

Cobalt Digital Inc.

**BBG-1190-DEC-MPEG Standalone Decoder
BBG-1090-DEC-MPEG Standalone Decoder
9990-DEC-MPEG openGear® Decoder
MPEG4 AVC and MPEG2 Decoder with ASI and IP
Inputs and SDI Outputs**

Product Manual

Version 1.3.0



**BBG-1x90/9990-DEC-MPEG-OM
Version: 1.3.0**



BBG-1190/1090/9990-DEC-MPEG • MPEG4 AVC and MPEG2 Decoders with ASI and IP Inputs and SDI Outputs Product Manual

- Cobalt Digital Inc. Part Number: **BBG-1x90/9990-DEC-MPEG-OM**
- Document Version: **1.3.0**
- Printed in the United States
- Last Author: CAN
- Printing Date: 11/30/2020

The information contained in this manual is subject to change without notice or obligation.

Copyright

© 2018-2020 Cobalt Digital Inc..

All rights reserved. Contents of this publication may not be reproduced in any form without the written permission of Cobalt Digital Inc. Reproduction or reverse engineering of copyrighted software is prohibited.

Notice

The material in this manual is furnished for informational use only. It is subject to change without notice and should not be construed as commitment by Cobalt Digital Inc. Cobalt Digital Inc. assumes no responsibility or liability for errors or inaccuracies that may appear in this manual.

Trademarks

-  is a registered trademark of Ross Video Limited.
- [COBALT](#) is a registered trademark of Cobalt Digital Inc.
- DashBoard Control System™ is a trademark of Ross Video Limited.

All other product names and any registered and unregistered trademarks mentioned in this manual are used for identification purposes only and remain the exclusive property of their respective owners.

Safety Instructions for the BBG-1090/1190-DEC-MPEG Appliances

Note: In this manual, “BBG-1x90-DEC” refers to either of the following. Where differences apply, the units are discussed separately.

- **BBG-1190-DEC-MPEG** – Standalone Decoder
- **BBG-1090-DEC-MPEG** – Standalone Decoder

The BBG-1x90-DEC appliance is turned off by using the power switch. Power may still be present in the appliance. To ensure that the appliance is completely shut down, unplug its power cord from its power source.

The BBG-1x90-DEC appliance ships with all required components installed. There is no need to open the chassis to add or remove components. Please contact Product Support regarding any malfunction or failure of the device.

Safety Notice and Warnings

FCC Notice

This device complies with Subpart B of Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

No Telecommunications Network Voltage (TNV)-connected PCBs shall be installed.

Other Certifications

This class A digital apparatus complies with Canadian ICES-003, Issue 4.

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

This device complies with EN 55022 standards.

This device complies with EN 61000-3-2 standards.

This device complies with EN 61000-4-2 standards.

This device complies with CISPR 22 Edition 6.

This device complies with AS/NZS CISPR 22.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Installation Safety Notes

- Do not place the BBG-1x90-DEC appliance underneath heavy loads or in an unstable position.
- Do not expose the BBG-1x90-DEC appliance under direct sunlight, high humidity or wet conditions.
- Do not use or expose the BBG-1x90-DEC appliance around magnetic fields as magnetic interference may affect the performance of the device.
- Do not block the air vents to this device or impede the airflow in any way.



Important Safety Information! Please note the following:

1. The BBG-1x90-DEC is intended for indoor use only.
2. In case of emergency, disconnect the power cords.
3. If power cords are not provided:
 - In the United States, use standard computer power cords (as specified below).
 - In Europe, for 230 volt operation, use a cord set marked “HAR” and consisting of a min 3 core H05VVF3G075 cord that has a minimum 0.75 square mm diameter conductors, provided with an IEC 320 receptacle and a male plug for the country of installation, rated 6A, 250V.
4. Do not block the equipment vents.

READ THE FOLLOWING SAFETY INFORMATION THOROUGHLY BEFORE INSTALLING THIS PRODUCT. FAILURE TO FOLLOW THIS SAFETY INFORMATION MAY LEAD TO PERSONAL INJURY OR DAMAGE TO THE EQUIPMENT.

Power Supply

- This unit must be grounded.
- The unit must be connected to a grounded outlet to comply with product safety standards.
- The grounded socket-outlet shall be installed near the equipment and shall be easily accessible.
- Do not connect the power supply unit to an AC outlet without a ground connection.
- All power cords must be disconnected before servicing.

Power Cords

The plug on the power supply cords is considered to be the equipment disconnect device and must be approved for the country where it is used.

For USA and Canada:

- The cord set must be UL-approved and CSA-certified.
- The attachment plug must be an earth-grounding type with a NEMA 5-15P (15A 125V) plug and an EN60320/IEC320 receptacle.

Electrostatic Discharge (ESD) and ESD Protection

Static electricity can damage boards, and other components. Before connecting or disconnecting any device to the BBG-1x90-DEC appliance, we recommend you discharge static electricity by first touching a metal part of a grounded PC.



CAUTION: To reduce the risk of electric shock, do not open chassis; do not defeat or remove the ground pin of the power cord; connect only to a properly grounded ac power outlet. No user-serviceable parts inside. Refer servicing to qualified service personnel.

Important Regulatory and Safety Notices

Before using this product and any associated equipment, refer to the “**Important Safety Instructions**” listed below to avoid personnel injury and to prevent product damage.

Products may require specific equipment, and/or installation procedures to be carried out to satisfy certain regulatory compliance requirements. Notices have been included in this publication to call attention to these specific requirements.

Symbol Meanings



This symbol on the equipment refers you to important operating and maintenance (servicing) instructions within the Product Manual Documentation. Failure to heed this information may present a major risk of damage or injury to persons or equipment.



Warning — The symbol with the word “**Warning**” within the equipment manual indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.



Caution — The symbol with the word “**Caution**” within the equipment manual indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices.



Notice — The symbol with the word “**Notice**” within the equipment manual indicates a situation, which if not avoided, may result in major or minor equipment damage or a situation which could place the equipment in a non-compliant operating state.



ESD Susceptibility — This symbol is used to alert the user that an electrical or electronic device or assembly is susceptible to damage from an ESD event.

Important Safety Instructions



Caution — This product is intended to be a component product of an 8300 series frame. Refer to the frame User Manual for important safety instructions regarding the proper installation and safe operation of the frame as well as its component products.



Warning — Certain parts of this equipment namely the power supply area still present a safety hazard, with the power switch in the OFF position. To avoid electrical shock, disconnect all A/C power cards from the chassis’ rear appliance connectors before servicing this area.



Warning — *Service barriers within this product are intended to protect the operator and service personnel from hazardous voltages. For continued safety, replace all barriers after any servicing.*

This product contains safety critical parts, which if incorrectly replaced may present a risk of fire or electrical shock. Components contained with the product's power supplies and power supply area, are not intended to be customer serviced and should be returned to the factory for repair. To reduce the risk of fire, replacement fuses must be the same time and rating. Only use attachments/accessories specified by the manufacturer.

Maintenance/User Serviceable Parts

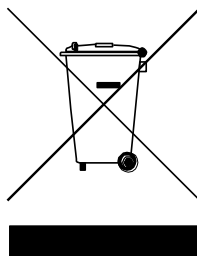
Routine maintenance to this Cobalt Digital Inc. product is not required. This product contains no user serviceable parts. If the frame does not appear to be working properly, please contact Technical Support using the numbers listed under the “Contact Us” section on the last page of this manual. All Cobalt Digital Inc. products are covered by a generous 5-year warranty and will be repaired without charge for materials or labor within this period. See the “Warranty and Repair Policy” section in this manual for details.

Environmental Information

The equipment that you purchased required the extraction and use of natural resources for its production. It may contain hazardous substances that could impact health and the environment.

To avoid the potential release of those substances into the environment and to diminish the need for the extraction of natural resources, Cobalt Digital Inc. encourages you to use the appropriate take-back systems. These systems will reuse or recycle most of the materials from your end-of-life equipment in an environmentally friendly and health conscious manner.

The crossed-out wheeled bin symbol invites you to use these systems.



If you need more information on the collection, reuse, and recycling systems, please contact your local or regional waste administration.

You can also contact Cobalt Digital Inc. for more information on the environmental performances of our products.

Contents

Safety Instructions for the BBG-1090/1190-DEC-MPEG Appliances	3
Safety Notice and Warnings	3
FCC Notice	3
Other Certifications	3
CE Mark Warning	3
Installation Safety Notes	4
Electrostatic Discharge (ESD) and ESD Protection	5
Contents	8
Introduction	11
Product Overview	12
BBG-1190-DEC-MPEG Indicators and Switches	14
Back Panel	14
Front Panel Indicators	16
The Presets Menu	17
The Config Menu	18
The Status Menu	19
Factory Configuration Reset	19
BBG-1090-DEC-MPEG Indicators and Switches	20
Rear Panel	20
Front Panel Indicators	22
Front Panel Default Switch	23
9990-DEC-MPEG Indicators and Switches	25
Rear I/O Panel Indicators	25
Front Indicators	26
Front Switches	27
DEC-MPEG Operation and Management	29
Product Tab	31
Network Tab	34
Network Configuration Tab	34
Network Configuration Interfaces Tab	34
Network Configuration RIST Tunnels Tab	36
Network Configuration Authentication Tab	39
Network Statistics Tab	41
Network Statistics Interfaces Tab	41
Network Statistics RIST Tunnels Tab	42
Network Statistics Authentication Tab	43
Network Statistics Tunnel Stats Tab	44
Network Statistics Remote Info Tab	45
ASI Input Port	47
ASI Input: Configuration Tab	47
ASI Input: Statistics Tab	48
ASI Output Port	49
ASI Output Port: Configuration Tab	49
ASI Output Port: Statistics Tab	50
Decoder	51

Decoder Configuration Tab	51
Decoder Input Configuration	51
ASI Input.....	52
UDP/RTP Stream.....	53
RIST Stream.....	55
HLS Stream.....	57
RTMP Client.....	58
RTMP Server	60
RTSP Client	60
Color Bars	62
Decoder Program and Audio Selection.....	62
Decoder Output Configuration	64
Digital Output: Disabled	64
Digital Output: SDI.....	64
Digital Output: HDMI.....	67
Decoder Ancillary Data Injection Configuration.....	67
Decoder Analog Audio Configuration.....	68
Decoder Apply/Cancel Buttons	69
Decoder Program Info Tab	70
Program Info Tab for ASI Input and UDP/RTP Stream.....	70
Program Info Tab for HLS Stream	71
Program Info Tab for RTMP Client and Server	72
Program Info Tab for RTSP Streams.....	73
Program Info Tab for Color Bars.....	73
Decoder Statistics Tab	73
Status Tab.....	73
Network Tab	75
Network Tab for ASI Input.....	75
Network Tab for UDP/RTP Stream.....	75
Network Tab for RIST Stream.....	77
Network Tab for HLS Stream.....	79
Network Tab for RTMP Client and Server.....	80
Network Tab for RTSP Client	81
Network Tab for Color Bars	82
Ancillary Data Tab.....	82
Configuration Tab.....	83
.....	83
IP Outputs Tab	84
IP Outputs Configuration Tab.....	84
IP Outputs Status Tab	90
Monitoring Tab	91
Monitoring Configuration Tab.....	91
PID Monitor Configuration Tab	91
PID Alarms Configuration Tab.....	92
Monitoring Status Tab	93
Admin	95

Admin General Tab.....	95
Admin Firmware Tab.....	96
Admin Config Files Tab	98
User-Saved Configurations.....	99
Pre-defined Templates	101
Clear Current Configuration Button	102
Admin License Keys Tab.....	102
Admin Event Log Tab	104
Control Tab	108
Control Port Configuration Tab	108
Control Port Statistics Tab	109
SNMP Configuration Tab	110
SNMP Statistics Tab	110
Support Tab.....	112
RIST Main Profile Authentication.....	113
Technology Overview.....	113
Certificate Validity and Expiration.....	114
Blacklists.....	114
Signing a Certificate	114
Cipher Suites	115
RIST Main Profile Encryption and Authentication in Cobalt Devices.....	116
Encryption options	116
Authentication Options	117
Authentication Security Model	118
Configuring the Local Credentials in the Device	119
Uploading Keys and Certificates	119
Obtaining a CSR for the Built-In Keys.....	120
Authenticating Remote Devices	121
Option 1: Use an External Certificate Authority	121
Option 2: Using one of the Cobalt Devices as the Certificate Authority.....	123
Option 3: Using the same CA Key in all Cobalt Devices.....	126
Creating a Blacklist.....	127
Creating a Certificate Authority with OpenSSL.....	128
Generating the CA Key and Certificate	128
Generating Device Keys	129
Generating CSRs.....	129
Generating Signed Certificates from the CSRs	130

Introduction

This manual covers the following products:

- The BBG-1190-DEC-MPEG Standalone MPEG4 AVC and MPEG2 Decoder
- The BBG-1090-DEC-MPEG Standalone MPEG4 AVC and MPEG2 Decoder
- The 9990-DEC-MPEG openGear® MPEG4 AVC and MPEG2 Decoder

All products have the same set of features, and essentially the same user interface. Unless specifically indicated, all features and controls described in this manual apply to all products. In this manual, the product is generically referred to as the “Decoder” or DEC-MPEG.

