

Convention	Description
Monospaced font	Indicates command names and options, filenames and code samples.
<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 X4 decoder CLI commands are divided in two main groups: operation and administration:

- **Operation Commands** are used to manage video decoding. 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.

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

[Operation Commands](#) [Administration Commands](#) [Access](#) [Other/Utilities](#)

Operation Commands

Command	Role			Description
	Admin	Operator	Guest	
<code>dec</code>	Yes	Yes	"get" only	Manage A/V decoder settings.
<code>leds</code>	Yes	Yes	"get" only	Display current LED status and initiate blinking of Status LEDs on the Makito X4 face-plate in order to help locate the device.
<code>mkstill</code>	Yes	Yes	No	Generate still images from a picture.
<code>still</code>	Yes	Yes	"list" only	Manage still image files on the Makito X4 file system.
<code>stream</code>	Yes	Yes	"get" only	Create and manage streams to map decoder inputs to output interfaces.
<code>temperature</code>	Yes	Yes	"get" only	Display the current temperature of the unit.

[Operation Commands](#) [Administration Commands](#) [Access](#) [Other/Utilities](#)

Administration Commands

Command	Role			Description
	Admin	Operator	Guest	
Network and Management				
<code>config</code>	Yes	Yes	"list" only	Manage configurations on the Makito X4.
<code>date</code>	Yes	Yes	Yes	Display the current date.

emspair	Yes	No	No	Pair and unpair the Makito X4 with a Haivision EMS (Element Management System).
ethercfg	Yes	No	No	View, manually control, and save the Ethernet configuration parameters.
haiversion	Yes	Yes	Yes	Display the Firmware Build ID, Build Time, and serial number for the Makito X4.
ipconfig	Yes	No	No	Set and view the parameters that specify the networking context for the Makito X4, including the IPv4 settings, hostname, and DNS.
ipv6config	Yes	No	No	Set and view the IPv6 settings.
license	Yes	No	No	Manage licensed features.
package (for upgrade)	Yes	No	No	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	No	No	Halt and restart the Makito X4.
service	Yes	No	No	Enable and disable network services, including HTTP, passthrough, snmp, ssh, talkback, telnet, and vf.
Security Commands				
account	Yes	No	No	Manage user accounts for the decoder.
audit	Yes	No	No	Enable remote logging of security and administrative events and configure the remote audit (<code>syslog</code>) server connection.
banner	Yes	No	No	Manage the Advisory Notice and Consent Banner.
certificate	Yes	No	No	Manage TLS certificates for the Web interface HTTPS server and the secured TLS connection to the remote audit server.
messages	Yes	No	No	View and manage administrative login messages.
policy	Yes	No	No	Manage security policy settings.
pubkey	Yes	Yes	Yes	Manage the user's own authorized SSH public keys.

[Operation Commands](#)
[Administration Commands](#)
[Access](#)
[Other/Utilities](#)

Access

Command	Role		
	Admin	Operator	Guest
Web access	Yes	Yes	Yes
Telnet to/from decoder	Yes	Yes	Yes

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.
tracert	Yes	Yes	Yes	Display the route (path) and measure transit delays of packets across an IP network.

For an overview of system access control on the Makito X4 decoder, see [Role-based Authorization](#).

Operation Commands

- `dec`
- `leds`
- `mkstill`
- `still`
- `stream`
- `temperature`

dec


The `dec` command is used to manage A/V decoder settings. The `dec start` and `dec stop` commands can be used to start and stop decoding video. ID can be `all` or `id1[,id2,id3,id4]` with values from `0` to `3`. You can specify a comma-separated list of IDs for the operation, as shown in the examples that follow.

Synopsis

```
dec ID start
dec ID stop
dec ID set parameter=value [parameter=value]
dec ID get [config/stats/all] [video/buffer/metadata/audio/clockrecovery/all]
dec ID capture [filename=value] [resolution=WxH]
dec ID clear
```

Actions

Action	Description
start	Starts decoding the video input.
stop	Stops decoding the video input.
set	Configures A/V decoder 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 decoder. You can choose to display the configuration (<code>config</code>), <code>stats</code> , or <code>all</code> [<code>config/stats/all</code>], and optionally specify a section of interest [<code>video/buffer/metadata/audio/clockrecovery/all</code>]
clear	Clears the decoder's statistics.
help	Displays usage information for the <code>dec</code> command.

 **Tip**

To display a summary of all the decoders in a table format, you can use `dec all get table`:

```
# dec all get table
ID STREAM ALT-STREAM STATE   FORMAT BUFFERING OUTPUTS
-----
0  1      (None)    ACTIVE  NATIVE  AUTOMATIC SDI-1
1  (None) (None)    STOPPED NATIVE  AUTOMATIC SDI-2
2  (None) (None)    STOPPED NATIVE  AUTOMATIC SDI-3
3  (None) (None)    STOPPED NATIVE  AUTOMATIC SDI-4
```

Parameters

Parameter	Default	Description/Values
streamId	n/a	Positive stream index. See Configuring Decoder Outputs .
stillImage	freeze	<p>The type of static image to display when the decoder is not receiving a video stream.</p> <ul style="list-style-type: none"> <code>freeze</code> : continues to display the last decoded video frame. <code>black</code> : displays a black screen. <code>blue</code> : displays a blue screen. <code>bars</code> : displays a series of vertical color bars across the width of the display. <code>mute</code> : disables the video output. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>When the still image is substituted on the display outputs, the video frame rate and resolution will be maintained. When the video decoder receives a new video stream, it waits until it receives a new IDR frame and re-starts the display with that IDR frame.</p> </div>
stillDelay	3	The delay in seconds before the still image is displayed: 1...1000
format	auto	<p>The output display format:</p> <ul style="list-style-type: none"> <code>Auto</code>: The decoder will select an output resolution that attempts to closely match the coded picture resolution, taking into account the capabilities of any displays connected to the HDMI interface. <code>Native</code>: The output resolution will be exactly the same as the coded picture resolution. If the coded picture resolution is not compatible with the output interfaces, nothing will be displayed. See "Output Resolution" in Decoder Settings. <p>Video scaling is not supported.</p>
frameRate	auto	<p>The output frame rate for the displays. <code>Auto</code>, <code>23</code>, <code>24</code>, <code>25</code>, <code>29</code>, <code>30</code>, <code>50</code>, <code>59</code> or <code>60</code></p> <ul style="list-style-type: none"> If <code>Auto</code> is selected, the actual frame rate generated will be the next highest valid frame rate supported by the SDI interface, plus the one that gives the best decimation factor. For example, 30Hz could be chosen instead of 29.970 Hz. Values set which are impossible to implement will be treated as <code>Auto</code>. Reasons for not supporting the selection can range from "Display does not support the frame rate" or "Frame rate is undefined for the detected input resolution".
buffering	automatic	<p>The type of buffering to use. A jitter buffer temporarily stores arriving packets in order to remove the effects of jitter from the decoded stream.</p> <ul style="list-style-type: none"> <code>automatic</code> - Set buffering automatically for good quality and proper sync <code>fixed</code> - Set buffering for fixed delay (use <code>delay=X</code> parameter) <code>multisync</code> - Set buffering for fixed delay from the encode time (use <code>multiSyncDelay=X</code> parameter, requires SYSTEM TC and NTP)
delay	n/a	The delay in ms when using <code>stc syncmode</code> with fixed buffering: 0...3000
multiSyncDelay	n/a	The delay in ms from encoder TC when using multisync buffering: 0...10000
hardwareDelayAdd	n/a	The number of ms to add to the delay for processing the output in the hardware. -20...200

Parameter	Default	Description/Values
dynamicrange	automatic	<p>Configures the decoder to detect the inbound High Dynamic Range (HDR) transfer function signaling and forward that information within the decoded stream.</p> <ul style="list-style-type: none"> • automatic: the decoder detects HDR transfer function from the source • off (SDR/BT.709) • 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 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>HLG and PQ override the settings in the stream.</p> </div>
outputs	n/a	<p>A list of physical SDI outputs the decoder core will feed: 1..4</p> <ul style="list-style-type: none"> • none, all, default, quad2SI, or id1[id2,id3,id4]

Examples

```
# dec 3,2,0 start
Starts decoders 3, 2 and 0 (in the order specified)

# dec 0 get stats
Returns (all) decoder statistics for decoder 0:

Decoder ID           : 0
Statistics
  State              : ACTIVE
  Up Time            : 2d11h42m30s
Buffering
  Buffering Mode      : AUTOMATIC
  Buffering State     : ACTIVE
  Video Latency      : 363ms
  PCR Updates        : 4 (Last One: 1d18h59m4s ago)
  STC Updates        : 13 (Last One: 1d11h14m44s ago)
  Buffering Adjustments : 6 (Last One: 1d11h14m44s ago)
  STC Lead Time Adjusts : 8 (Last One: 1d11h14m44s ago)
  STC to PCR Lead Time : -201ms (STC is behind PCR by 201ms)
  Packets Sent Late   : 21 (Last One: 8h44m12s ago, Max Late=95443694ms, Max Burst=11)
  Max Input Jitter    : 100ms (last changed 1d18h58m57s ago)
  Non-Video Late      : 0ms (max=0ms occurred Never)
  Video Decoder Latency : 42ms (max=57ms occurred 1d10h42m54s ago)
  Video Decoder Jitter : 33ms (max=153ms occurred 8h44m4s ago)
  Hardware Delay      : 50ms
  Video STC Lead Time : 168ms (Min=166ms, Max=199ms, Range=33ms)
  Last Video Skip/Replay: 8h44m11s ago
  Audio STC Lead Time : 446ms (Min=426ms, Max=463ms, Range=37ms)
  Last Audio Skip     : 1d18h59m11s ago
Video
  Preprocessor State  : ACTIVE
Stream Properties
  Compression         : H.265
  Color                : 4:2:0 8-bit
  Profile              : Main
  Level                : 5.1
  Format               : 1920x1080p59.94
  Bit Rate             : 10.18 Mbps
  Framing              : IP
  GOP Interval        : 60
```



```

    Slices per Frame      : 1
    Dynamic Range Stream : SDR
    Dynamic Range Output : SDR
    Metadata Present     : None
Format Changes         : 1 (Last One: 2m29s ago)
Input Frame Rate       : 59.94 [100.0%] (measured)
Video Decoder State    : ACTIVE
Display Format          : 1920x1080p59.94
Video Decoder Load     : 24%
Still Image            : FREEZE (INACTIVE) [Count=0, Max=0s, Last On=Never, Last Off=Never]
Decoder Counters
    VCU Frm not Release  : 3 (Last One: 0s ago)
    VCU IN Discontinuity : 1 (Last One: 2m29s ago)
HW Counters
    Displayed Output Frms : 8,750 [98.1162%] (Last One: 1s ago)
    Skipped Output Frames : 8 [0.0897%] (Last One: 1m47s ago)
    Replayed Output Frames : 160 [1.7941%] (Last One: 31s ago)
Audio
    Audio Decoder State  : ACTIVE
    Number of Pairs      : 1
    Played Output Frames : 6,939 [99.0578%] (Last One: 0s ago)
    Skipped Output Frames : 66 [0.9422%] (Last One: 1m48s ago)
    TS Discontinuities   : 1
    AUDIO PAIR #1
        Compression      : AAC-ADTS
        Bit Rate          : 80.32 kbps
        A/V Sync          : -2ms (Video TS 2830607135, Audio TS 2830607316)
        TS Discontinuities : 3
        Decoder Errors    : 0
        Output Errors     : 0
        Sample Rate In    : 48000 Hz
        Sample Rate Out   : 48000 Hz
Metadata
    Metadata State       : IDLE
Clock Recovery
    Tracking Mode        : ENABLE
    Status                : UNLOCKED (more than +-5PPM)
    ReSync Count         : 2
    PCR Updates          : 2 (Last One: 2m19s ago)
    Current STC          : 27,000,723Hz (26PPM from Nominal)
    STC Avg (last 2 min) : 27,000,495Hz (Deviation 14.0PPM)