The decoders have the following features:

- Multi-Standard Decoder (MPEG-2 and H.264), with support for both SD (Standard Definition) and HD (High Definition) content.
- Resolution resizing support (both upscale and downscale support).
- Frame rate conversion.
- Support for RIST on Ethernet.
- Support for generic ancillary data extraction and insertion into SDI VBI where SMPTE-2038 is present on received streams.
- Support for SCTE 35 to SCTE-104 conversion.
- Audio decoding support: MPEG-1 Layer III, AAC-LC, HE-AAC and Dolby AC-3.
- ASI input and output ports. All ports support the full ASI line rate of 213 Mb/s.
- Ethernet port for streaming with 100/1000 Mb/s support.
- Internet Protocol support:
 - UDP/RTP/SMPTE-2022 auto-sensing
 - RIST support, including:
 - RIST Simple Profile, compliant to VSF TR-06-1
 - RIST Main Profile Baseline Level, compliant to VSF TR-06-2
 - RIST Main Profile DTLS Level, compliant to VSF TR-06-2
 - HTTP Live Streaming (HLS) client
 - RTMP Client mode – connects to an RTMP server and plays the content
 - RTMP Server mode – accepts connections from an RTMP encoder
 - RTSP Client mode – connects to an RTSP server, such as a camera, and plays the content
- (P)SI and ATSC table parsing.

Typical application scenarios for the DEC-MPEG are:

- Contribution and Distribution: reception of MPEG-2/H.264 content.
- Contribution feeds over the Internet.
- Ingestion of traffic cameras for broadcast use.

Product Overview

Note: Some GUI depictions shown in this manual may show “9990-DEC-MPEG” for device ID. Models 9990-DEC-MPEG and BBG-1090/1190-DEC-MPEG are functionally identical.

The DEC-MPEG is a multi-standard broadcast decoder with the following features:

- Video Decoding: MPEG-2 and H.264 4:2:0 High Profile video streams with resolution up to 1920×1080p60.
- Audio Decoding capabilities: summarized in the table below. Note that 5.1 and 7.1 audio services are down-converted to stereo when decoded.

Standard	Max Sample Rate	Max Channels
Dolby Digital ¹	48 kHz	5.1
Dolby Digital Plus ¹	48 kHz	7.1
WMA	48 kHz	2
WMA PRO	48 kHz	5.1
MPEG-1 Layer I/II/III	48 kHz	2
MPEG-2 Layer II MC	48 kHz	5.1
AAC-LC	48 kHz	5.1
HE-AAC V1	96 kHz	5.1
HE-AAC V2	96 kHz	2
DRA	96 kHz	7.1
FLAC	96 kHz	5.1
OGG Vorbis	48 kHz	5.1

- Inputs:
 - ASI Input
 - IP Input using an auto-sensing 10/100/1000 Gb/s Ethernet
- Internet Protocol support²:
 - UDP/RTP (auto-detected)
 - RIST (based on VSF TR-06-1)
 - SMPTE-2022 FEC (auto-detected, support for both row and column)
 - HTTP Live Streaming (HLS) client
 - RTMP client (flash content playback from servers)
 - RTMP server (accepts connections from live encoders)³
 - RTSP client (connects to IP cameras)
- Outputs
 - Composite video output
 - HDMI video output with embedded audio
 - SDI video output with embedded audio, SMPTE-334 closed-captions, and (where present) SMPTE-2038 generic ancillary data, and SCTE-104 ancillary data
 - Analog stereo audio output

¹ A separate license is required for Dolby decoding. Please contact Cobalt Digital Inc. if you need this license.

² A separate license is required for the IP input. Please contact Cobalt Digital Inc. if you need this license.

³ A separate license is required for RTMP Server operation. Please contact Cobalt Digital Inc. if you need this license.

-
- ASI loop-through output

For the remainder of this manual, we will use the term *port* for a physical input/output port (such as ASI or Ethernet), and *stream* for a transport stream present in the port. ASI ports support only one stream, while Ethernet ports support multiple streams. A transport stream can have one or more *programs*. In this manual, we will use the words *program* and *service* interchangeably.

BBG-1190-DEC-MPEG Indicators and Switches

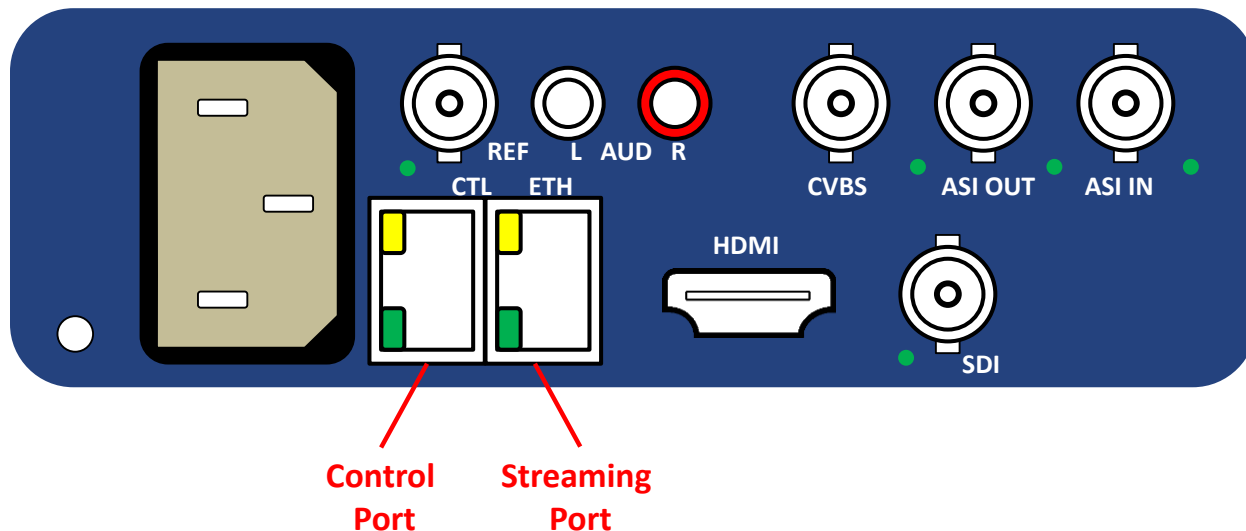
The BBG-1190-DEC-MPEG can be used as a desktop decoder, or in a 19" rack-mount tray that holds up to three units:



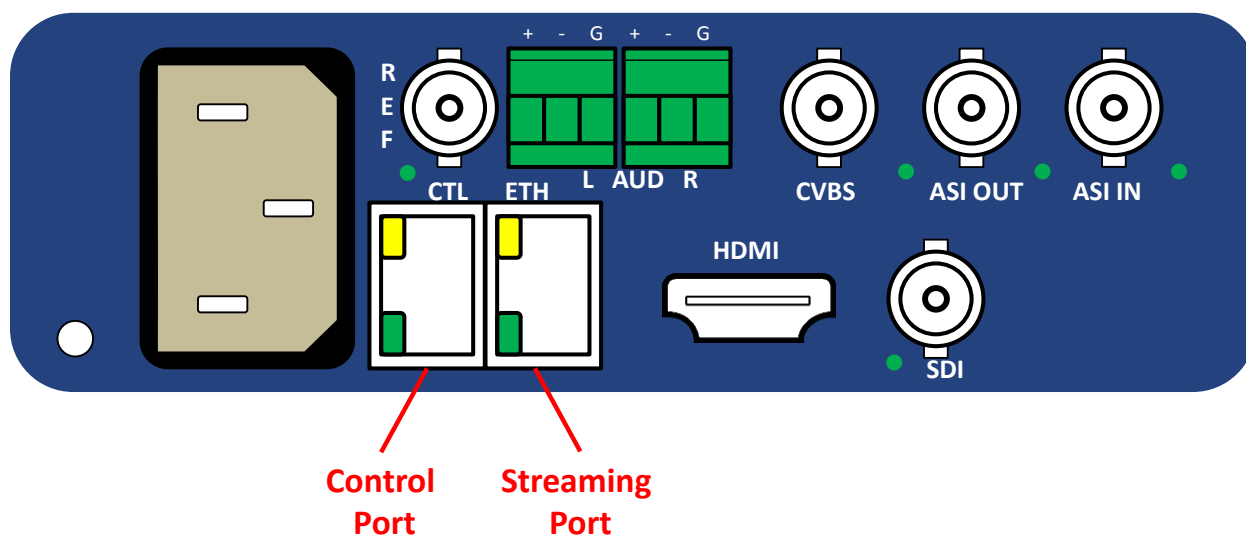
Back Panel

There are two types of rear I/O panels available for the BBG-1190-DEC-MPEG, depicted below. Both types include one ASI input, one ASI output, one composite output, one SDI output and one genlock reference input on standard BNC connectors, one HDMI output and one 100/1000 Mb/s Ethernet port on a standard RJ-45 connector. The panels differ only on the type of analog audio output: one type has balanced audio on terminal blocks, and the other type has unbalanced audio on RCA connectors.

Unbalanced Audio Version



Balanced Audio Version



The ASI input port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing once every 3 seconds:** the ASI port is not locked to a signal (i.e., there is no input signal).
- **LED flashing once per second:** the ASI port is locked to a signal.

The ASI output port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing multiple times per second:** ASI port is transmitting packets.

The Video output ports share one green indicator LED, with the following states:

- **LED off:** the BBG-1190-DEC-MPEG is not currently decoding a stream. There may be a valid video signal in the output, but it does not correspond to a decoded stream.
- **LED flashing once per second:** the BBG-1190-DEC-MPEG is currently outputting an SD stream on the selected output ports.
- **LED flashing multiple times per second:** the BBG-1190-DEC-MPEG is currently outputting an HD stream on the selected output ports.

The Reference Input port has one green indicator LED, with the following states:

- **LED off:** reference signal not valid.
- **LED on:** reference signal valid.

The Reference signal is deemed valid if all the following conditions are met:

- The BBG-1190-DEC-MPEG is configured for output genlock.
- The BBG-1190-DEC-MPEG is receiving a valid genlock signal from the selected chassis reference input.
- The genlock signal is compatible with the selected SDI output resolution and frame rate.