```

```
# dec 0 get stats video
```

Returns (video) decoder statistics for decoder 0:

```
Decoder ID          : 0
Statistics
  State             : ACTIVE
  Up Time           : 4m15s
Video
  Preprocessor State : ACTIVE
  Stream Properties
    Compression      : H.265
    Color            : 4:2:0 8-bit
    Profile          : Main
    Level            : 5.1
    Format           : 1920x1080p29.97
    Bit Rate         : 10.03 Mbps
    Framing          : IP
    GOP Interval     : 60
    Slices per Frame : 1
    Dynamic Range Stream: SDR
    Dynamic Range Output: HLG
    Metadata Present : None
  Stream ID Changes : 1 (Last One: 4m14s ago)
  Format Changes    : 1 (Last One: 4m14s ago)
  Input Frame Rate  : 29.96 [100.0%] (measured)
  Still Image       : FREEZE (INACTIVE) [Count=0, Max=18857d13h38m27s, Last On=Never, Last
Off=4m10s ago]
  Video Decoder State : ACTIVE
  Display Format     : 1920x1080p29.97
  Video Decoder Load : 12%
Decoder Counters
  VCU Frm not Release : 2 (Last One: 8s ago)
  VCU IN Discontinuity: 0
HW Counters
  Displayed Output Frms: 7,473 [92.9131%] (Last One: 0s ago)
  Skipped Output Frames: 178 [2.2131%] (Last One: 3m50s ago)
  Replayed Output Frames: 392 [4.8738%] (Last One: 4m ago)
```

```
# dec 1 set stillimage=blue
```

Sets the static image to blue. You will receive the following confirmation:

```
Decoder configured successfully.
```

Related Topics

- [Configuring Decoder Outputs](#)
- [Decoder Settings](#)
- [Decoder Statistics](#)

leds

The `leds` command may be used to help locate a Makito X4 device by initiating blinking of the Status LEDs on the Makito X4 face-plate. This allows easy location of the device in large server room deployments, for example, to help identify a specific blade in a rack.

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

Synopsis

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

Actions

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

Parameters

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

Examples

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

Initiates blinking of the Status LEDs, provides the following confirmation:

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

```
# leds get
```

Displays current LED status:

```
LED States:
```

```
Status      : Green
4K Status   : Off
Error       : Off
SDI-1 Status : Off
SDI-2 Status : Green
SDI-3 Status : Green
SDI-4 Status : Green
```

```
# leds stop
```

Cancels blinking of the LEDs.
 LEDs no longer blinking.

Related Topics

- [LED Status Indicators](#)
- [Viewing System Status Information](#)

mkstill

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

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

Note

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

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

Synopsis

```
mkstill <infile> resolution [-f]
```

Parameters

Name	Default	Option	Description/Values
infile	n/a		The name of the image file to convert into a still image.
resolution	n/a		Specifies the desired resolution of the still image. Supported values include: <ul style="list-style-type: none"> • 1080 for 1920x1080 • 720 for 1280x720 • 480, NTSC for 720x480 • 576, PAL for 720x576 • VGA for 640x480 • SVGA for 800x600 • XGA for 1024x768 • XGA+ for 1152x864 • WXGA for 1280x768 • WXGA2 for 1280x800 • SXGA for 1280x1024 • WXGA3 for 1360x768 • WXGA4 for 1366x768 • WXGA+ for 1440x900 • SXGA+ for 1400x1050 • HD+ for 1600x900 • UXGA for 1600x1200 • WSXGA+ for 1680x1050 • WUXGA for 1920x1200
		-f	Forces overwrite of the still image at the destination.

Example

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

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

Related Topics

- [still](#) (CLI command)

still

The `still` command is used to manage available still image files on the Makito X4 file system.

Static image files must already have been generated (see following NOTE) and be located the folder `/usr/share/haivision/still_images` on the Makito X4 file system.

Note

You can generate the image file using the `mkstill` command.

Static images may be used to replace the “real” video stream when streaming is paused. You can then configure a Makito X4 stream with a static image using the `dec set` command.

Synopsis

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

Actions

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

Example

```
# still delete myimage.png
Deletes the image file myimage.png
```

Related Topics

- `mkstill` (CLI command)
- `stillImage` under `dec` Parameters
- “Still Image” under `Decoder Settings`

stream

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

When creating a stream you can specify a unique id to assign to it or let the system assign one for you. You can also specify a name for the stream if needed. The IP Address (`addr` field) is only required for multicast, but not for unicast streams. Most commands will accept the stream id or name in order select the proper stream to manage.

Once a stream is connected to the decoder (using the `dec` command), you can start/stop the decoder by way of the stream ID (e.g., `stream 1 start`).

Synopsis

```
stream create [port=udpport] [addr=ipaddr] [id=number] [name=text]
[encapsulation=ts-udp | ts-udp | ts-srt] [decoderId=number (0-3)]
[sourceaddr=mcastsenderaddr]

stream id/name start
stream id/name stop
stream id/name delete
stream id/name/all get
stream all get table
stream id/name clear
```

Possible Encapsulation Formats

Possible encapsulation formats and their specific options:

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

If encapsulation is ts-srt, you can specify a passphrase (10-79 characters) and the maximum latency (how long the decoder will buffer received packets, from 20-8000 ms).


Actions

Action	Description
create	Creates a decoder streaming session. A series of one or more <code>parameter=value</code> pairs can be specified at once.
delete	Removes the specified stream (entirely).
start	Starts the stream and its associated decoder.
stop	Stops the stream and its associated decoder.

Action	Description
get	Displays stream information. See Parameters below. You can specify to display the stream configuration, statistics, or all. <code>stream all get table</code> displays a summary of all the streams in a table format.
clear	Clears the stream's statistics.
help	Displays usage information for the <code>stream</code> command.

Parameters

Parameter	Default	Description/Values
port	n/a	The UDP port for the Decoder. Enter a number in the range <code>1025..65,535</code> . Note that RTP streams use even numbers only within this range.
addr	n/a	(Optional, only required for multicast) Enter a Multicast IP address in dotted-decimal format. <div style="border: 1px solid #ccc; padding: 5px;"> <p>⚠ Note</p> <p>The Multicast address range is from <code>224.0.0.0</code> to <code>239.255.255.255</code>. Multicast addresses from <code>224.0.0.0</code> to <code>224.0.0.255</code> 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 (<code>239.192.0.0/14</code>).</p> </div>
id	n/a	<div style="border: 1px solid #ccc; padding: 5px;"> <p>i Note</p> <p>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.</p> </div> <p>Most commands will accept the stream id or name (see below) in order to select the proper stream to manage.</p>
name	n/a	(Optional) When creating a stream, you can also specify a name for the stream. <code>1</code> to <code>32</code> characters
encapsulation	ts-rtp	(Optional) The Encapsulation Type for the stream. <ul style="list-style-type: none"> <code>ts-rtp</code> - MPEG2 transport stream over RTP <code>ts-udp</code> - MPEG2 transport stream over UDP (no RTP header) <code>ts-srt</code> - MPEG2 transport stream over SRT (Secure Reliable Transport)
decoderId	n/a	The decoder SDI output port selected for the stream. <code>0</code> to <code>3</code> <div style="border: 1px solid #ccc; padding: 5px;"> <p>i Important</p> <p>Decoder 0 has highest priority, and the video decoding resources are prioritized with the lower decoder numbers (i.e., 0, then 1, 2, and 3) having higher priority. For more information, see Oversubscription of Decoder Channels.</p> </div>

sourceaddr	n/a	(Multicast streams only) Enter the multicast sender IP address in dotted-decimal format (i.e., what address is broadcasting). See "Source Address" under Stream Settings .
ts-rtp only		
FEC	None	(Optional) To enable Forward Error Correction (FEC), specify <code>fec=yes</code> . FEC varies with the protocol (encapsulation): <ul style="list-style-type: none"> • TS over UDP = VF FEC • TS over RTP = Pro-MPEG FEC NOTE: VF FEC is a proprietary FEC and is not interoperable with devices outside of the Haivision family. The FEC level is read from the encoded stream.
ts-srt only		
latency	125	Specifies how long the decoder will buffer received packets, from 20-8000 ms. See "Latency" under SRT Stream Settings .
passphrase	n/a	(Optional) A sequence of words or other text used to control access to the stream. Similar to a password in usage, but is generally longer for added security. This parameter is required if the stream is encrypted and is used to retrieve the cryptographic key protecting the stream. From 10-79 characters.
rejectunencrypted	yes	(Listener Connection mode only) For security reasons, when encryption is enabled in the decoder's SRT Listener stream configuration, this option causes the decoder to reject all unencrypted SRT Caller streams.
mode	listener	Specifies the SRT Connection Mode (to simplify firewall traversal): <ul style="list-style-type: none"> • <code>caller</code> : The SRT stream acts like a client and connects to a server listening and waiting for an incoming call. • <code>listener</code> : The SRT stream acts like a server and listens and waits for clients to connect to it. • <code>rendezvous</code> : Allows calling and listening at the same time. Also, to simplify firewall traversal, Rendezvous Mode allows the encoder and decoder to traverse a firewall without the need for IT to open a port.
sourceport		<div style="border: 1px solid #FFD700; padding: 5px;"> <p> Note This simplifies firewall configuration as the firewall/NAT rules can be precisely tailored to the SRT stream.</p> </div>
SRT to UDP Stream Conversion (ts-srt only)		
flipaddr	n/a	Specifies the destination IP address for the stream. See "SRT to UDP Stream Conversion (TS over SRT only)" under SRT Stream Settings .
flipport	n/a	Specifies the UDP source port for the stream.
flipttl	64	(Time-to Live for stream packets) Specifies the number of router hops the stream packet is allowed to travel/pass before it must be discarded. <code>1..255</code>
fliptos	184 or 0xB8	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range = <code>0..255</code> (decimal) or <code>0x00..0xFF</code> (hex)

stream Examples

```
# stream create addr=10.6.230.106 port=2000 name=infodev
```

Creates a streaming session from IP Address 10.6.230.106 at port 2000. Returns a confirmation such as:
Stream created successfully - ID: 1.

```
# stream 1 start
```

Starts the the stream and its associated decoder. Returns a confirmation such as:
Stream started successfully.

```
# stream 1 get all
```

Returns configuration information for decoder stream #1, such as:

```
Stream ID      : 1
Name          : (None)
Configuration
  Address      : 10.65.135.55
  UDP Port     : 3436
  Decoder      : 0
  Encapsulation : TS-SRT
  Mode         : Rendezvous
  AES Encryption : On
  Latency      : 250 ms
  Stream Flipping : Off
Statistics:
  State        : ACTIVE
  Up Time      : 8m21s
  Source Address : 10.65.135.55 port 3436
  Bit Rate     : 5.87Mbps
  Received Packets : 53,460 (Last One: 0s ago)
  Received Bytes  : 382,894,959
  Connections   : 1 (Last One: 8m20s ago)
  Program Number : 1
  PCR PID       : 34
  Streams       : 2 (1 video, 1 audio, 0 KLV, 0 filtered)
SRT Stats
  Local Version  : 1.3.2
  Peer Version   : 1.3.2
  Connections    : 1
  Local Port     : 3436
  Remote Port    : 3436
  AES Encryption : On
  Key Length     : 128 bits
  Decryption     : Active
  Sent ACKs      : 32,573
  Link Bandwidth : 161,005 kbps
  RTT            : < 1 ms
  Local Buffer Level : 222 ms
  Latency        : 250 ms
```

```
# stream 1 get stats
```

Returns status information for decoder stream #1, such as:

```
Stream ID      : 1
Name           : (None)
Statistics:
  State        : Streaming
  Output       : DECODER-1
  Up Time      : 2d4h42m4s
  Bitrate      : 6,149 kbps
  Received Packets : 20,260,289
  Received Bytes : 1,479,361,480
  Received Errors : 0
  Last Received  : 0s ago
  Stream PCR    : 0x1f9c7ab31
  MPEG2TS Lost Packets : 4
  Corrupted Frames : 2
  Pauses       : 0
  Source Address : fd00:10:65:132:5e77:57ff:fe00:ae6a
```

```
# stream 1 delete
```

Deletes Stream #1.

Related Topics

- [Configuring Streams](#)
- [Stream Settings](#)

temperature

The `temperature` command is used to display the current temperature of the unit.

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 1s ago
  Maximum Temperature  : 48 Celsius measured 20m48s ago
  Minimum Temperature  : 45 Celsius measured 20m48s ago
```

Administration Commands

- `account`
- `audit`
- `banner`
- `certificate`
- `config`
- `date`
- `emspair`
- `ethercfg`
- `haiversion`
- `ipconfig`
- `ipv6config`
- `license`
- `messages`
- `nmcfg`
- `package`
- `passwd`
- `policy`
- `pubkey`
- `reboot`
- `service`
- `system_snapshot.sh`

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.
lock	Locks the user account (if Enabled).
unlock	Unlocks the user account (if Locked).

Action	Description
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: <ul style="list-style-type: none"> 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. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Tip Connect to the audit server in verbose mode to help diagnose connection or certificate problems.</p> </div>

Parameters

Parameter	Default	Description/Values
server	n/a	<p>The server IP address. Enter an IP address in one of the following formats:</p> <ul style="list-style-type: none"> fqdn[:port] ipv4_addr[:port] [ipv6_addr][:port] <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>When configuring an IPv6 server, the address must be enclosed in square brackets.</p> </div> <ul style="list-style-type: none"> hostname[:port]
transport	UDP	<p>The transport protocol, either:</p> <ul style="list-style-type: none"> UDP (User Datagram Protocol): Default UDP port = 514 TLS (Transport Layer Security): Default TLS port = 6514
trusted	All	<p>If transport is TLS, the type of server authentication:</p> <ul style="list-style-type: none"> All : No server authentication CA-signed : Root-CA certificate imported Self-signed : Fingerprint
fingerprint	n/a	<p>If trusted is self-signed, specify the audit server certificate fingerprint (md5 or sha1):</p> <ul style="list-style-type: none"> md5-fingerprint: sha1-fingerprint:

Example

```
# audit get
```

Returns audit server configuration information, such as:

Configuration:

```
Audit server address : syslog.example.com:10533
Transport            : TLS
Trusted servers      : CA-signed
```

Related Topics

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

banner

Note

In the current release, banners uploaded from the CLI will only show from the CLI.

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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important</p> <p>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.</p> </div>
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. <div data-bbox="500 1472 529 1507" style="float: left; margin-right: 5px;"></div> <div data-bbox="544 1472 609 1503">Note</div> <div data-bbox="544 1518 1468 1606">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.</div>
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.
verify	Verifies the validity of the specified certificate.

Parameters

Parameter	Default	Description/Values
sign	self	The signature type for the certificate: <ul style="list-style-type: none"> <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: <ul style="list-style-type: none"> <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: <ul style="list-style-type: none"> <code>/C</code> Two Letter Country Name <code>/ST</code> State or Province Name <code>/L</code> Locality Name <code>/O</code> Organization Name <code>/OU</code> Organizational Unit Name <code>/CN</code> Common Name
type	id	The type of certificate to either import or generate: <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Note</p> <p>Only ID certificates can be generated. Chain and CA certificates can only be imported.</p> </div> <ul style="list-style-type: none"> <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: <ul style="list-style-type: none"> <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>px</code> : PKCS#12 <code>der</code> : Distinguish Encoding Rules
infile	N/A	The name of the file to import. <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Note</p> <p>The administrator has previously downloaded/uploaded the certificate file to import in its home directory (using SCP, for example).</p> </div>

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.

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]
config delete [cfgname, all]
config list
```

Actions

Action	Description
save	Saves the current configuration. Saves every parameter in the system, including encoder or decoder settings and stream destination and status (excluding the system IP address). All configuration files are stored in <code>/usr/share/haivision/config</code> . See the note below in <code>cfgname</code> description. Using <code>config save</code> with no other parameters stores the current settings as the startup configuration using a default name of <code>haistartup.cfg</code> . When saving a named configuration, using the <code>overwrite</code> option prevents a prompt for confirmation when a configuration with the same name already exists.
load	Loads a previously saved configuration identified by <code><cfgname></code> . Reassigns every parameter in the system, including encoder or decoder settings and stream destination and status (excluding the system IP address).
delete	Deletes a previously saved configuration identified by <code><cfgname></code> . If no filename is specified, the system deletes the default configuration (<code>haistartupcfg.ini</code>).
list	Displays a list of the available configuration files.
help	Displays usage information for the <code>config</code> command.

Parameters

Parameter	Default	Description/Values
cfgname	n/a	<p>Note</p> <p>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:</p> <ul style="list-style-type: none"> • Single Quote ` • Ampersand & • Parentheses (or) • Semicolon ; • Apostrophe ' • Double Quote " • Left and Right Angle Brackets < or >
startup	no	Sets saved configuration as the startup configuration. <code>yes, no</code>

Examples

<pre># config save Class430 startup=yes</pre> <p>Saves the current configuration under the name "Class430" and sets it to be the startup configuration.</p>
<pre># config load Class430</pre> <p>Loads a previously saved configuration identified by the name "Class430" (located in the active (local) directory).</p>

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

- [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 CIqn9+kFUncKDDEwLjY1LjExLjE4NxCzRVJkCkBmZTB1MD
A1ZGYyNmM3MmI4MmY0Njc1ODUzZGQ3MDhhZDk4MWE2NGJjNDEyODliNDNlMDAxYzJjNTJmMmZhODZhEi
A4N2YyM2ZkNi1kNGEyLWExNGYtNzNhZi0yMjliNmRiZA==
```

Pairing configuration:

Expires: Sun Jul 28 16:55:38 2019

Server: 10.65.11.187:8883

* Starting operation...
* Waiting for completion...
* Operation completed successfully!

Status Report:

Last State: PAIRED
Server: 10.65.11.187:8883
Device ID: 26637ed0-7a22-ab4f-71bf-baf4dc59
Enabled: Yes
Waiting To Unpair: No

```
# emspair unpair
* Starting operation...
* Waiting for completion...
* Operation completed successfully!
```

Status Report:

Last State: UNPAIRED
Server: (None)
Device ID:
Enabled: Yes
Waiting To Unpair: No

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

Status Report:

Last State: PAIRED
Server: 10.66.131.132:8883
Device ID: 37a1de75-4aac-bf4f-70bf-ee7f66dc
Enabled: Yes
Waiting To Unpair: No

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

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

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

Reconnect Delay 5 sec
```

Related Topics:

- [Pairing the Decoder with Haivision EMS](#)

ethtool

The `ethtool` 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.

```
ethtool
Speed           : 1000mbps
Duplex          : Full
Auto-Negotiation : On
Advertised Mode : All
Link Detected   : Yes
Ceiling         : 1000000kbps
```

Synopsis

```
ethtool [-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

```
# ethtool -s 100
Sets the line speed to 100 Mbps (which also modifies the advertised mode, see example below).
# ethtool -s 100
Speed          : 100mbps
Duplex         : Full
Auto-Negotiation : On
Advertised Mode : 100mbps Full-Duplex
Link Detected  : Yes
Ceiling        : 100000kbps

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

Related Topics

- [Configuring Network Settings](#)

haiversion

The `haiversion` command is used to display status information about Makito X Series devices. Status information can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support.

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

 **Tip**

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

Synopsis

```
haiversion
```

Actions

N/A

Parameters

N/A

Example

```
# haiversion

Displays information about the hardware and software components.
Card Type           : "Makito X4 SDI Decoder"
Part Number        : S-MX4D-SDI
Serial Number      : HAI-031950010016
MAC Address        : 5c:77:57:00:e0:be
Firmware Version   : 1.0.0-6
Firmware Date      : "Apr 23 2020"
Firmware Time      : "12:16:51"
Hardware Version   : A
Hardware Compatibility : -002G
CPLD Version       : 4 (Official, Internal flash)
Boot Version       : "U-Boot 2018.01 (Feb 05 2019 - 15:29:26) Makito4K"
```

Related Topics

- [Viewing System Status Information](#)

ipconfig

The `ipconfig` command is used to view and set the parameters that specify the IP (IPv4) networking context for Makito X Series devices, including the IP settings, hostname, and DNS. It may also be used to set the Network Time Protocol (NTP) server address and Time Zone.

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

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

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

Note

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

Warning

If you are connecting to the Makito X Series through an IPv4 connection, disabling the IPv4 interface will drop your connection. You will need to reconnect using IPv6 or the serial interface (if available).

You must reboot for any changes to take effect.

Synopsis

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

Actions

Action	Description
display	Displays the current IP configuration.
configure	Configures IP settings.
renew	Renews DHCP address lease.

Action	Description
release	Releases current DHCP address lease.
disable	Disables IPv4 functionality. Use to configure the device to use IPv6 network only. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note You cannot disable IPv4 if IPv6 is already disabled.</p> </div>

Parameters

N/A

Examples

```
# ipconfig display

Returns current IP settings for decoder that does not use DHCP:
Current IP Settings:
  IP Address           : 10.65.135.35
  Network Mask         : 255.255.255.0
  Gateway              : 10.65.135.1
  Hostname              : MX4D-HAI-test
Current DNS Settings:
  Domain                : haivision.com
  Primary Server        : 10.65.0.11
  Alternate Server      : 10.65.0.13
  DNS Resolve Precedence : IPv6
Current Multicast DNS (mDNS) Settings:
  Responder             : Enabled
  Identifier             : "MX4D-HAI-test"
Current NTP Settings:
  Server                : 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 Decoder"
DHCP Client Retries  : 3
DHCP Client Timeout  : 3 secs

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 Decoder"):
Configure advanced DHCP client parameters (retries and timeout)? (y,N): y
DHCP Client Retries (1 - 100): 3
DHCP Client Timeout (1 - 60) : 3

Current Hostname      : MX4D-HAI-2
Change hostname? (y,N):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):N

Current Multicast DNS (mDNS) Settings:
Responder             : Enabled
Identifier            : "MakitoX4D HAI--2"
Change Multicast DNS Settings? (y,N):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!
```

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. <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 5px;"> <p>Note You cannot disable IPv6 if IPv4 is already disabled.</p> </div>

Parameters

N/A

 **Tip**

For descriptions of the parameters that follow, see [Network Settings](#).