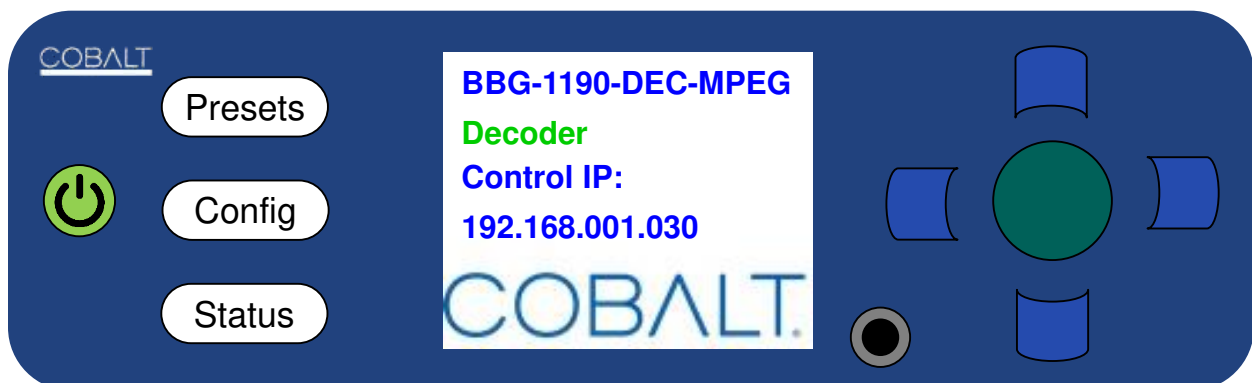
Consult the Decoder Output Configuration section later in this manual for the genlock source selection and the SDI output configuration.

The Control and Streaming Ethernet ports have two indicator LEDs, with the following states:

- **Green LED:**
 - **Off:** No link
 - **On:** Link
- **Yellow LED:**
 - **Off:** No activity (transmit and/or receive)
 - **Flashing:** Port is currently transmitting and/or receiving

Front Panel Indicators

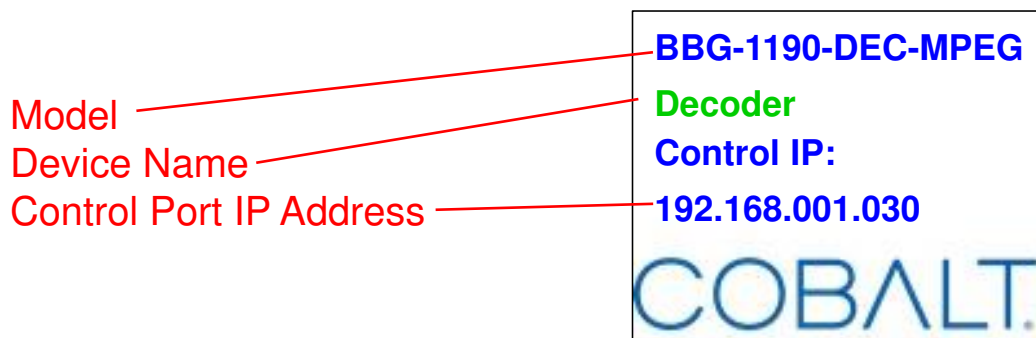
The BBG-1190-DEC-MPEG has a front panel with an LCD display and buttons:



Operation of the panel is as follows:

- The device powers up as soon as the power cable is connected to power. In order to turn off the power, press and hold the power button on the left. The button will flash red for about 3 seconds, and after that power turns off.
- By default, the LCD screen shows the following information:
 - **Device Model:** BBG-1190-DEC-MPEG
 - **Device Name:** User-assigned name, configured through DashBoard in the Control Port Configuration Tab.
 - **Control Port IP Address:** Current IP address assigned to the control port.

An example is depicted below:



- The LCD automatically turns off after 1 minute of inactivity. It turns back on as soon as any key in the front panel is pressed.
- Three function buttons to the left of the LCD screen, marked as **Presets**, **Config** and **Status**. These buttons can light up either green or red. Their functions are:
 - **Presets** button: brings up the 5 presets defined in DashBoard and allows one of them to be selected and applied to the device.
 - **Config** button: allows for some more common items to be configured.
 - **Status** button: allows for quickly inspecting the status and alarms in the device.
- Navigation buttons to the right of the LCD screen. The center (green) button is the **Enter** button, used to accept selections. There are 4 blue buttons to navigate menus (up, down, left, right).

The Presets Menu

The BBG-1190-DEC-MPEG has the ability to save up to 5 configurations (presets). The **Presets** front panel key brings up a menu to select any of the presets. Use the Up/Down (blue) keys to select the desired preset, and the Enter (green) key or the right (blue) key to select it. Use the left key to exit the menu (or press one of the other function buttons).

Here is an example of the presets screen:

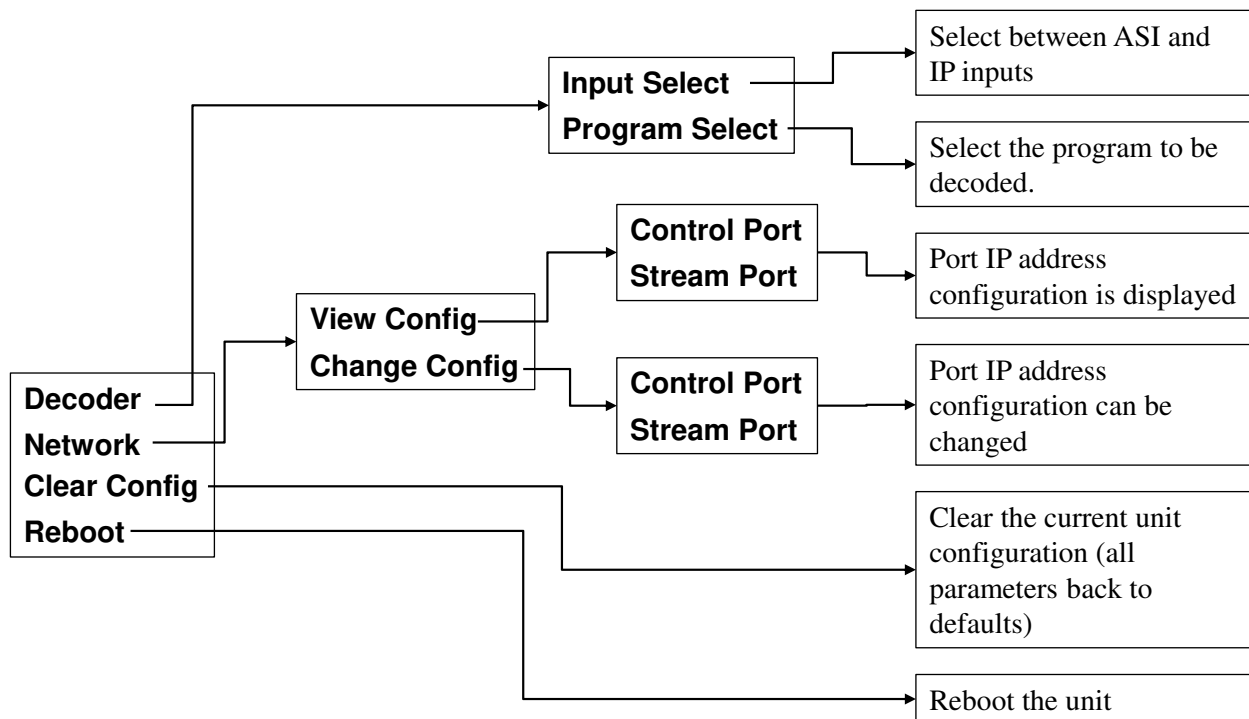
PRESETS:

- >1: Satellite Transmis
- 2: Microwave Link
- 3: IPTV Configuration
- 4: Internet Streaming
- 5: (empty)

Config	Status	Name
1	Saved	Satellite Transmission
2	Saved	Microwave Link
3	Saved	IPTV Configuration
4	Saved	Internet Streaming
5	Empty	

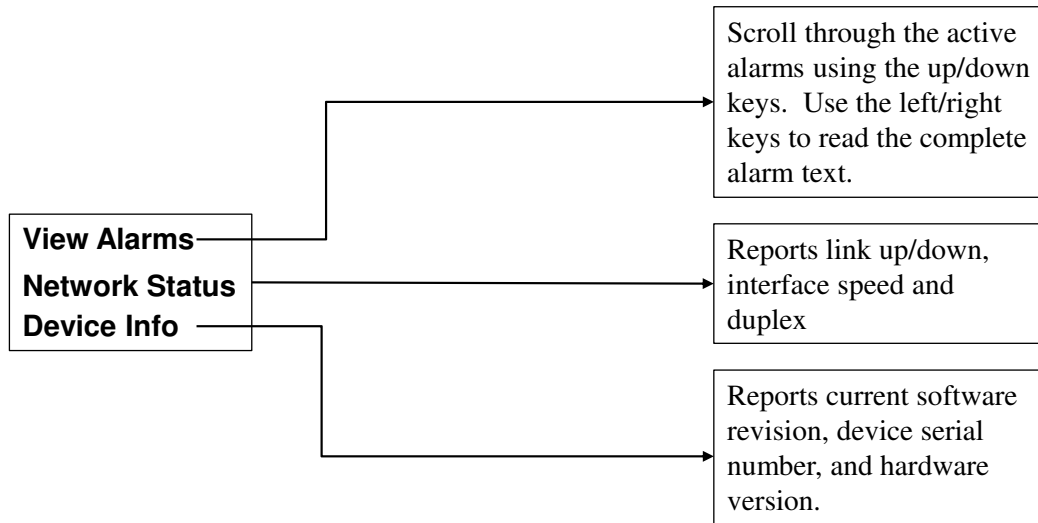
The Config Menu

The **Config** front panel key bring up the configuration menu tree. Only a few selected parameters can be configured in this menu; these are the most common configuration parameters. The Config menu tree is displayed below.



The Status Menu

The **Status** button will be lighted steady green if there are no active alarms, or flashing red if there are active alarms. Pressing the **Status** button will bring up the status menu tree, depicted below:



Factory Configuration Reset

It is possible to reset the configuration of the BBG-1190-DEC-MPEG to the factory default. This can be used as a “last resort” in case of a configuration error. The steps are as follows:

- Power off the unit by pressing and holding the Power button for 3 seconds or more.
- Power on the unit again.
- Watch the front panel and left-side buttons. They will go through the following steps:
 1. The buttons will light up and the company logo will be displayed.
 2. The button lights turn off.
 3. The company logo disappears, replaced by a black screen.
 4. The company logo appears.
- When the panel gets to step 4, press and hold the **Config** button. Keep holding the button until you see the message **Config Clear** at the bottom of the screen.

BBG-1090-DEC-MPEG Indicators and Switches

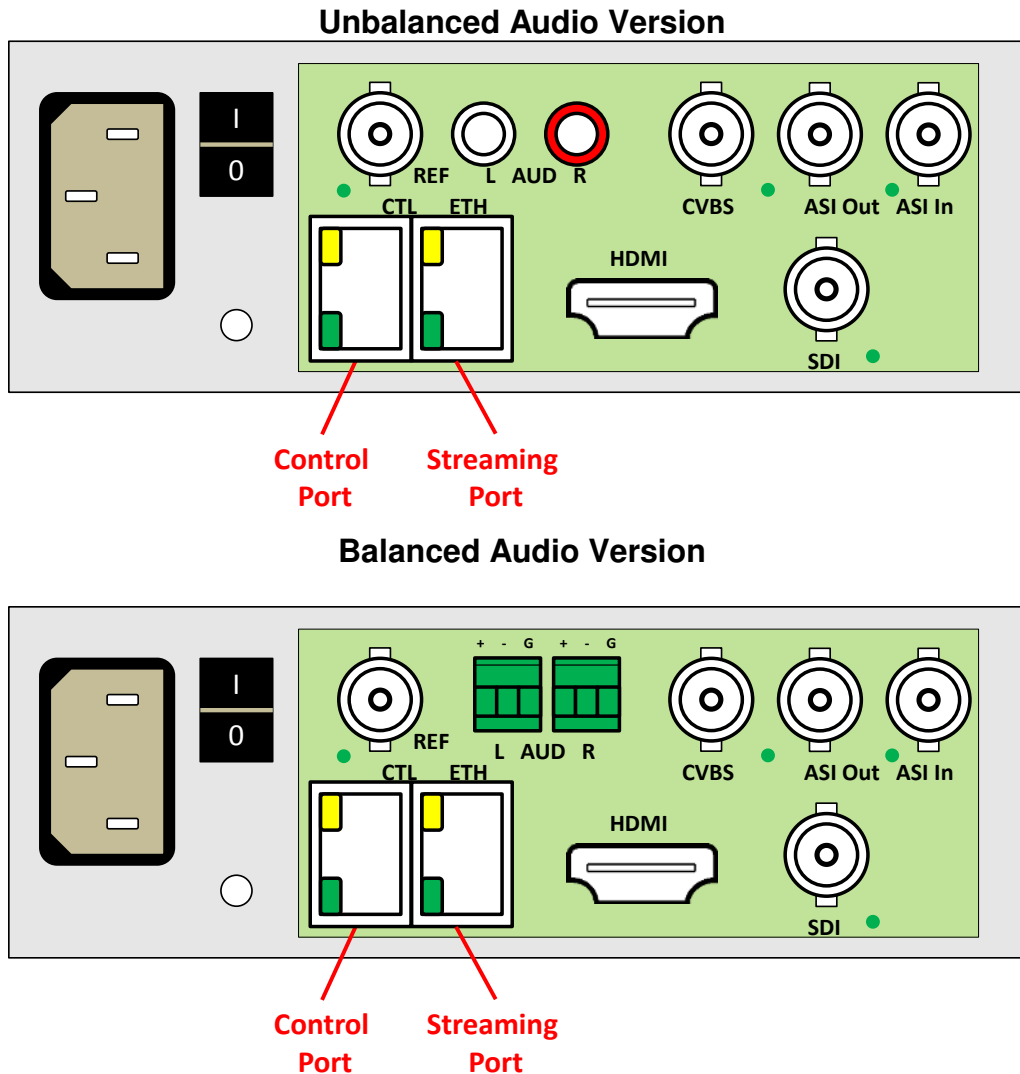
The BBG-1090-DEC-MPEG can be used as a desktop decoder, or in a 19" rack-mount tray that holds up to three units:



Rear Panel

There are two types of rear I/O panels available for the BBG-1090-DEC-MPEG, depicted below. Both types include one ASI input, one ASI output, one composite output, one SDI output and one genlock reference input on standard BNC connectors, one HDMI output and one 100/1000 Mb/s Ethernet port on a standard RJ-45 connector. The panels differ only on the type of analog audio output:

- Model **BBG-1090-DEC-MPEG-B** is fitted with 3-pin terminal block audio connectors providing balanced analog audio outputs.
- Model **BBG-1090-DEC-MPEG-U** is fitted with "RCA" connectors providing unbalanced analog audio outputs.



The ASI input port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing once every 3 seconds:** the ASI port is not locked to a signal (i.e., there is no input signal).
- **LED flashing once per second:** the ASI port is locked to a signal.

The ASI output port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing multiple times per second:** ASI port is transmitting packets.

The Video output ports share one green indicator LED, with the following states:

- **LED off:** the decoder is not currently decoding a stream. There may be a valid video signal in the output, but it does not correspond to a decoded stream.
- **LED flashing once per second:** the decoder is currently outputting an SD stream on the selected output ports.
- **LED flashing multiple times per second:** the decoder is currently outputting an HD stream on the selected output ports.

The Reference Input port has one green indicator LED, with the following states:

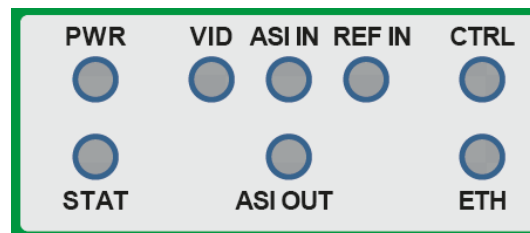
- **LED off:** no reference signal is detected.
- **LED flashing:** reference signal present.

The Control and Streaming Ethernet port have two indicator LEDs, with the following states:

- **Green LED:**
 - **Off:** No link
 - **On:** Link
- **Yellow LED:**
 - **Off:** No activity (transmit and/or receive)
 - **Flashing:** Port is currently transmitting and/or receiving

Front Panel Indicators

A similar set of indicators exist in the front panel of the unit. The layout is depicted below.



The front panel LED indicators are as follows:

- **STAT:** indicates the overall status of the unit.
 - **Green:** no active alarm
 - **Red:** at least one critical alarm present

When powering up the unit, this LED will be red until the board starts operation. At that point, it will turn green if there is no active alarm or stay red if there is at least one alarm.
- **PWR:** indicates that the power is OK.
 - **Green:** power OK
 - **Off:** no power or insufficient voltage
- **ASI In LED:** behaves exactly the same as the ASI input rear I/O panel indicator.
- **ASI Out LED:** behaves exactly the same as the ASI output rear I/O panel indicator.
- **VID LED:** behaves exactly the same as the Video output rear I/O panel indicator.

-
- **Ref In LED:** this LED blinks when the decoder is receiving a genlock signal from the chassis reference input.
 - **ETH and CTRL LEDs:** indicate the status of the corresponding back panel Ethernet connection.
 - **Off:** no link
 - **On:** link OK, no activity
 - **Blinking:** link OK, port is transmitting and/or receiving packets

Front Panel Default Switch

The front panel has a recessed switch that can be used to restore the unit to its defaults. Use a pen or a small screwdriver to press this switch.



If the switch is pressed during normal operation, the control port IP address, mask and gateway are restored to the following factory default settings:

- IP Address: 192.168.1.30
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

The **STAT** front panel indicator will change colors for about 3 seconds to acknowledge the change. Note that this operation **may glitch the video**.

If you press and hold this switch when the unit is powered off, and then power up the unit while holding the switch, the following actions will be performed:

- The control IP address, mask and gateway are reset to the factory defaults as described above.
- The unit configuration is cleared.
- The unit reverts to the factory-installed firmware.

As before, the **STAT** LED will temporarily change color to acknowledge the command. When it changes color, you can release the switch. You can use this feature in the unlikely event of a corrupted firmware upgrade or a corrupted configuration.

9990-DEC-MPEG Indicators and Switches

The 9990-DEC-MPEG card is intended for installation in the 20-slot openGear frames. Earlier 10-slot frames are not supported. Prior to installing the card, first install the corresponding rear panel I/O module.

Rear I/O Panel Indicators

There are four types of rear I/O panels available for the 9990-DEC-MPEG, depicted below. All types include one ASI input, one ASI output, one composite output and one SDI output on standard BNC connectors, and one 100/1000 Mb/s Ethernet port on a standard RJ-45 connector. The panels differ as follows:

- Type of analog audio output: either balanced audio on terminal blocks, or unbalanced audio on RCA connectors.
- Number of SDI/HDMI outputs: either two SDI outputs, or one SDI output and one HDMI output.

Note that the panels with dual-SDI output are only compatible with Revision 2 decoders. Revision 1 decoders will not recognize these panels.

The ASI input port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing once every 3 seconds:** the ASI port is not locked to a signal (i.e., there is no input signal).
- **LED flashing once per second:** the ASI port is locked to a signal.

The ASI output port has a green indicator LED, with the following states:

- **LED off:** ASI port is disabled.
- **LED flashing multiple times per second:** ASI port is transmitting packets.

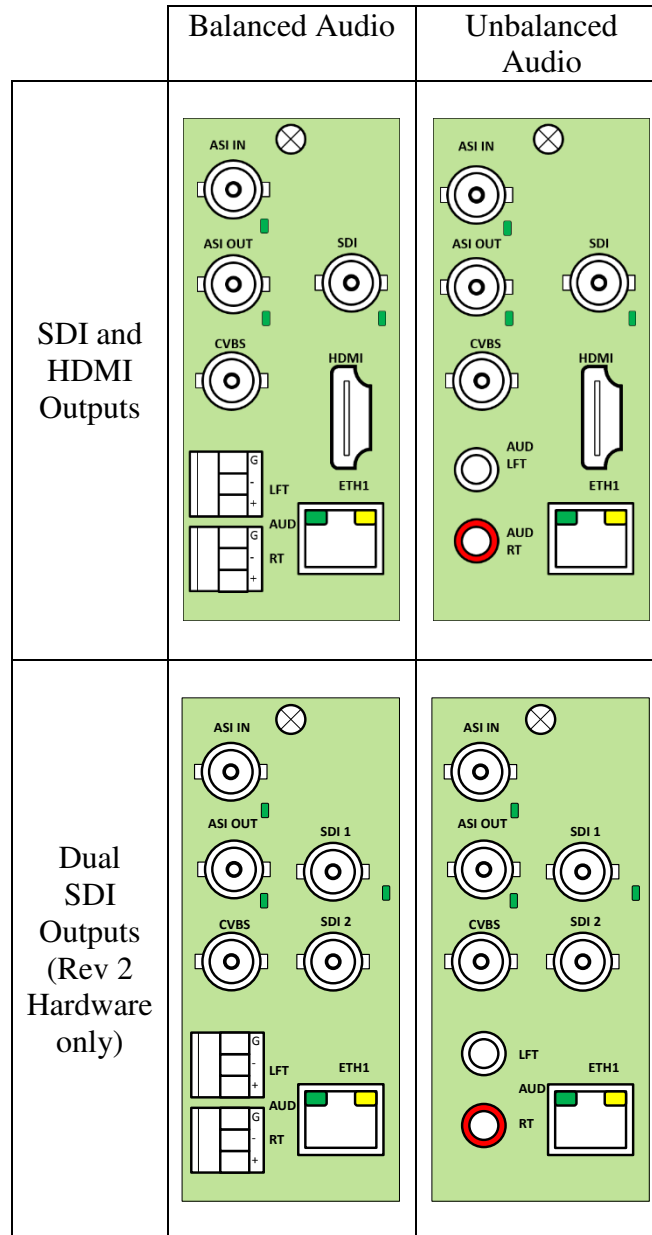
The Video output ports share one green indicator LED, with the following states:

- **LED off:** the 9990-DEC-MPEG is not currently decoding a stream. There may be a valid video signal in the output, but it does not correspond to a decoded stream.
- **LED flashing once per second:** the 9990-DEC-MPEG is currently outputting an SD stream on the selected output ports.
- **LED flashing multiple times per second:** the 9990-DEC-MPEG is currently outputting an HD stream on the selected output ports.

The Gigabit Ethernet port has two indicator LEDs, with the following states:

- **Green LED:**
 - **Off:** No link

- **On:** Link
- **Yellow LED:**
 - **Off:** No activity (transmit and/or receive)
 - **Flashing:** Port is currently transmitting and/or receiving

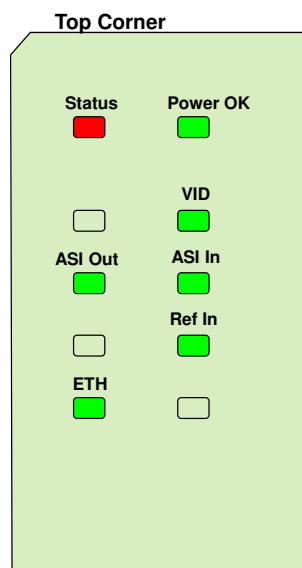


Front Indicators

A similar set of indicators exist in the front of the board. These are visible when the frame front door is opened. The indicator layout is depicted below.

The LED indicators are as follows:

- **Status LED:** indicates the overall status of the board.
 - **Green:** no active alarm
 - **Red:** at least one critical alarm presentWhen inserting a board in the frame, this LED will be red until the board starts operation. At that point, it will turn green if there is no active alarm or red if there is at least one alarm.
- **Power OK LED:** indicates that the power received from the frame is OK.
 - **Green:** power OK
 - **Off:** no power (or insufficient voltage – check the frame power status)
- **ASI In LED:** behaves exactly the same as the ASI input rear I/O panel indicator.
- **ASI Out LED:** behaves exactly the same as the ASI output rear I/O panel indicator.
- **VID LED:** behaves exactly the same as the Video output rear I/O panel indicator.
- **Ref In LED:** this LED blinks when the 9990-DEC-MPEG is receiving a genlock signal from the chassis reference input.
- **ETH LED:** indicates the status of the back panel Ethernet connection.
 - **Off:** no link
 - **On:** link OK, no activity
 - **Blinking:** link OK, port is transmitting and/or receiving packets

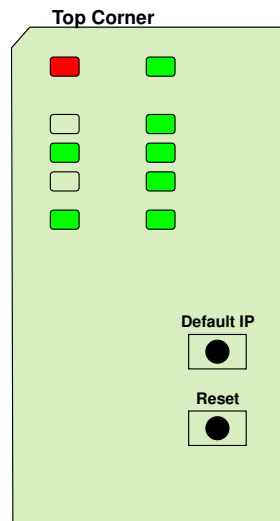


The 9990-DEC-MPEG board has other LEDs that may or may not be illuminated. They are intended for engineering debug only.