Example

```
# ipv6config display

Returns current IPv6 settings for a decoder configured to use IPv6:
Current configured IPv6 Settings:
  Global IPv6 Address : fd00:10:65:135::1297/128
  Global IPv6 Address : fd00:10:65:135:5e77:57ff:fe00:e0be/64
  Link-Local IPv6 Address : fe80::5e77:57ff:fe00:e0be/64
  Gateway Address : fe80::2efa:a2ff:febl:a959
  Hostname : MX4D-test
Current DNS Settings:
  Domain : haivision.com
  Primary Server : 8.8.8.8
  Alternate Server : 8.8.4.4
  DNS Resolve Precedence : IPv6
Current Multicast DNS (mDNS) Settings:
  Responder : Enabled
  Identifier : "MX4D-test"
Current NTP Settings:
  Server : ca.pool.ntp.org
  Timezone : "America/Montreal"
```

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. <div data-bbox="500 1283 1495 1465" style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>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.</p> </div>
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):
QA-MX4D-Full.lic
```

```
# license info all
```

Displays options information for the license file:

```
[L1] QA-MX4D-Full.lic: Ok
System:
  Maximum Upgradable Release      9.9
  Firmware Expiration Date        Never
Audio/Video Outputs:
  Number of decode channels        4
  Maximum output resolution        HD
Video:
  High Efficiency Video Coding (H.265) On
  Maximum Video Bit Depth          10
  Maximum Video Color Subsampling  4:2:2
Metadata:
  Key-Length-Value (KLV)          On
Stream:
  Secure Reliable Transport (SRT)  On
```

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

Tue Jun 9 11:56:34 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Tue Jun 9 11:56:53 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Tue Jun 9 12:33:50 EDT 2020: There were 3 failed login attempts on the admin account since the
last successful login.
Tue Jun 9 16:05:00 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Tue Jun 9 16:12:55 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Tue Jun 9 16:27:19 EDT 2020: Software package makitox4_dec_v1.0.0-35.hai was successfully
installed.
Tue Jun 9 16:35:02 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Wed Jun 10 10:08:49 EDT 2020: There was 1 failed login attempt on the admin account since the
last successful login.
Wed Jun 10 10:31:57 EDT 2020: Software package makitox4_dec_v1.0.0-36.hai was successfully
installed.
Wed Jun 10 10:40:30 EDT 2020: There was 1 failed login attempt 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	<p>Defines the access permissions for the community or the user.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Info</p> <p>Access permissions may be additive. For example, permitting a new source for an existing community adds to the existing one if it complements it.</p> </div>
delete	Deletes the specified object.
help	Displays usage information for the command, or if specified, the option.

 **Note**

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

Parameters

N/A

Example #1: Initializing a Community-Based (v1/v2c) System

In the example below, a system with default settings is configured to add a distant host access (198.51.100.122) to the existing localhost and localnet accesses of the admin community. Note that the localnet source is a special keyword that translates at runtime to the network settings of the LAN interface. System parameters are also defined. Both IPv4 and IPv6 are enabled.

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

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

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

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

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

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

Example #2: Creating an SNMPv3 User

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

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

Example #3: Initializing a USM-only (SNMPv3) System

In the example below, system security is enforced by completely disabling SNMPv1/v2c access, and by requiring v3 USM authentication only for users group-based access, and encryption for admins and operators group-based access. Both IPv4 and IPv6 are enabled.

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

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

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

# nmcfg agent stop

# nmcfg system define contact "joe net <jnet@example.org>"

# nmcfg system define location "Media Lab"

# nmcfg community delete admin

# nmcfg community delete public

# nmcfg user define joenet SHA "arfds23dsjs" AES "2394urscxkvn"
nmcfg: snmp agent is not running, user settings will apply when started

# nmcfg user define johnsmith SHA "89ss5dkj" AES "jfdsf78998sd"
nmcfg: snmp agent is not running, user settings will apply when started

# nmcfg user define guest MD5 "nososecret"
nmcfg: snmp agent is not running, user settings will apply when started

# nmcfg access usm permit joenet administrator priv

# nmcfg access usm permit johnsmith operator priv

# nmcfg access usm permit guest guest

# nmcfg agent start
Starting SNMP Service

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

system parameter	value				
engineid	0x80001f88035c775700b3dc				
contact	joe net <jnet@example.org>				
location	Media Lab				
model	perm/group	level	user/community	af	source
usm	guest	auth	guest	-	-
usm	administrator	priv	joenet	-	-
usm	operator	priv	johnsmith	-	-
auth protocol	priv protocol	user			
MD5	nopriv	guest			
SHA	AES	joenet			
SHA	AES	johnsmith			

Related Topics

- [SNMP Agent Components](#)

package

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

Note

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

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

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

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

Synopsis

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

Actions

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

Parameters

N/A

Example #1: Package Download and Installation

```
# package download makitox_enc_v2.2.0-59.hai mytftp.example.com
1/5) Temporarily pausing encoder(s)...
2/5) Downloading package makitox_enc_v2.2.0-59.hai from mytftp.example.com...
3/5) Verifying integrity of downloaded package...Package verified successfully.
4/5) Synching file system...
5/5) Resuming encoder(s)...
Package downloaded successfully.

# package install makitox_enc_v2.2.0-59.hai
Package makitox_enc_v2.2.0-59.hai will be installed on next boot sequence.
You must REBOOT to complete the update process!
```

Example #2: Package Download Verification Failure

```
# package download makitox_enc_v2.2.0-59.hai mytftp.example.com
1/5) Temporarily pausing encoder(s)...
2/5) Downloading package makitox_enc_v2.2.0-59.hai from mytftp.example.com...
3/5) Verifying integrity of downloaded package...Package verification failed!
Try downloading the package again.
```

Examples (General)

```
# package list

Displays the list of downloaded packages:
Package Files (in /usr/share/haivision/packages/):
  makitox_enc_v2.2.0-59.hai
  makitox_enc_v2.2.0-58.hai
```

```
# package info makitox_enc_v2_2_0.hai

Displays information about the package.
```

```
# package install makitox_enc_v2_2_0.hai

Installs the package.
```

Related Topics

- [messages](#) (CLI command)

passwd

The `passwd` command is used to change your own password.

Note

To modify the password for other users' accounts, see the `account` CLI command (link below). Passwords can be up to 80 characters long. See "Password Requirements" under "Changing Your Password" (link below) for the supported character set. Password policies set by the administrator may enforce the selection of strong passwords.

Synopsis

```
passwd
```

Actions

N/A

Parameters

N/A

Examples

```
# passwd
```

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

Related Topics

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

policy

The `policy` command is used to configure and manage security policy settings 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	<p>Specifies the required cryptographic compliance, either:</p> <ul style="list-style-type: none"> • 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 <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p> Note Either selection reinforces security for all management functions of the device in terms of cryptography. This setting takes effect upon the next reboot.</p> </div>
ssl3	See Note	<p>Enables or disables SSLv3 as a supported TLS version: Yes, No</p> <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p> 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.</p> </div>
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	<p>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.</p> <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p> Note When preparing a Makito X Series device for hardening, you need to enable the HSTS policy.</p> </div>
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	<p>Specifies the number of days (since the last login) after which the user account will be disabled: 1..365 days</p> <p>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.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p> Tip The system adds one (1) day (or 24hour grace period) to the setting configured by the user.</p> </div>
password		
quality	Basic	<p>Specifies the required password strength, either:</p> <ul style="list-style-type: none"> • Basic • Strong
minlen	6	Specifies the minimum password length. Range: 6..40
minupper	See Note	<p>(quality must be Strong) Specifies the minimum number of uppercase letters. Range: 0..40</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p> Note Default is N/A if quality=Basic, 0 if quality=Strong.</p> </div>
mindigits	See Note	<p>(quality must be Strong) Specifies the minimum number of digits. Range: 0..40</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p> Note Default is N/A if quality=Basic, 0 if quality=Strong.</p> </div>
minsymbols	See Note	<p>(quality must be Strong) Specifies the minimum number of symbols. Range: 0..40</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p> Note Default is N/A if quality=Basic, 0 if quality=Strong.</p> </div>
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		
autologout	No	<p>Enables or disables Auto-Logout after the specified length of time: Yes, No</p> <div style="border: 1px solid yellow; padding: 5px; margin-top: 10px;"> <p> Note Enabling the Auto-Logout Session policy also limits the number of concurrent sign-ins per account to 4.</p> </div>

Parameter	Default	Description/Values
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

```
# policy crypto set compliance=NDPP11
Sets the required cryptographic compliance to Network Device Protection Profile v1.1.

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

# policy all get
Returns policy information for the Makito 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 Decoder](#)

service

For security purposes, you may need to stop one or more network services from accessing the Makito X4. The service command is used to enable and disable the following decoder network services: all, or (depending on the platform) EMS, HTTP, SNMP, SSH, and TELNET.

⚠ 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, snmp, ssh, telnet
```

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, 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
snmp service is currently enabled
snmp service is enabled at system startup
ssh service is currently enabled
ssh service is enabled at system startup
telnet service is currently enabled
telnet service is enabled at system startup
```

```
# service
```

Displays usage information for the service command .

Usage: service svcname action

svcname can be: all, ems, http, 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 X4.

```
# service telnet restart
```

Re-starts telnet connections to the Makito X4.

Related Topics

- [Enabling and Disabling Network Services](#)
- [Services Settings](#)

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](#)

Technical Specifications

This appendix lists the technical specifications for the Makito X4 decoder.

Topics Discussed

- [Audio/Video Interface Specifications](#)
- [Video Decoding](#)
- [Audio Decoding](#)
- [Advanced Features](#)
- [Metadata \(Optional\)](#)
- [Network and Management Interfaces](#)
- [Chassis Options](#)
- [Power Connector Pinouts \(Single-Height Chassis\)](#)
- [Regulatory/Compliance](#)

Audio/Video Interface Specifications

[Video Interfaces](#) [Audio Interfaces](#)

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

[Video Interfaces](#) [Audio Interfaces](#)

Digital Embedded Audio		
SD-SDI	SMPTE-272M	Formatting AES/EBU Audio and Auxiliary Data into Digital Video Ancillary Data Space
HD/3G-SDI	SMPTE 299M	Formatting 24-Bit Digital Audio Format for SMPTE Bit-Serial Interfaces

Video Decoding

Video Decoding - H.264 AVC/H.265 HEVC (MPEG-4 Part 10)	
Output Video Resolutions	<ul style="list-style-type: none"> • 3840x2160p 60/59.94/50/30/29.97/25 HZ • 1920x1080p 60/59.94/50/30/29.97/25/24/23.98 HZ • 1920x1080i 60/59.94/50 HZ • 1280x720p 60/59.94/50/30/29.97/25 HZ (interlaced show in fields per second) No scaling capabilities
H.264/AVC Video Decoding	<ul style="list-style-type: none"> • MPEG-4 AVC part 10 / ISO/IEC 14496-10 • Baseline, Main and High Profiles up to Level 5.2 • I, IP, IBP, IBBP, IBBBBP, IBBBBP framing • 8-bit or 10-bit pixel depth • Chroma sub-sampling 4:2:0 or 4:2:2
H.265/HEVC Video Decoding	<ul style="list-style-type: none"> • ISO/IEC 23008-2 • Baseline, Main and High Profiles up to Level 5.1 • I, IP, IBP, IBBP, IBBBBP, IBBBBP framing • 8-bit or 10-bit pixel depth • Chroma sub-sampling 4:2:0 or 4:2:2
Video Decoding	Configurable output frame rate

Additional Video Decoding Specifications

- Video elementary streams may contain one HEVC or H.264 coded video ES.
- Field coded, frame coded, MBAFF and PAFF coded frames are supported.
- The GOP size may vary from 1 to 1000.
- Open or Closed GOP is supported.
- Intra-refresh is supported providing the ability to tune into a stream at any random access point.
- CAVLC or CABAC coding is supported for H.264.
- The following interlaced or progressive coded picture resolutions are supported for HEVC/H.265: 480i, 576i, 720p, 1080i, 1080p, 2160p.

! Important

Video Decoding Limitations: The Makito X4 decoder does *not* support decoding H.264 interlaced video coded pictures.

Audio Decoding

Audio Decoding	
Audio Channels	Up to 16 stereo pairs per blade (SDI)
Audio Bitrates	Mono: 56 to 160 kbps per audio pair Stereo: 80 to 320 kbps per audio pair
Frequency Response	From 20 Hz to 22 kHz
Compression Standards	MPEG-2 AAC-LC ISO/IEC 13818-7 MPEG-4 AAC-LC ISO/IEC 14496-3

Advanced Features

Advanced Features
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
SMPTE 2016 AFD (Active Format Description for SDI)
Timecode Support (SMPTE 12M)
Advanced Buffering Control
Still Image Insertion
Synchronized playback between decoders

Metadata (Optional)

Metadata Outputs
<ul style="list-style-type: none"> • KLV over SDI (SMPTE 336) • SMPTE 336M compliant • MISB 0601.10 compliant • MISB 0604.2 compliant, supporting: <ul style="list-style-type: none"> • 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) • Time Code Support (SMPTE 12M) • CTA-608/SDI and CTA-708/SDI Closed Captioning as per SMPTE 334-1/2

Network and Management Interfaces

[IP Network Interfaces](#) [Management Interfaces](#)

IP Network Interfaces

Standard	<ul style="list-style-type: none"> • Single Ethernet 10/100/1000 • Base-T, auto-detect, Half/Full-duplex • Unicast streaming IPv4/IPv6 • Multicast unicast streaming (IGMPv3, Internet Group Management Protocol and IPv6) • 10G SFP+ Port (future use)
Streaming Protocols	<ul style="list-style-type: none"> • MPEG-TS over UDP • MPEG-TS over RTP • Secure Reliable Transport (SRT)
Advanced Streaming Features	<ul style="list-style-type: none"> • AES encryption 128-bit or 256-bit • SRT Latency Control • Still image insertion on loss of stream • Forward Error Correction (FEC)

[IP Network Interfaces](#) [Management Interfaces](#)

Management Interfaces

Physical Interface	<ul style="list-style-type: none"> • IP/Ethernet (IPv4 and IPv6)
Management Protocols	<ul style="list-style-type: none"> • HTTPS (Web browser) • Command line over SSH/Telnet • SFTP/TFTP/SCP Client/Server • SNMP v1, v2c, and v3 • Haivision EMS (option)

Chassis Options

Topics in This Chapter

- [Single-Height Appliance](#)
- [MB6X – 6 Blade Chassis](#)
- [MB21X \(#F-MB21X-R\)](#)

Single-Height Appliance

Single Blade Appliance (#S/B-MX4D-SDI4)	
Dimensions (H x W x D)	21mm H x 129mm W x 196mm D (0.83" H x 5.1" W x 7.7" D)
Weight	Appliance (no PSU): Approximately 1.14 kg (2.5 lbs.) Blade with heat sink: Approximately 240 gm (0.529 lbs.)
Power Requirements	12 VDC Nominal, 18W (each blade) <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note IEC 60601-1 Class I and II power supplies are available from Haivision.</p> </div>
Power Connector	On unit: Conxall p/n 17282-3PG-300 Mating connector: Conxall p/n 16282-3SG-318
Temperature**	Operating: 0°C to 40°C (32°F to 104°F) Non-operating*: -30°C to 70°C (-22°F to 158°F) *Limited by the power supply storage: -30°C **Ambient environmental temperature
Relative Humidity	Up to 95% without condensation
Heat	20 Watts or 68.3 BTU/hr
Sound Emission	41.2 dB(A) L'p(AVG)

Compatible with Haivision MB6X and MB21X multi-blade chassis.

Related Topics

- [Install the Decoder](#)
- [Power Connector Pinouts \(Single-Height Chassis\)](#)

MB6X – 6 Blade Chassis

MB6X - 6-Blade Chassis (#F-MB6X-RAC, #F-MB6X-MED, #F-MB6X-DC)	
Dimensions (H x W x D)	19" rack mountable, 1 RU 44.069mm H x 440.004mm W x 420.37mm D (1.735" H x 17.323" W x 16.55" D) Tolerances are +/-0.50mm (+/- 0.020in.)
Weight	6 slot empty chassis: 7.94 kg. (17.5 lbs.) Single blade: Approximately 240 g (0.529 lbs.)

MB6X - 6-Blade Chassis (#F-MB6X-RAC, #F-MB6X-MED, #F-MB6X-DC)	
Power Requirements	Single Internal Power Supply: <ul style="list-style-type: none"> • F-MB6X-RAC (Redundant AC type): 90-264VAC 47Hz-63Hz • F-MB6X-MED (Medical Grade): 90-264VAC 47Hz-63Hz • F-MB6X-DC (DC type): 20-36 VDC 300 watt maximum (all types)
Temperature	Operating: 0°C to 50°C (32°F to 122°F) Non-operating: -40°C to 70°C (-40°F to 158°F)
Relative Humidity	Up to 95% without condensation
Heat	155 Watts or 530 BTU/hr
Sound Emission	<ul style="list-style-type: none"> • Room temperature: 57.0 dB(A) L'p(AVG) • 50°C Ambient: 65.9 dB(A) L'p(AVG)

MB21X (#F-MB21X-R)

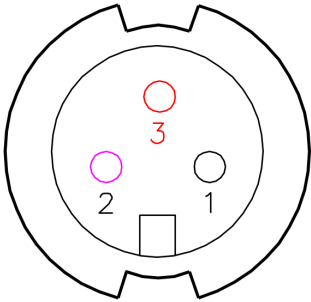
MB21X - 21-Blade Chassis (#F-MB21X-R)¹	
Dimensions (H x W x D)	19-inch rack mountable, 4RU *177.29 mm H x +441.35 mm W x 461.92 mm D (6.980 inches H x 17.376 inches W x 18.186 inches D) *186.76 mm / 7.353 inches H with rubber feet installed +482.60 mm / 19.000 inches W including mounting flanges
Weight	Empty 21-slot chassis: 32.5 pounds Single blade: Approximately 240 gm (0.529 lbs.)
Power (internal power supply)	Dual redundant power supplies: <ul style="list-style-type: none"> • 100-240VAC 47Hz-63Hz • 600 watt maximum per PSU
Temperature	Operating: 0°C to 50°C (32°F to 122°F) Non-operating: -40°C to 70°C (-40°F to 158°F)
Relative Humidity	Up to 95% without condensation
Heat	560 Watts or 1910 BTU/hr *assumes chassis full of Makito X Series blades
Sound Emission	<ul style="list-style-type: none"> • Room temperature: 56.4 dB(A) L'p(AVG) • 50°C Ambient: 63.3 dB(A) L'p(AVG)
Advanced Features	<ul style="list-style-type: none"> • Removable fan trays • Station Alarm Interface

1. Supports Makito X/X4 products *only*; excludes classic Makito encoder/decoder or Torpedo blades

Power Connector Pinouts (Single-Height Chassis)

The power connectors for the Single-Height Chassis have the following pinout:

Single-Height - Power Connector

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

Regulatory/Compliance

Regulatory/Compliance	
Certification	UL / CSA / CE
Compliance	Electromagnetic Compatibility: EN 55022 (Emissions) / 55024 (Immunity) / EN 61000-3-2 / EN 61000-3-3
	Safety (Low Voltage Directives): EN 60950-1 (CSA C/US) / IEC/EN 60950-1 (International /CB Scheme)
	Industry Canada Warnings: Canadian ICES-003, "Electromagnetic Compatibility" / Avis d'Industrie Canada: la norme NMB-003 du Canada, "La Compatibilité électromagnétique"
	FCC Part 15, Subpart B, Class A
	STANAG 4609 compliant (NATO Digital Motion Imagery Standard)
Compliance with Environmental Regulations	RoHS2, European Union Directive 2011/65/EU
	RoHS, Marking Control for China, Regulation SJ/T 11364-2006
Acoustic Noise	Telcordia GR-63 Section 4.6, Issue 3

⚠ Note

Please refer to the product Declaration of Conformity (DoC) for complete details.

Accessing the REST API

The Makito X4 decoder Application Programming Interface (API) is a modern Representational State Transfer (REST) API stack that provides all functionality from the Makito X4 Web Interface and is harmonized with other Haivision appliances.

To access the API endpoint documentation, simply type in the IP hostname of your Makito X4 into your browser's address bar, followed by `/apidoc`.

 **Tip**

You can also access the API endpoint documentation on the demo Makito X4 Decoder at: <https://mx4d.demo.haivision.com/apidoc/>

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

Filter... X

1.3.0 ▾

Makito X4 Decoder

REST API doc

Authentication

Authentication - GET - user session /apis/authentication 1.0.0 ▾

GET

/apis/authentication

Success 200

Field	Type	Description
gid	Number	group id
passwordExp	Number	password expired. 0 == valid, 1 == expired
uuid	Number	userid
username	String	username

Success response

```
HTTP/1.1 200 OK
{"username": "admin", "uid": 500, "gid": 511, "passwordExp": 0}
```

Error unauthorized

```
HTTP/1.1 401 Unauthorized
```

Authentication - POST - login /apis/authentication 1.0.0 ▾

POST

/apis/authentication

Success 200

Field	Type	Description
username	String	username
password	String	plain text password (note that the server only accepts request over encrypted HTTPS)

Success response

```
HTTP/1.1 200 OK
data: {username: "admin", uid: 500, gid: 511, passwordExp: 0}
```

Filter...

Authentication

- GET - user session /apis/authentication
- POST - login /apis/authentication

Decoders

- GET - get decoder /apis/decoders/:id
- GET - get decoder stats /apis/decoders/:id/stats
- PUT - start decoder /apis/decoders/:id/start
- PUT - stop decoder /apis/decoders/:id/stop
- PUT - update decoder /apis/decoders/:id

Streams

- DELETE - delete existing stream /apis/streams/:id
- GET - get all streams /apis/streams
- GET - get stream config /apis/streams/:id
- GET - get stream stats /apis/streams/:id/stats
- POST - create new stream /apis/streams
- PUT - edit stream /apis/streams/:id

Multi-channel Synchronization

The Makito X Series Multi-channel Synchronization feature is designed to work in the broadcast industry where remote producers typically capture multiple views of the same content and transport it over a network to a central production facility. All these channels need to be synchronized to within one frame period at the decoders to avoid replay issues on downstream equipment when switching between video and audio sources.