Front Switches

The 9990-DEC-MPEG board has two pushbutton-type switches in the front, just below the LEDs, as depicted below. Their operation is as follows:

-
- **Default IP Switch:** This switch is used to recover the board in the unlikely case of a corrupted or broken firmware update. In most cases, the 9990-DEC-MPEG will detect the error and automatically fall back into the factory-default firmware load. If it does not, pull the card out, press and hold this switch, and push the card back into the frame while still holding the switch. You can release the switch once the Status LED turns orange. This action causes the card to revert to the factory-default firmware.
 - **Reset Switch:** Pressing this pushbutton switch causes the card to reset.



DEC-MPEG Operation and Management

The DEC-MPEG is configured using the free Dashboard™ application, which is available for Windows, Apple OS X, and Linux. Dashboard can be downloaded from this link:

<https://www.opengear.tv/frame-and-control/control-system/download/>⁴

The DEC-MPEG user interface is depicted below. As with any openGear™ device, it is divided into a statistics panel on the left, and a configuration panel on the right. Each panel has multiple tabs, corresponding to the various functions in the card. Note that the **Card State** alarm indicator is also reflected in the green/red **Status** LED in the front of the board. The Status LED will be green when Card State is green or yellow, and will be red when Card State is red.

The following tabs are available:

- **Product:** this tab provides general information on the card, including firmware version, uptime, temperatures, and other parameters. It appears only on the Statistics panel.
- **Network:** this tab is used to configure the IP addresses and network information for the Ethernet ports. The statistics side of the panel includes some additional information such as link state.
- **ASI Input:** this tab is used to configure/monitor the ASI Input port.
- **ASI Output:** this tab is used to configure/monitor the ASI Output port.
- **Decoder:** this tab is used to configure/monitor the decoding function.
- **IP Outputs:** this tab is used to configure/monitor the ASI to IP turnaround function.
- **Monitoring:** this tab is used to configure the decoder stream monitoring function, and to inspect any monitoring alarms.
- **Admin:** this tab is used for general administrative functions, such as firmware upgrades, licensing, logs, and configuration management.
- **Control:** this allows for the configuration of the Ethernet control port and the SNMP function. It is present only for the BBG models.
- **Support:** this tab has information on how to contact Customer Support, and has the ability to generate a tech support dump for the unit.

⁴ Please note that DashBoard versions 4.0 and 4.1 have GUI performance problems with the BBG-1x90-DEC-MPEG. We recommend version 5.0 or higher

Slot 8: 9990-DEC-MPEG
Card state: ● OK
Connection: ● ONLINE

Decoder

ASI Output

Admin

Product

Network

ASI Input

Build Date: Oct 6 2015 15:56:49
Supplier: Cobalt Digital Inc
Product: 9990-DEC-MPEG
Software Rev: 0.5.1
DSP Version: 1.1
Serial Number: ac83f0009004
Hardware Version: 1
Rear Module: ● OK
Analog Audio Output: Unbalanced
Card Uptime: 5 days, 6 hours, 30 minutes
Ambient Temp: 30.13
Internal Temp: 35.88
MDP Core Temp: 37.25
Card Power (W): 4.5

ASI Output

Admin

Support

Network

ASI Input

Decoder

Ethernet Configuration

Alarm on Link Loss: ☒ Yes ☐ No
IP Address: 10.10.9.128
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
IGMP Version: Auto-Detect
Interface Speed: Auto-Negotiate
Interface Settings:

Apply

Cancel

Statistics Panel

Configuration Panel

Product Tab

The Product Tab contains basic information about the DEC-MPEG.

The screenshot shows a web-based monitoring interface with a dark grey background and yellow text. At the top, there are two main tabs: 'Monitoring' and 'Admin'. Under 'Monitoring', there are three sub-tabs: 'Decoder', 'IP Outputs', and 'ASI Output'. Under 'Admin', there are three sub-tabs: 'Product', 'Network', and 'ASI Input'. The 'Product' tab is currently selected. Below the tabs, there is a list of system parameters, each with a label and a value in a yellow box. The parameters are: Build Date (Mar 10 2018 11:05:58), Supplier (Cobalt Digital Inc.), Product (9990-DEC-MPEG), Software Rev (1.1.0), DSP Version (1.1), Serial Number (ac83f00093f2), Hardware Version (2), Rear Module (OK, indicated by a green dot), Installed I/O Panel (Balanced), Card Uptime (1 day, 20 hours, 59 minutes), Ambient Temp (26.00), Internal Temp (37.75), MDP Core Temp (37.06), and Card Power (W) (6.3).

Parameter	Value
Build Date	Mar 10 2018 11:05:58
Supplier	Cobalt Digital Inc.
Product	9990-DEC-MPEG
Software Rev	1.1.0
DSP Version	1.1
Serial Number	ac83f00093f2
Hardware Version	2
Rear Module	OK
Installed I/O Panel	Balanced
Card Uptime	1 day, 20 hours, 59 minutes
Ambient Temp	26.00
Internal Temp	37.75
MDP Core Temp	37.06
Card Power (W)	6.3

The following information is available:

- **Build Date:** Date the firmware image was built.
- **Supplier:** Cobalt Digital Inc.
- **Product:** Indicates the actual product type.
- **Software revision:** This indicates the firmware revision currently running. The format is Major Version • Minor Version • Build Number.
- **DSP version:** This indicates the firmware revision for the decoding subsystem. The format is Major Version • Minor Version. DSP firmware will only occasionally be updated by Cobalt Digital Inc..
- **Serial Number:** This is the serial number of this particular DEC-MPEG card.
- **Hardware Version:** This indicates the board version number.
- **Rear Module:** This indicates the status of the Rear I/O Module. It can have one of the following states:

- **OK:** The Rear Module is the correct module for the 9990-DEC-MPEG card. In the standalone models this indicator will be always green.
- **Not Installed:** The 9990-DEC-MPEG openGear card is not connected to a rear module. The card is operating normally, but it will not be useful as there are no input and output connections to it.
- **Wrong Module:** The 9990-DEC-MPEG openGear card is connected to a rear module that was not designed for it (most likely from another openGear® vendor). Depending on the signals present on that module, there may be a small chance of damage to the 9990-DEC-MPEG; Cobalt recommends that this situation be rectified immediately. This alarm will cause the front status LED to turn red. A card with hardware version 1 will show this alarm for the dual-SDI rear I/O panel.
- **Installed I/O Panel:** The DEC-MPEG can be fitted with either balanced or unbalanced analog audio outputs. For the BBG models, this is fitted at the factory. For the openGear model, this indicates the detected I/O panel. This indicator has the following values:
 - **Unknown:** This can only be shown for the 9990-DEC-MPEG. It indicates that the rear panel is either not installed or incompatible with the 9990-DEC-MPEG.
 - **Balanced:** the rear panel has balanced audio and SDI/HDMI outputs. Shown for all models.
 - **Unbalanced:** the rear panel has unbalanced audio and SDI/HDMI outputs. Shown for all models.
 - **Balanced/Dual-SDI:** the rear panel has balanced audio and dual SDI outputs. Available only for the 9990-DEC-MPEG openGear card, and only supported for Rev 2 hardware or later.
 - **Unbalanced/Dual-SDI:** the rear panel has unbalanced audio and dual SDI outputs. Available only for the 9990-DEC-MPEG openGear card, and only supported for Rev 2 hardware or later.
- **Card Uptime:** Indicates how long the card has been running since it was last rebooted.
- **Ambient Temperature:** Temperature, in degrees centigrade, of the air intake of the card (measured at the front edge of the card).
- **Internal Temperature:** Temperature, in degrees centigrade, at the back of the card.
- **MDP Core Temperature:** Temperature, in degrees centigrade, of the core processing element.
- **Card Power (W):** Indicates the current power draw of the unit, in watts.

The DEC-MPEG is designed to operate in environments with an ambient temperature between 0 and 50 °C.

The BBG-1190-DEC-MPEG includes two additional indicators in the Product tab:



The BBG-1190-DEC-MPEG has two internal redundant power supplies. Each power supply is capable of individually powering up the device. The **PS1 Status** and **PS2 Status** indicate the status of each of the internal power supplies, as follows:

-  **OK:** The power supply is working normally.
-  **No Power:** The power supply has failed and is not providing power. Contact product support to get the unit repaired.

Network Tab

The Network Tab allows for configuration/monitoring of the streaming Ethernet port.

Network Configuration Tab

The Network Configuration Tab is used to set the individual parameters for the streaming Ethernet port.

- The **Interfaces** tab is used to set the individual parameters for each of the Ethernet ports.
- The **RIST Tunnels** tab is used to manage RIST Main Profile tunnels.
- The **Authentication** tab is used to configure RIST Main Profile authentication options.

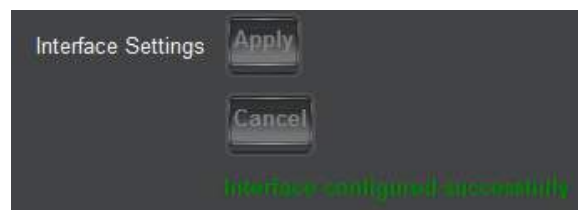
The screenshot shows a software interface with three tabs at the top: 'Network', 'ASI Input', and 'Decoder'. The 'Network' tab is selected. Inside the 'Network' tab, there is a sub-tab labeled 'Ethernet Configuration'. Below this, the 'Alarm on Link Loss' is set to 'Yes' with a radio button. The following fields are filled with text: 'IP Address' (10.10.9.90), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (0.0.0.0), 'DNS Server 1' (0.0.0.0), and 'DNS Server 2' (0.0.0.0). The 'IGMP Version' is set to 'Auto-Detect' and the 'Interface Speed' is set to 'Auto-Negotiate', both with dropdown arrows. At the bottom of the configuration area are 'Apply' and 'Cancel' buttons. At the very bottom of the window are three tabs: 'Interfaces', 'RIST Tunnels', and 'Authentication'.

Network Configuration Interfaces Tab

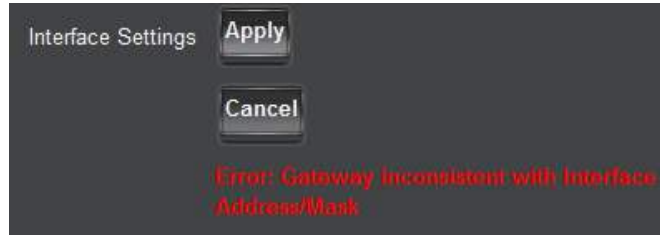
The following parameters can be configured:

- **Alarm on Link Loss:** If set to Yes, the card will raise an alarm if this Ethernet interface loses link. The Card State indicator in Dashboard™ and the front Status LED will both be red. If set to No, the card will still report loss of link in the Statistics page but no alarm will be raised. Cobalt Digital Inc. recommends turning on the alarm for ports that are in use; only turn it off if you do not plan to connect that port to a network.