Makito X Series encoders and decoders can be configured to synchronize the output of two or more decoded streams with single frame accuracy. The Multi-channel Synchronization feature works by continuously monitoring the end-to-end transit time and dynamically adjusting the internal decoder buffers to compensate.

This tutorial provides a description of this feature, along with deployment instructions.

Note

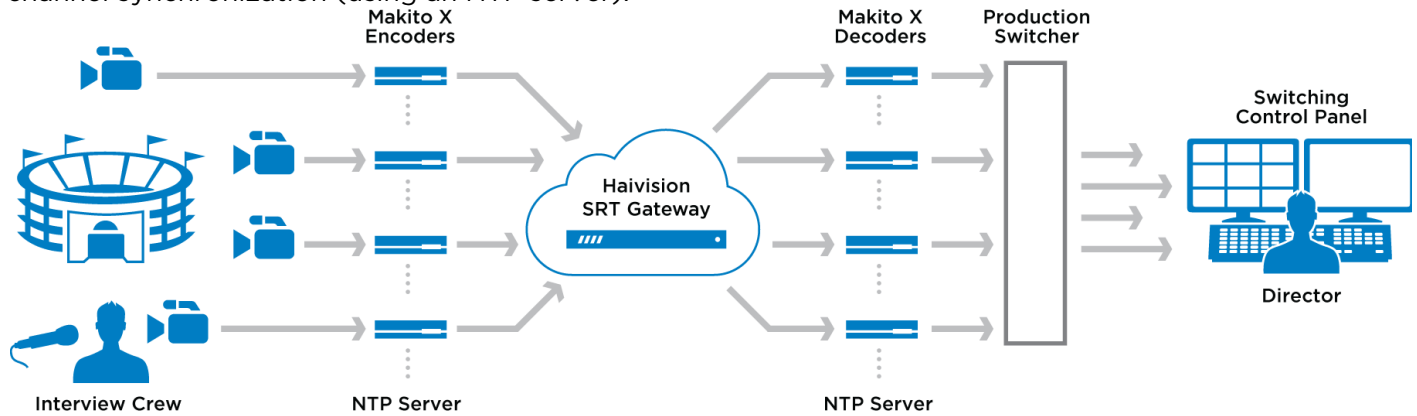
Unless otherwise specified, references to the "Makito X Series" can be taken to include the Makito X and Makito X4 family of encoders and decoders.

Topics Discussed

- [Multi-Sync Overview](#)
- [Step 1: Configure NTP Settings](#)
- [Step 2: Configure Encoder Settings](#)
- [Step 3: Configure Decoder Settings \(Decoder Pass 1\)](#)
- [Step 4: Observe and Measure Delay Ranges \(Decoder Pass 2\)](#)
- [Step 5: Configure MultiSync Delay \(Decoder Pass 3\)](#)

Multi-Sync Overview

The Multi-channel Synchronization feature leverages timecode synchronization to enable users to capture and encode multiple channels of video and audio from a remote venue and stream it to a central production studio. The various channels can be encoded using different codecs, bit rates, frame rates, resolutions, etc. The following diagram shows a sample live production scenario configured for multi-channel synchronization (using an NTP server).



Two or more Makito X Series decoders can synchronize their output by using a frame buffer that holds a frame (or field if the signal is interlaced) momentarily until it falls into alignment with the other channels. This is accomplished by applying a fixed delay (referred to as *MultiSync Delay*) from the time the video is captured or encoded to the time it is ultimately displayed.

Note

There are two approaches to configuring MultiSync Delay/Multi-channel Synchronization:

- **Use timecodes generated by the encoder.** Select “System” as the Timecode Source in the Video Encoder settings (with Counting Mode set to “UTC Conversion”). Also the encoders must be “NTP locked” in order to insert timecodes into the encoded stream based on the System Time.
- **Use timecodes that are pre-synchronized by the upstream equipment and embedded into the SDI signal.** Select “Video” as the Timecode Source in the Video Encoder settings. The cameras must be genlocked and “NTP locked” in order to generate and insert a valid timecode into the video signal. In this case, the video source must generate timecodes that are locked to the same master clock. For information on this, please refer to your camera documentation.

This tutorial recommends the first approach, i.e., to use timecodes generated by the encoder (as explained in the following tutorial step).

Following is a summary of the steps we recommend to configure Multi-channel Synchronization:

1. [Configure NTP Settings](#)
2. [Configure Encoder Settings](#)
3. [Configure Decoder Settings \(Decoder Pass 1\)](#)
4. [Observe Delay Ranges \(Decoder Pass 2\)](#)
5. [Configure MultiSync Delay \(Decoder Pass 3\)](#)

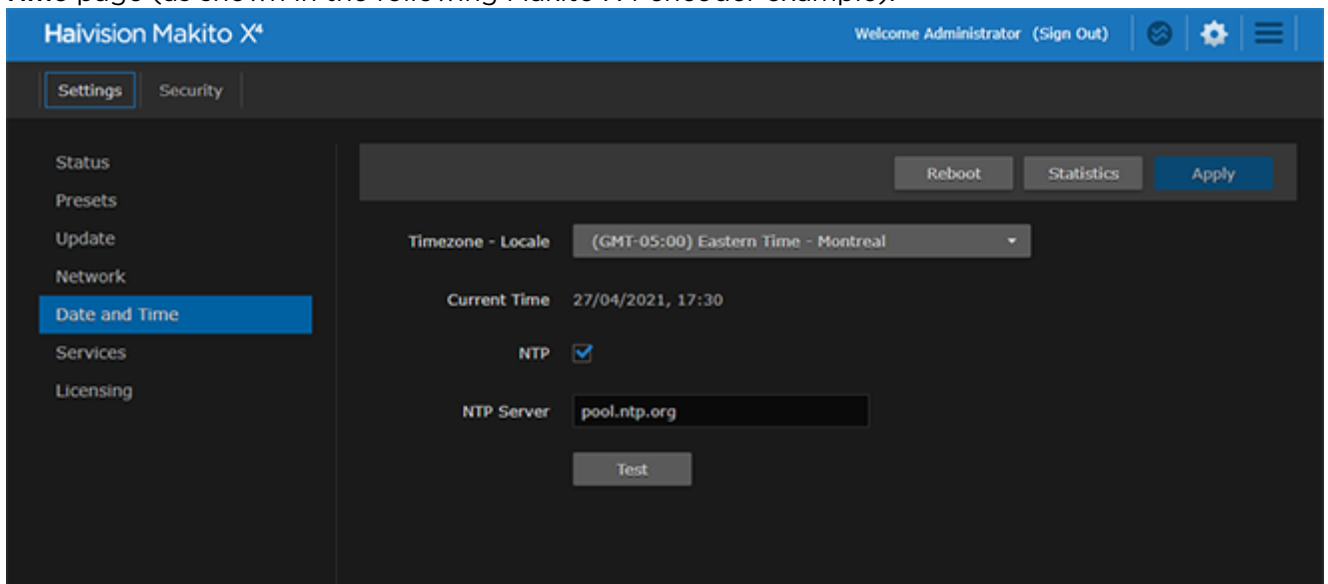
Step 1: Configure NTP Settings

Note

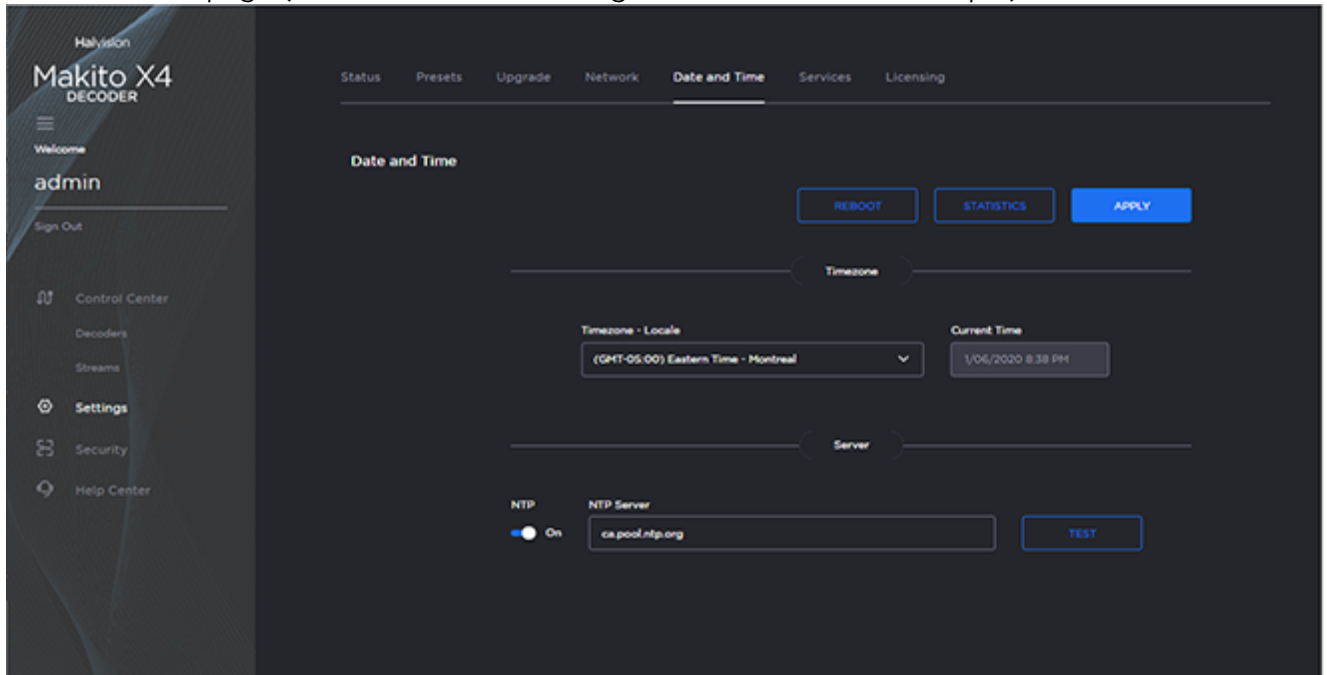
This tutorial recommends that you configure the encoders to use “System” timecodes. This requires that the encoders be “NTP locked” in order to insert timecodes into the encoded stream based on the System Time (as explained in the tutorial step below). Also, where selectable (i.e., on the Makito X4 encoder), set the Counting Mode to “UTC Conversion”.

Configure the encoder and the decoder to use NTP:

1. Configure the encoder to use NTP on the (Web interface) **Administration > Settings > Date and Time** page (as shown in the following Makito X4 encoder example).



- Likewise, configure the decoder to use NTP on the (Web interface) **Administration > Settings > Date and Time** page (as shown in the following Makito X4 decoder example).



- To validate that the NTP server is reachable, be sure to click **Test** (below or next to the NTP server field).
If you do *not* see a green checkmark (indicating that the connection is successful), it is a good idea take a system snapshot and contact Haivision Technical Support.

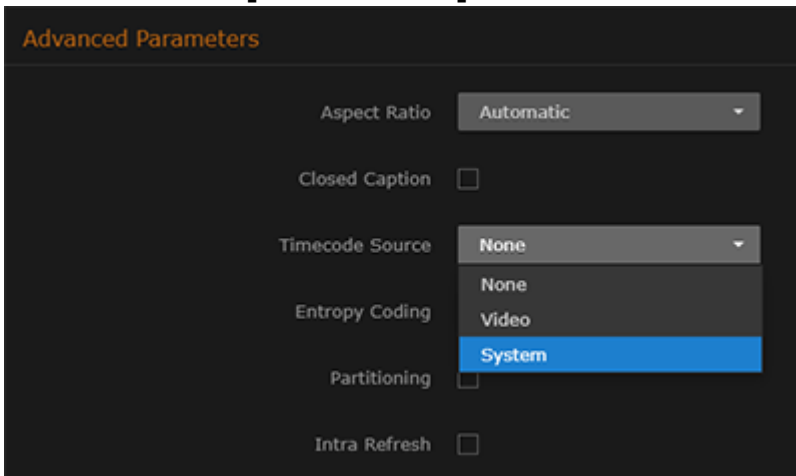
Tip

We recommend an offset - i.e., the difference between the local clock (on the Makito/camera) and remote clock (on the NTP server) - of around 5 ms.

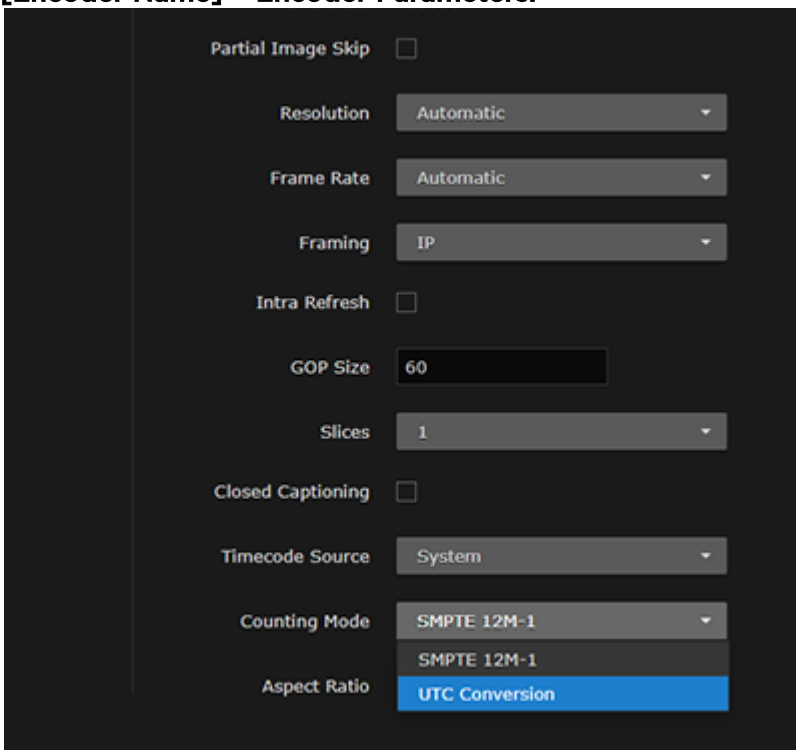
Step 2: Configure Encoder Settings

Next, on the encoders, select the Timecode Source (either embedded SDI, "Video" or their internal clock, "System"), and start the streams. As explained in [Multi-Sync Overview](#), we recommend that you configure the encoder to use timecodes generated by the encoder ("System").

1. Create the streams on the Makito X Series encoders.
2. Configure the Video Encoder settings for multi-sync:
 - On the Makito X encoder, select "System" as the **Timecode Source** under **General Settings > Video Encoders > [Encoder Name] > Advanced Parameters**:



- On the Makito X4 encoder, select "System" as the **Timecode Source** under **Video Encoders > [Encoder Name] > Encoder Parameters**.



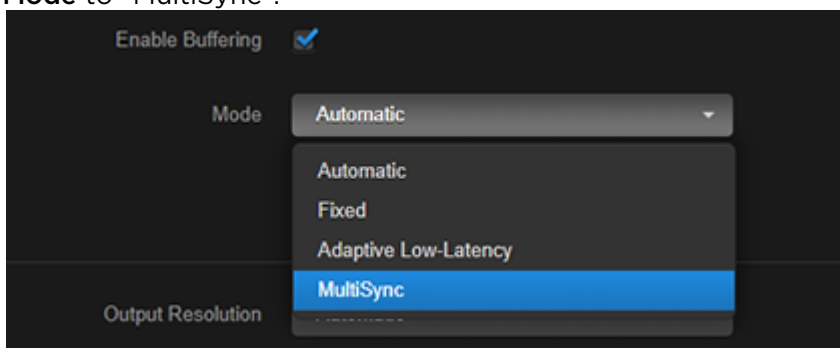
- On the Makito X4 encoder, select "UTC Conversion" as the **Counting Mode**.

3. Start the stream outputs on all the encoders.

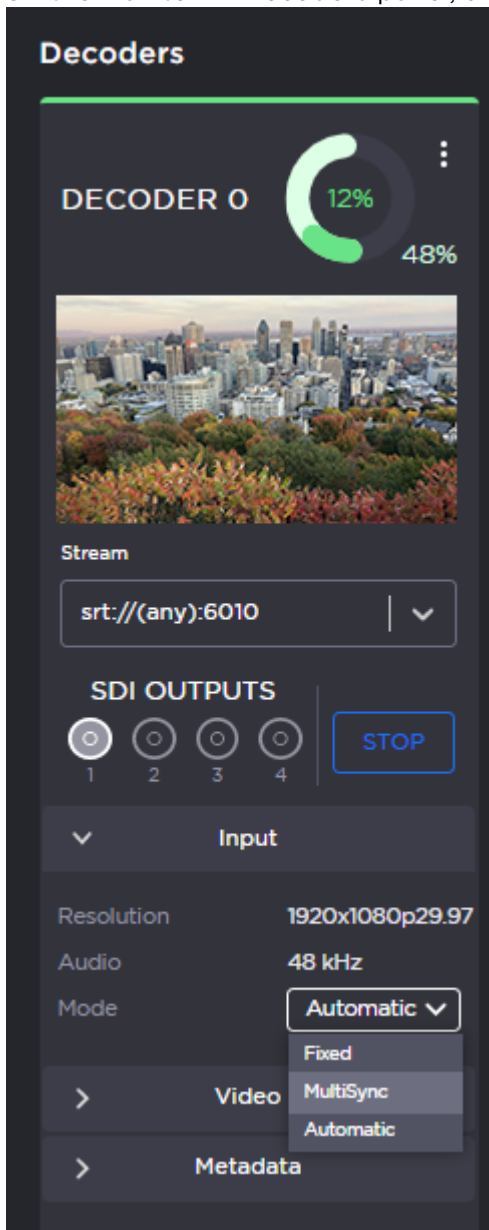
Step 3: Configure Decoder Settings (Decoder Pass 1)

Configure the decoders to receive the streams, specifying MultiSync as the Buffering Mode:

1. Configure the Makito X Series decoders to receive the streams.
2. For each decode channel to be synchronized, select MultiSync for the buffering Mode.
 - On the Makito X SDI 1 or SDI 2 Decoder page, check the **Enable Buffering** checkbox, and set the **Mode** to “MultiSync”.



- On the Makito X4 Decoders panel, under **Input**, set the **Mode** to “MultiSync”.



3. Initially, enter a value such as the default (1000ms) for the **MultiSync Delay**.

Tip

For streams configured with SRT, enter the negotiated SRT latency value for the MultiSync Delay. In many cases, this will already fall within the acceptable MultiSync Delay Range.

4. Start the stream reception on all the decoders.

Step 4: Observe and Measure Delay Ranges (Decoder Pass 2)

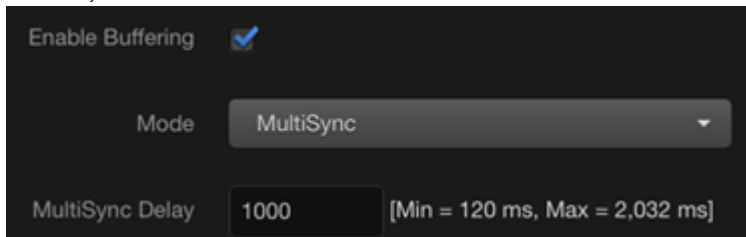
Step 4: Measure (Decoder Pass 2)

Once a decoder starts receiving a stream, it gathers and computes various statistics. It then displays a range of possible **MultiSync Delay** ranges (e.g., “Min = 120 ms, Max = 2,032 ms” on the Makito X).

To observe Delay Ranges, wait 20 to 30 seconds while the decoder starts receiving the stream and gathering statistics. Then examine the MultiSync Delay Range on each of the decoders.

Makito X Decoder

1. On the Makito X SDI 1 or SDI 2 Decoder page, either open the Statistics pane or check beside the MultiSync Delay field, and you will see a range of valid multisync values, such as “Min=1,317 ms, Max=3,112 ms”.