-
- **IP Address:** Enter the desired IP address for this Ethernet port.
 - **Subnet Mask:** Enter the desired subnet mask for this Ethernet port.
 - **Default Gateway:** Enter the desired default gateway for this Ethernet port, or 0.0.0.0 if no gateway is available.
 - **DNS Server 1, DNS Server 2:** Enter up to two DNS IP addresses, or 0.0.0.0 if the DNS functionality is not required. The DEC-MPEG will need to consult a DNS server when operating as an HLS or RTMP client, if the servers are to be specified by host names instead of IP addresses⁵.
 - **IGMP Version:** The DEC-MPEG implements the IGMP protocol for multicast reception. This parameter controls the version of the protocol to be used.
 - **Auto-Detect:** The DEC-MPEG will attempt to auto-detect the IGMP version in use by inspecting the Group Membership Requests received from the router. It defaults to IGMP Version 3 if no messages are received.
 - **IGMP Version 1:** Force the use of Version 1 only (not recommended)
 - **IGMP Version 2:** Force the use of Version 2 only
 - **IGMP Version 3:** Force the use of Version 3 only
 - **Interface speed:** Configures the speed of the interface. The following modes can be selected:
 - **Auto-Negotiate:** The Ethernet port will auto-negotiate the speed. All modes are available.
 - **100 Mb/s Full-Duplex:** Force the port to 100Mb/s Full-Duplex mode. Note that the port will still perform auto-negotiation, but it will only advertise this mode.
 - **1Gb/s Full-Duplex:** restrict the operation to 1Gb/s Full-Duplex mode. Note that the port will still perform auto-negotiation, but it will only advertise this mode.
 - **Interface Settings:** If you make any changes to the IP Address, Subnet Mask, Default Gateway and/or DNS fields, the **Apply** and **Cancel** buttons become active. The changes only take effect when you press the **Apply** button. Pressing the **Cancel** button reverts the fields back to their original values. Note that the DEC-MPEG will check the consistency of the data entered and will reject invalid combinations. Once the **Apply** button is pressed, a status message appears just below the **Cancel** button, as follows:



⁵ If the DEC-MPEG has connectivity to the Internet and there is no DNS in your local network, Cobalt Digital Inc. recommends using the Google public servers at addresses 8.8.8.8 and 8.8.4.4.



Note: If default gateways are defined for both the control and streaming ports, the streaming port default gateway will be used to reach RTMP, RTSP and HLS servers, and the control port default gateway will be used to reach DashBoard and SNMP managers.

Network Configuration RIST Tunnels Tab

This tab allows the creation and management of RIST Main Profile tunnels. The DEC-MPEG supports the creation of one RIST Main Profile tunnel. Creation of RIST tunnels requires the **+RIST/ARQ-DEC** license. RIST Main Profile tunnels use the GRE over UDP protocol.

In order to create a tunnel, check the **Tunnel Enable** box below:



Once the box is checked, the tunnel parameters are shown:

- **Tunnel IP:** this is the inner IP address of the encoder in the tunnel. It is not usually necessary to configure this parameter.
- **Tunnel Mask:** this is the subnet mask for the tunnel interface. It is not usually necessary to configure this parameter.
- **UDP Port:** this is the UDP port to be used in the tunnel establishment, as follows:
 - If the DEC-MPEG is a **Server**, it will listen on this UDP port for incoming tunnel connections.
 - If the DEC-MPEG is a **Client**, it will attempt to connect to this port in the server.
- **Tunnel Mode:** The DEC-MPEG can be either a **Server** or a **Client**. If it is a server, it will wait to be contacted. If it is a client, it will actively attempt to contact the server. If **Client** is selected, an additional field appears where the server IP address can be entered:

- **Interface:** selects the network interface to use for this communication. The value of **Any** allows the device to select the most convenient interface based on the IP address. In particular, if the BBG-1090/1190-DEC-MPEG is configured as a server, it will accept incoming connections on both control and streaming Ethernet ports if the interface is set to **Any**.

- **Reduced Overhead:** RIST Main Profile defines a Reduced Overhead mode where only a simplified header. This reduces the overhead from 2.4% to 0.6%. This checkbox enables the use of Reduced Overhead mode for transmitted packets. Note that the DEC-MPEG automatically detects incoming reduced overhead packets.
- **Remap UDP:** This box, if checked, causes the DEC-MPEG to assume that all UDP packets coming in from the tunnel are destined to it regardless of their destination address. This control disappears in Reduced Overhead mode.
- **Encryption:** If this box is checked, the tunnel will be encrypted using DTLS, with optional authentication. Checking this box requires the **+RIST/ENCRP-ENC** license. Once this box is checked, the following additional options become available:

The screenshot shows a configuration window with the following settings:

- Encryption:** Checked (checkbox with a checkmark).
- Authentication:** Not checked (checkbox).
- Allowed Ciphers:** A row of five buttons: **AES128-RSA**, **AES128-ECDSA**, **AES256-RSA**, **AES256-ECDSA**, and **NULL**. Below each button is a checkbox. The checkboxes for **AES128-RSA**, **AES128-ECDSA**, **AES256-RSA**, and **AES256-ECDSA** are checked. The checkbox for **NULL** is not checked.

- **Authentication:** If this box is not checked, the DEC-MPEG will accept encrypted connections from any other device (regardless of whether it is operating as a client or a server). If it is checked, only authenticated connections will be accepted. Note that authentication requires prior setup to define acceptable connections; simply checking this box without any preparation will cause all connections (both incoming and outgoing) to fail. For a detailed explanation of how to set up the authentication function, please consult the section entitled “RIST Main Profile Authentication” later in this manual.
- **Allowed Ciphers:** When the DEC-MPEG negotiates an encrypted channel with a remote peer, it will negotiate a cipher suite, which includes both encryption and authentication options. This list indicates which cipher suites the DEC-MPEG is allowed to negotiate. The full names of the cipher suites are:
 - **AES128-RSA:** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - **AES128-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - **AES256-RSA:** TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - **AES256-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - **NULL:** TLS_RSA_WITH_NULL_SHA256

Notes:

- The **NULL** cipher has **NO ENCRYPTION**, only authentication. It is provided for testing purposes and **should not be enabled in production**.
- The use of AES 256 encryption is not allowed in some jurisdictions. Check your local laws before enabling.
- If there are no common ciphers enabled between the DEC-MPEG and the peer, the connection will fail to be established.
- The DEC-MPEG will negotiate the most secure cipher suite available. AES256 is preferred over AES128, and, for authentication, ECDSA is preferred over RSA.

- **Restart Tunnel:** This button causes a configured tunnel to disconnect and reconnect. Note that if the DEC-MPEG is a server, it will be up to the peer to reconnect.
- **Apply/Cancel:** Each tunnel has independent Apply/Cancel buttons. Clicking on **Apply** causes the configuration changes to become active and persisted. Clicking on **Cancel** causes any changes to be discarded.

Network Configuration Authentication Tab

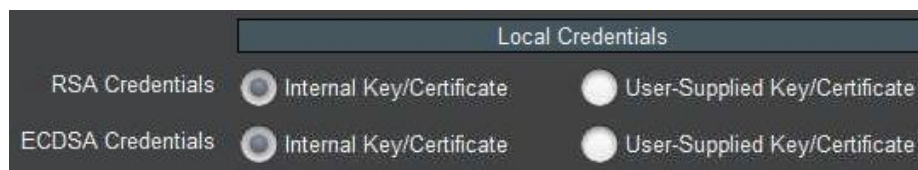
This tab controls the authentication options that are common for all RIST tunnels. Setting up authentication also requires access to web pages exposed by the DEC-MPEG. The section entitled “RIST Main Profile Authentication” later in this document provides a detailed explanation of this process, and shows the relationship between the controls presented here and the web interface.

Access to the web interface is controlled by these settings:



- **Web Interface Password:** Web interface operations that are privileged require a password. This configuration item sets the password. You can select any password and enter it here. When executing a web interface operation that requires a password, use the same password there. The default password is **Admin** and it is strongly recommended that it be changed to something else.
- **Enable Web Config:** For security reasons, the web interface should only be enabled on Ethernet ports connected to a secured management network. Checking the box enables the web interface in the corresponding Ethernet port. If the box is not checked, the web interface is not available in that port.

The next section of the authentication tab pertains to the credentials the DEC-MPEG uses for itself when negotiating a connection with a peer. The DEC-MPEG has built-in keys and certificates. Using the web interface, custom keys and certificates can be uploaded to the device. The settings below select whether the DEC-MPEG will use the built-in keys and certificates or the user-supplied keys and certificates:



Notes:

- The RSA and ECDSA methods use different keys and certificates. Independent choices can be made for these two methods.
- The **User-Supplied Key/Certificate** option can only be selected if a user-supplied set of credentials has been previously uploaded to the device. The process of uploading credentials is described in the section entitled “Uploading Keys and Certificates” later in this manual.

This section of tab controls how the DEC-MPEG authenticates remote devices:

If authentication is enabled, the DEC-MPEG will agree to communicate with any peer presenting a certificate signed by a trusted Certificate Authority (CA). The DEC-MPEG has a built-in CA, or an external CA certificate can be uploaded to it. Uploading an external CA certificate is done through the web interface; the process is described in the section entitled “Option 1: Use an External Certificate Authority” later in this document. The **CA Selection** configuration item can choose between the local CA and the user-supplied CA. Note that selecting **User-Supplied CA Certificate** can only be done after a certificate is actually uploaded.

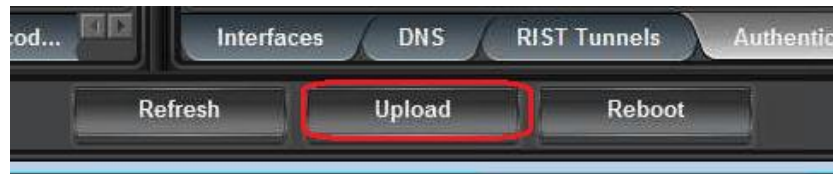
The DEC-MPEG implements a blocked device list. This is a list of devices which have proper credentials (i.e., a certificate signed by the trusted CA) but should not be allowed to connect. Devices are identified by their **Common Name (CN)**. Section “Creating a Blacklist” later in this manual provides more detail on this process.

If you made any changes to the above parameters, these changes only take effect after you click on the **Apply** button. Clicking on the **Cancel** button reverts the changes.

If you are using the built-in CA in the DEC-MPEG, it is important to back up its CA key. This section of the GUI provides this functionality:

Clicking on the **Save** button will generate a file called **CA_KEY.BIN** with the device's internal CA key. This file is encrypted and uses a proprietary format; it is not compatible with any third-party application.

If you need to restore a saved CA key to another Cobalt device, use the standard DashBoard upload function, available at the bottom of any tab:



Once the file is uploaded and validated, it is automatically installed as the device's CA key. A CA certificate is automatically generated to match this key, and can be downloaded through the web interface. An overview of the process can be found in the section entitled "Authenticating Remote Devices" later in this manual.

If you uploaded a new CA key to the DEC-MPEG but later decide to revert to the original built-in key, this can be done simply by clicking on this button:



Network Statistics Tab

The Network Statistics Tab reports the current IP configuration the Ethernet port, as well as its link state and running status.

Network Statistics Interfaces Tab

The following parameters are reported in the Network Statistics tab:

- **Alarm on Link Loss:** Reports the current setting of this parameter.
- **IP Address:** Reports the current IP Address for the port.
- **Subnet Mask:** Reports the current Subnet Mask for the port.
- **Default Gateway:** Reports the current Default Gateway for the port.
- **DNS Server 1, DNS Server 2:** Report the current DNS IP addresses.
- **IGMP Version:** Reports the current setting for this parameter.
- **Interface Speed:** Reports the current setting for this parameter.
- **Port 1 Link:** This indicator has the following states:
 - **Link OK:** The port has established link with the switch.
 - **No Link:** The port does not currently have link. If Alarm on Link Loss is set to Yes, the Dashboard™ Card State will be red and the Status LED in the front of the board will also be red. If Alarm on Link Loss is set to No, this indicator will still be red, but the alarm will not propagate.

-
- **Link Speed (Mb/s):** This parameter reports the actual speed negotiated with the switch for the port. If the port has no link, the value reported here is zero.
 - **MAC Address:** This reports the MAC address of the Ethernet port.

Ethernet Configuration	
Alarm on Link Loss	Yes
IP Address	10.10.9.128
Subnet Mask	255.255.255.0
Default Gateway	10.10.9.1
DNS Server 1	8.8.8.8
DNS Server 2	0.0.0.0
IGMP Version	Auto-Detect
Interface Speed	Auto-Negotiate
Port 1 Link	 Link OK
Link Speed (Mb/s)	1000
MAC Address	ac:83:f0:00:90:04

Network Statistics RIST Tunnels Tab

This tab shows the current configuration of the RIST tunnels. Only the enabled parameters are displayed.

RIST Tunnel 1

Tunnel Enable	Yes			
Tunnel IP	10.254.241.1			
Tunnel Mask	255.255.255.252			
UDP Port	5000			
Tunnel Mode	Client			
Server IP	10.10.9.14			
Interface	Ethernet 1			
Reduced Overhead	No			
Remap UDP	No			
Encryption	Yes			
Authentication	No			
	AES128-RSA	AES128-ECDSA	AES256-RSA	AES256-ECDSA
Allowed Ciphers	Yes	Yes	Yes	No

RIST Tunnels

Authentication

Tunnel Stats

Remote Info

Network Statistics Authentication Tab

This tab shows the current authentication options.

Authentication Web Interface	
Web Interface Password	*****
Ethernet 1 Ethernet 2	
Enable Web Config	No No
Local Credentials	
RSA Credentials	Internal Key/Certificate
ECDSA Credentials	Internal Key/Certificate
Remote Device Authentication	
CA Selection	Internal CA
Blocked Device 1	
Blocked Device 2	
Blocked Device 3	
Blocked Device 4	
Blocked Device 5	
Blocked Device 6	
Blocked Device 7	
Blocked Device 8	

Network Statistics Tunnel Stats Tab

This tab is only present if there is at least one tunnel enabled, and only has entries for the enabled tunnels. The content is displayed below.

RIST Tunnel 1 Statistics			
	TX	RX	Dropped
Full Datagram	8399	0	0
Reduced Overhead	0	0	0
Keep-Alive	1763	1757	0
TX Rate (b/s)	4,649,728		
RX Rate (b/s)	1,349		
Remote Endpoint	10.10.9.14:5000		
Remote Name	9992-DEC_AC:83:F0:02:00:40		
Remote MAC	ac:83:f0:02:00:40		
Current Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		

The fields are:

- **Full Datagram, Reduced Overhead, and Keep-Alive:** These fields show the number of received, transmitted, and dropped packets of each kind since the tunnel was established. A non-zero dropped count means that invalid packets are being received in the tunnel.
- **TX Rate (b/s):** This field shows the rate at which the DEC-MPEG is transmitting in the tunnel, in bits/second.
- **RX Rate (b/s):** This field shows the rate at which the DEC-MPEG is receiving packets from the tunnel, in bits/second.
- **Remote Endpoint:** This field shows the IP address and UDP port of the remote endpoint to which the DEC-MPEG is connected. If the tunnel is configured as a client, this should match the server IP address and UDP port. If the tunnel is configured as a server, this will report the client's IP address and UDP port (which does not necessarily match the port at which the server is listening).
- **Remote Name:** This field reports the Common Name (CN) of the remote device. If encryption is not being used, this field will be blank. Note that, if this field is blank when authentication is enabled, it means that the peer did not send a CN or sent a blank CN. If you turn on authentication, connections with this peer will be rejected.
- **Remote MAC:** This field reports the remote MAC Address, if supplied in the Keep-Alive message. This field will be blank if the remote side does not send RIST Keep-Alive messages. While Cobalt devices will always send this information, it is legal for third-party devices to not include it.
- **Current Cipher:** This field shows the canonical name of the cipher suite currently in use. It will be blank if encryption is not enabled.

Network Statistics Remote Info Tab

RIST Main Profile defines an optional informational Keep-Alive message. If such message is present, its contents will be displayed in this tab. While all Cobalt devices generate these messages in RIST Main Profile mode, it is legal for peers not to send them. If these messages are not present, all the fields in this tab will be blank.

RIST Tunnel 1 Remote Info	
Features	RBEVJ
Tunnel IP	10.254.241.2
Remote IP	
Routing	
Vendor	Cobalt Digital Inc.
Product	9992-DEC
Version	0.5.37-FS

The fields are:

- **Features:** The Keep-Alive message has a number of feature flags. This field shows which flags are present in the message, as follows:

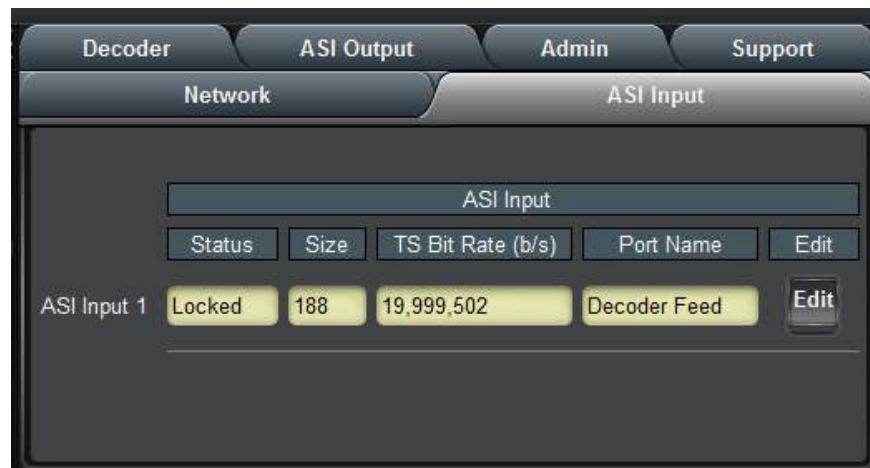
-
- **X:** More capabilities. If this flag is set, it indicates that there are more capabilities included in the message.
 - **R:** Routing capability. If this flag is set, the device is willing to transmit and receive non-RIST traffic.
 - **B:** If this flag is set, device supports Bonding.
 - **A:** If this flag is set, device supports Adaptive Encoding.
 - **P:** If this flag is set, device supports SMPTE-2022 FEC.
 - **E:** If this flag is set, device supports seamless redundancy switch as per SMPTE-2022-7.
 - **L:** If this flag is set, device supports load sharing.
 - **N:** If this flag is set, device supports NULL packet deletion.
 - **V:** If this flag is set, device supports Reduced Overhead Mode.
 - **J:** If this flag is set, device is capable of sending, receiving and processing JSON information.
 - **Tunnel IP:** This indicates the remote inner (tunnel) IP address, reported by the peer.
 - **Remote IP:** This indicates the IP address the peer would like the DEC-MPEG to take. This feature is not supported by the DEC-MPEG. This value, if present, will be reported here but ignored.
 - **Routing:** This indicates that the peer is capable of routing. Cobalt devices currently do not generate this flag.
 - **Vendor:** This indicates the vendor of the peer. Cobalt devices will report “Cobalt Digital Inc”.
 - **Product:** This indicates the product name of the peer. The DEC-MPEG will report “DEC-MPEG”.
- Version:** This indicates the software version currently running in the peer. The DEC-MPEG will report the value found in the **Software Rev** field found in the Product Tab.

ASI Input Port

The DEC-MPEG decoder has one fixed-function ASI Input Port. This tab is used to configure and manage it.

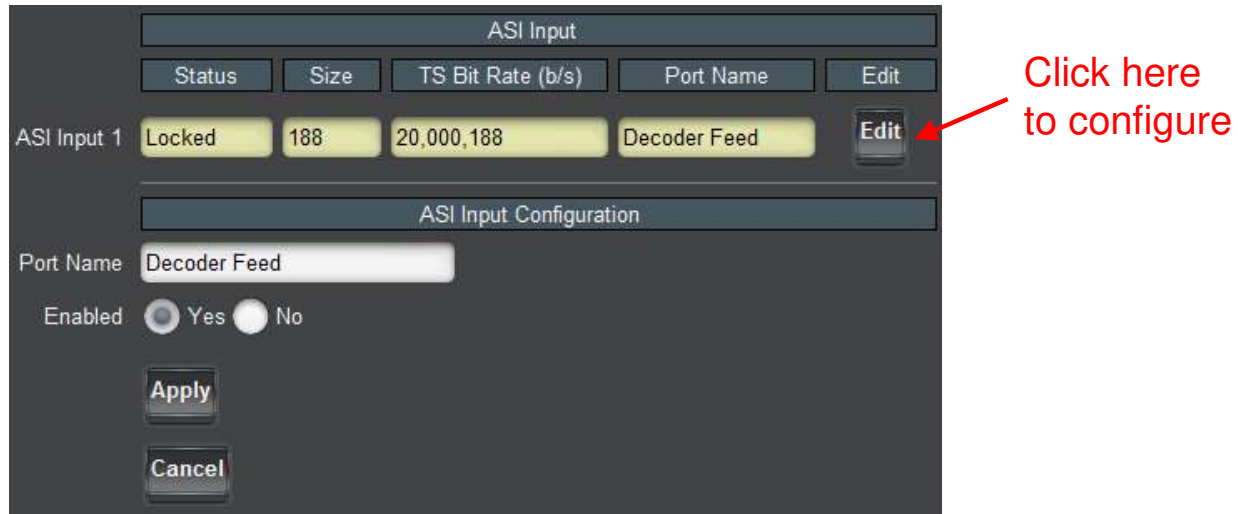
ASI Input: Configuration Tab

The Configuration Tab for the ASI inputs is shown below:



The Configuration tab is divided into two areas:

- The **ASI Input** table, which displays an overview of the ports. It contains the following fields:
 - **Status:** Indicates the current status of the port. The possible values are:
 - **Locked:** the port is enabled and locked to a valid ASI signal.
 - **Unlocked:** the port is enabled, but has no signal.
 - **Disabled:** the port is disabled by user configuration.
 - **Size:** Indicates the detected ASI transport packet size (188 or 204 bytes). If the port is disabled or unlocked, this field will show a value of 0 (zero).
 - **TS Bit Rate (b/s):** Measured transport stream bit rate, in bits/second.
 - **Port Name:** All DEC-MPEG ports can be assigned a user-defined name, which is displayed here. The default name is **ASI Input 1**.
 - **Edit:** This button, when clicked, brings up the configuration area of the port.
- The configuration area of the port, which is accessed by clicking on the **Edit** button, as shown below.



The following parameters are available:

- **Port Name:** All DEC-MPEG inputs and outputs can be assigned a user-defined port name. This name is used to identify the port later when making connections. Use any descriptive name suitable for your application, or accept the default.
- **Enabled:** the ASI Input can be enabled/disabled using this parameter. When the port is disabled, the corresponding LED in the front and back panels stays off.

Once the desired configuration is entered, click on the **Apply** button to have them take effect. This will cause the changes made in the Configuration Parameters to be implemented. Clicking on the **Cancel** button will discard any changes.

ASI Input: Statistics Tab

The Statistics Tab for the ASI Ports provides a quick visual summary status for the ports. A sample is depicted below:



The ASI Input Port indicator can have the following values:

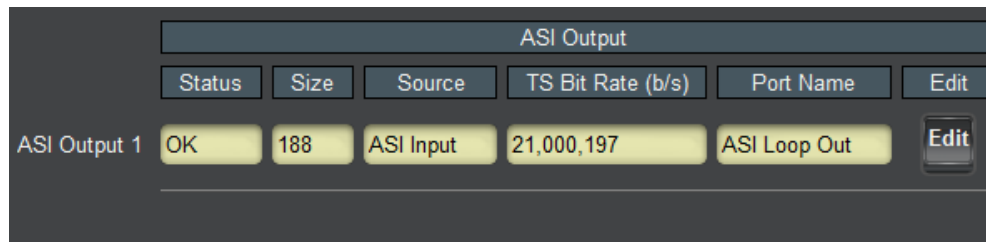
- **● RX Locked:** The port is locked to an input signal.
- **○ RX Disabled:** The port is disabled.
- **● RX Unlocked:** The port is not locked to any signal.

ASI Output Port

The DEC-MPEG decoder has one fixed-function ASI Output Port. This tab is used to configure and manage it.