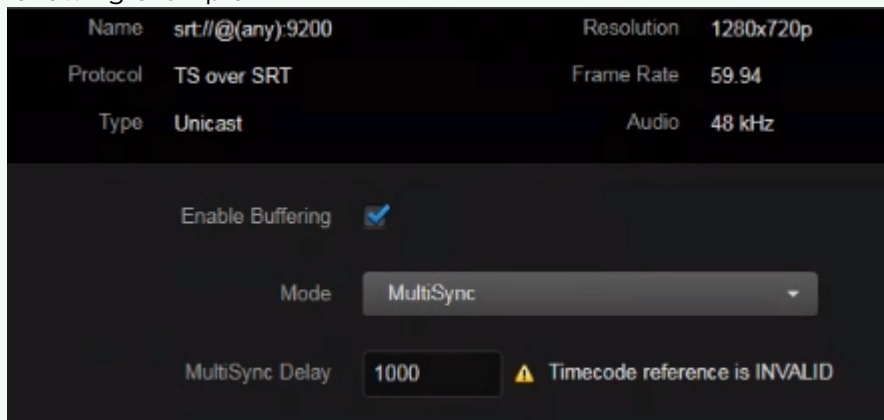


2. Note down the minimum/maximum ranges for all channels to be synchronized.

Tip

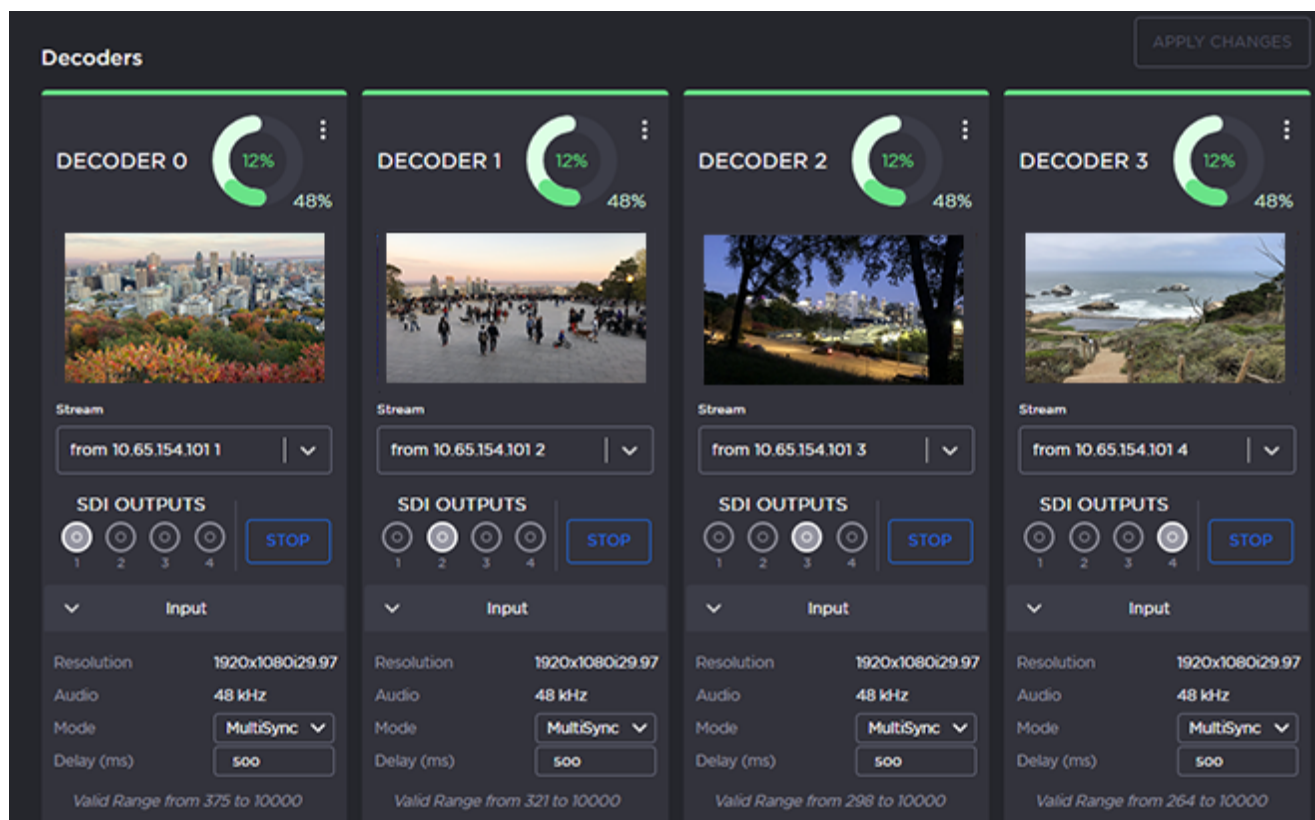
If you are synchronizing many decoder channels, complete **Step 2** for all of them and then go back to record the range values.

A yellow triangle appears next to the **MultiSync Delay** field if the value is outside the acceptable range. Position the cursor over the triangle to see a tool tip explaining the problem, as shown in the following example.



Makito X4 Decoder

1. On the Makito X4 Decoders panel, under **Input>** “Mode>MultiSync>Delay”, you will see the range of valid multisync values for each decoder.

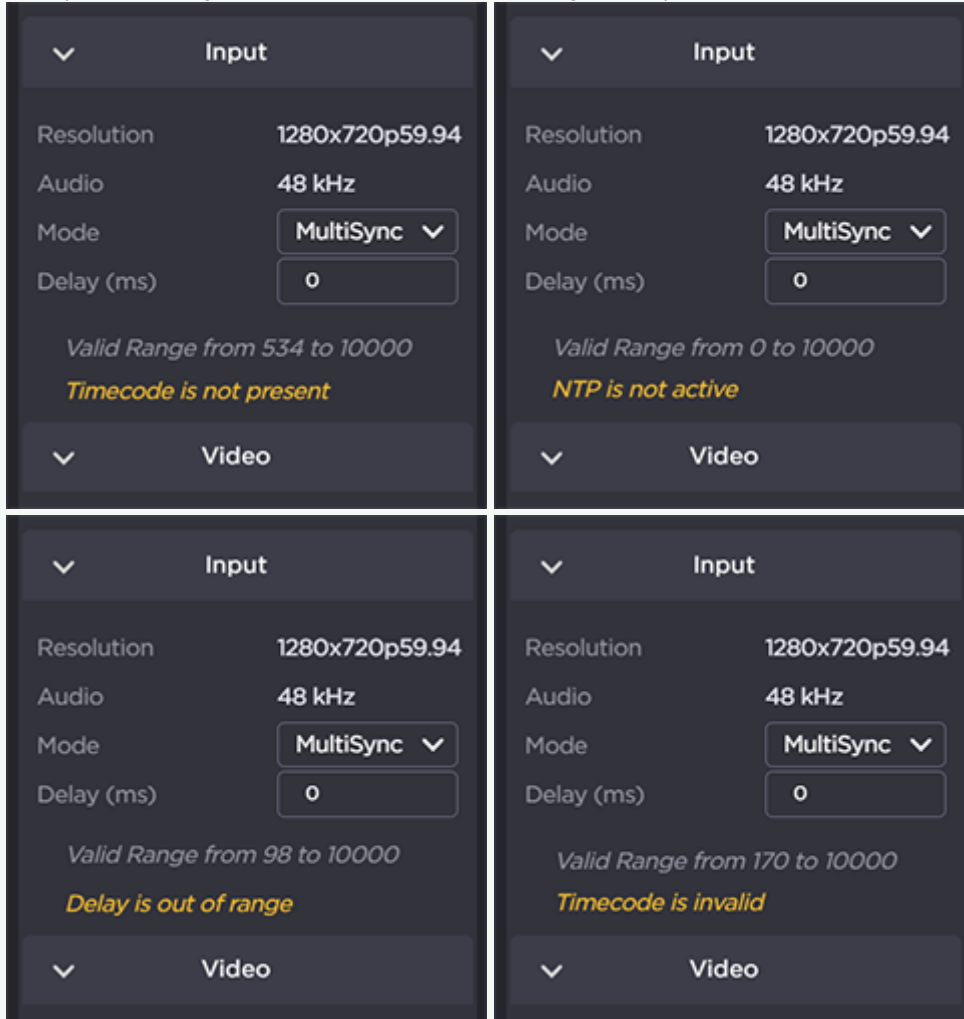


2. Note down the minimum/maximum ranges for all channels to be synchronized.

Tip

If you are synchronizing many decoder channels, complete **Step 2** for all of them and then go back to record the range values.

A yellow tip explaining the problem appears below the **Valid Range** field if the value is outside the acceptable range, as shown in the following examples.



Step 5: Configure MultiSync Delay (Decoder Pass 3)

Finally, change all the MultiSync Delays to a value that falls in the ranges for all decoder channels, and your channels should begin to synchronize.

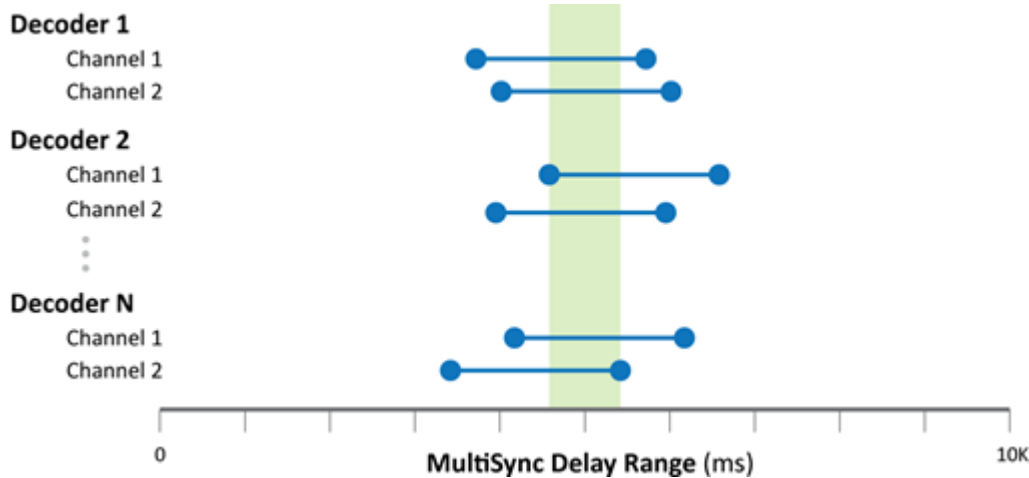
Step 5: Finalize (Decoder Pass 3)

Based on the results of Decoder Pass 2:

1. Select a single delay value that is in the acceptable range for all of the decoders. Avoid using the minimum or maximum values.
2. On the Decoder panel, set the MultiSync Delay on all of the decoder channels to the same value.

After a few seconds of playback, all of the decoder channels will be playing in sync with each other.

Perform [Steps 1 to 4](#) on all decoder channels you want to synchronize. Take a note of the valid **MultiSync Delay Range** for every decoder channel. Pick a single value that is in the acceptable range for all of the decoders (green area in diagram below), and then set the **MultiSync Delay** on all of the decode channels to that value.



After a few seconds of playback, all of the decoder channels will be playing almost perfectly in sync with each other.

Warranties

1-Year Limited Hardware Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

- (a) to cosmetic damage, including but not limited to scratches, dents and broken plastic on ports;
- (b) to damage caused by accident, abuse, misuse, flood, fire, earthquake or other external causes;
- (c) to damage caused by operating the product outside the permitted or intended uses described by Haivision;
- (d) to a product or part that has been modified to alter functionality or capability without the written permission of Haivision; or
- (e) if any Haivision serial number has been removed or defaced.

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

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

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

OBTAINING WARRANTY SERVICE

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

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

APPLICABLE LAW

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

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

EULA - End User License Agreement

READ BEFORE USING

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

Click the following link to view the Software End-User License Agreement: [Haivision EULA.pdf](#)

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

SLA - Service Level Agreement

1. Introduction

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

2. Definitions

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

3. Service Levels for the Video Content Management System

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

Type of Access	Definition	Availability Level
Write Functions	<ul style="list-style-type: none"> • Access to all functions through the administrative user interface. • Ability to add or modify objects and metadata through the application programming interface (“API”) • Ability of ingest service to check for new or updated files or feeds 	99.999%
Read-Only Functions	<ul style="list-style-type: none"> • Ability to retrieve data through the API • Ability for Audience Members to authenticate through the Access Service • Ability for Audience Members to play Published Media Objects • Ability for Audience Members to play Haivision VCMS-authenticated or entitled Published Media Objects • Ability to complete Transactions 	99.999%

4. Exceptions to Availability for the VCMS

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

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

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

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Normal	<ul style="list-style-type: none"> • Preventive maintenance on the software/hardware components of Haivision VCMS • Addition of new features/functions • Repair errors that are not immediately affecting Your use of Haivision VCMS 	No	Yes	10 Hours	6 Hours	10:00p m - 5:00a m	48 Hours
Urgent	<ul style="list-style-type: none"> • Repair errors that are immediately affecting Your use of Haivision VCMS 	No	Yes	30 Minutes	15 Minutes	Any Time	3 Hours

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Upgrades	<ul style="list-style-type: none"> Perform upgrades on software or hardware elements necessary to the long term health or performance of Haivision VCMS, but which, due to their nature, require that certain components of Haivision VCMS to be shut down such that no access is possible 	No	No	1 Hour	1 Hour	12:00am - 4:00am M-F	5 Days

5. Credits for Downtime for the VCMS

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

6. Support Services for the VCMS

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

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

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

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

7. Service Levels for Haivision Streaming Media Service

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

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

Agents and Polling Frequency

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

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

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

8. Credits for Outages of Haivision Streaming Media Service

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

9. No Secondary End User Support

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

Getting Help

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