ASI Output Port: Configuration Tab

The ASI Output Configuration Tab is show below:



	Status	Size	Source	TS Bit Rate (b/s)	Port Name	Edit
ASI Output 1	OK	188	ASI Input	21,000,197	ASI Loop Out	Edit

The **ASI Output** table is always displayed, and its columns are:

- **Status:** Indicates the port status. It can contain the following values:
 - **OK:** Port is operating normally.
 - **Unlocked:** Port is unlocked. This status means that the port is in Automatic mode and it has no input.
 - **Overflow:** This means that the ASI Output is in Manual mode, and the configured bit rate is insufficient to carry the input connected to it. This situation will raise an alarm.
- **Size:** Indicates the transport packet size, in bytes.
- **Source:** Indicates the current source for the data being outputted in the port.
- **TS Bit Rate (b/s):** This reports the actual transport stream bit rate, in bits/second.
- **Port Name:** This reports the configured Port Name.
- **Edit Button:** Clicking on this button allows reconfiguration of the port. The ASI Port Configuration screen appears, with the settings for the port.

Clicking on the **Edit** button will cause the configuration area of the port will to open, as depicted below. The configurable parameters are:

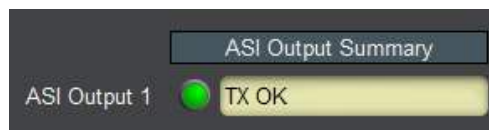
- **Port Name:** All DEC-MPEG inputs and outputs can be assigned a user-defined port name. This name is used to identify the port later when making connections. Use any descriptive name suitable for your application, or accept the default.
- **Packet Size:** Select between 188 or 204 bytes.
- **ASI Rate:** The available selections are:
 - **Manual:** In this mode, the ASI output bit rate is manually set. If the content routed to the port exceeds the configured bit rate, packets will be dropped and the port will raise an alarm.
 - **Automatic:** In this mode, the ASI output bit rate is automatically set by the DEC-MPEG to match the source connected to the port.

- **Bit Rate:** This field is only shown if the **ASI Rate** control is set to **Manual**. Enter the desired bit rate in bits/second.
- **Source:** This field indicates the source for the ASI Output content. For the current firmware version, the only option is the ASI Input content. Future versions of the firmware will offer additional options.

Once the desired configuration is entered, click on the **Apply** button to have them take effect. This will cause the changes made in the Configuration Parameters to be implemented. Clicking on the **Cancel** button will discard any changes.

ASI Output Port: Statistics Tab

The Statistics Tab for the ASI Output Port provides a quick visual summary status. An example is depicted below.



The ASI Port indicator can have the following values:

- **● TX OK:** The port is operating normally in transmit mode (ASI Output).
- **● TX Overflow:** The port is in manual bit rate setting, and the connected bit rate is excessive. The Dashboard Card State will be red and the Status LED in the front of the board will also be red. To correct this problem, either externally reduce the input bit rate, or increase the ASI output bit rate, or configure the port in Automatic mode. **If this alarm is active, data is being dropped.**
- **● TX Unlocked:** The port is in transmit mode, automatic bit rate, and there is no data rate coming to it. Any downstream ASI receivers will lose lock.

Decoder

The Decoder Configuration Tab contains the configuration parameters for the decoding function. The Statistics tab provides quick feedback on the configuration and status of the decoding process.

Decoder Configuration Tab

The decoder configuration tab is divided into two bottom tabs (depicted below):

- The **Configuration** tab, where all the main decoder parameters are configured.
- The **Program Info** tab, where program-specific information is displayed. If the decoder is in HLS mode, this tab allows for manual configuration of the decoded profile.



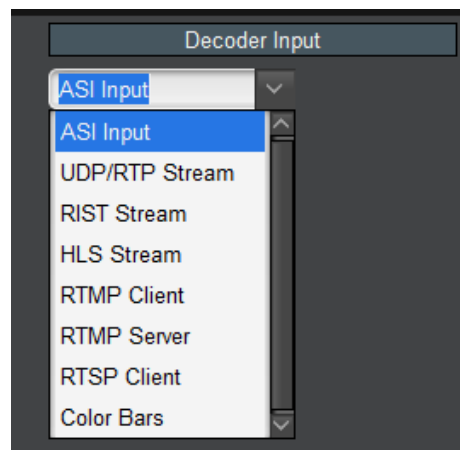
The decoder configuration tab is divided into the following functional areas:

- The **Decoder Input** configuration area
- The **Program and Audio Selection** configuration area
- The **Output Configuration** area
- The **Ancillary Data Injection** area
- The **Analog Audio Configuration** area
- The **Apply/Cancel** buttons

The settings displayed in each of the areas will vary according to the specific configuration.

Decoder Input Configuration

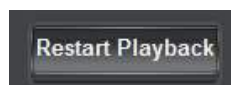
The primary decoder input configuration parameter is the **Source**, which selects the input and protocol from which the decoder will take its content:



The following stream sources are supported:

- **ASI Input:** the decoder will accept content on its ASI Input port.
- **UDP/RTP Stream:** the decoder will accept content on Ethernet over UDP/RTP, with optional support for SMPTE-2022 FEC. The DEC-MPEG also supports the notion of a backup flow – if the primary flow disappears, the decoder will switch to the backup. Note that, in the DEC-MPEG, multicast UDP/RTP streams are only accepted in the streaming Ethernet port.
- **RIST Stream:** the decoder will accept content using RIST. When needed, the decoder will send retransmission requests (ARQ) as per VSF TR-06-1.
- **HLS Stream:** the decoder will retrieve the stream in real-time from an HTTP Live Streaming web server.
- **RTMP Client:** the decoder will retrieve a Flash stream from an RTMP Server, such as the Adobe Media Server or similar.
- **RTMP Server:** the decoder will accept a Flash stream from a publishing RTMP client.
- **RTSP Client:** the decoder will connect to an RTSP server, such as an IP Camera, and play the content.
- **Color Bars:** the decoder will output standard color bars.

In all modes, the following button is available:

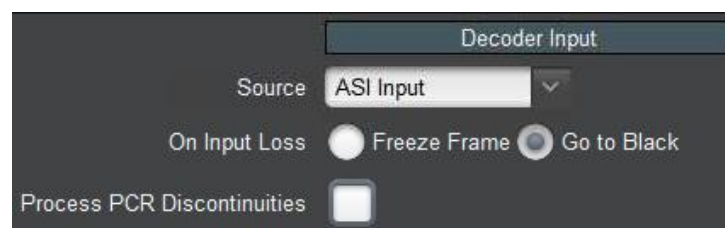


This button can perform a fast decoder restart if it stops for any reason and does not recover automatically.

The remaining parameters in the **Decoder Input** section will depend on the **Source** selection.

ASI Input

When ASI Input is selected, the following control becomes available:



- **On Input Loss:** selects the decoder behavior when the input signal disappears. If **Freeze Frame** is selected, the decoder displays the last valid frame; if **Go to Black** is selected, the decoder resets the signal and goes to black. The criterion for signal disappearance is loss of tables.
- **Process PCR Discontinuities:** selects the decoder behavior when there is a PCR discontinuity in the stream. If this box is checked, the DEC-MPEG will restart the

decoding process when there is a PCR discontinuity, otherwise it will attempt to keep decoding. If your stream stops and starts with different resolutions, check this box.

UDP/RTP Stream

When UDP/RTP Stream is selected, the following controls become available:

The screenshot shows a configuration window titled "Decoder Input". The "Source" is set to "UDP/RTP Stream". Below this, there are several controls: "On Input Loss" with radio buttons for "Freeze Frame" and "Go to Black" (the latter is selected); "Process PCR Discontinuities" with a checked checkbox; "Primary Reception" with radio buttons for "Unicast" and "Multicast" (the latter is selected); "Primary Source" with radio buttons for "Any Address" and "Specific Address" (the former is selected); "Primary Interface" with radio buttons for "Any", "Eth1", and "RIST1" (the former is selected); "Primary UDP Port" with a text field containing "2000" and a dropdown arrow; and "Redundant Reception" with an unchecked checkbox.

- **On Input Loss:** selects the decoder behavior when the input signal disappears. If **Freeze Frame** is selected, the decoder displays the last valid frame; if **Go to Black** is selected, the decoder resets the signal and goes to black. The criterion for signal disappearance is loss of tables.
- **Process PCR Discontinuities:** selects the decoder behavior when there is a PCR discontinuity in the stream. If this box is checked, the DEC-MPEG will restart the decoding process when there is a PCR discontinuity, otherwise it will attempt to keep decoding. If your stream stops and starts with different resolutions, check this box.
- **Primary Reception:** select between **Unicast** and **Multicast**. In **Unicast** mode, the stream must be sent to the decoder's streaming port IP address (see the Network Tab). In **Multicast** mode, the decoder will join an IP Multicast stream. When this mode is selected, a new field appears for the multicast address:

This close-up shows the "Primary Reception" section where "Multicast" is selected. Below it, the "Primary Multicast Address" is set to "226.10.1.1".

- **Primary Multicast Address:** enter the desired IP multicast address. The decoder will only accept addresses between 224.0.0.0 and 239.255.255.255 in this field.
- **Primary Source:** if this is set to **Any**, the DEC-MPEG will accept packets from any source IP address. If it is set to **Specific Address**, the DEC-MPEG will only accept packets from a specific address, and a new field appears to configure this address:

- **Primary Source Address:** enter the specific source IP address from which the DEC-MPEG will accept packets. If **Primary Reception** is set to **Multicast** and the DEC-MPEG is configured for IGMPv3 operation, it will generate source-specific IGMP Join messages.
- **Primary Interface:** the selections are:
 - **Any:** accept packets on any interface. That includes the control Ethernet port.
 - **Eth1:** only accept packets on the streaming interface Ethernet 1.
 - **RIST1:** only accept packets on the RIST tunnel. If the RIST tunnel is not configured, no packets will be received.
- **Primary UDP Port:** enter a valid UDP port. Valid values are between 1 and 65535.
- **Redundant Reception:** if this box is checked, a backup UDP flow can be configured. If the Decoder stops receiving packets in the primary flow, it will switch to the backup. When this box is checked, the following new fields appear:

- **Flip Time (s):** this configures how long the Decoder will wait to decide to flip between primary and backup streams.
- **Backup Reception, Backup Multicast Address, Backup Source, Backup Source Address and Backup Interface:** these controls operate in the same fashion as the primary ones described above.
- **Flip Redundancy:** if this button is clicked, the Decoder will manually flip to the other stream (i.e., if it is receiving from the primary, it will go to the backup, or vice-versa).
- **Reset Network Statistics** button: when clicked, this button causes the UDP/RTP statistics shown in the Network Tab on the Statistics area to be cleared. This is useful to manage network performance (i.e., packet loss) from a known state.

The DEC-MPEG will automatically detect UDP/RTP/SMPTE-2022 FEC (if licensed).

RIST Stream

When RIST Stream is selected, the following controls become available:

The screenshot shows a configuration window titled "Decoder Input". The "Source" is set to "RIST Stream". Under "On Input Loss", "Go to Black" is selected. "Process PCR Discontinuities" is unchecked. Under "Multi-Link", "Single Link" is selected. "Primary Reception" is set to "Unicast". "Primary Source" is set to "Any Address". "Primary Interface" is set to "Any". "Primary UDP Port" is set to "2000". "Redundant Reception" is unchecked. The "RIST Configuration" section includes: "NACK Window (ms)" set to "2000", "Packet Retries" set to "10", "Reorder Buffer (ms)" set to "0", "Min Buffer (Pkts)" set to "0", "NACK Mode" set to "Bitmask", and "NACK Target" set to "Source IP".

- **On Input Loss:** selects the decoder behavior when the input signal disappears. If **Freeze Frame** is selected, the decoder displays the last valid frame; if **Go to Black** is selected, the decoder resets the signal and goes to black. The criterion for signal disappearance is loss of tables.
- **Process PCR Discontinuities:** selects the decoder behavior when there is a PCR discontinuity in the stream. If this box is checked, the DEC-MPEG will restart the decoding process when there is a PCR discontinuity, otherwise it will attempt to keep decoding. If your stream stops and starts with different resolutions, check this box.
- **Multi-Link:** this controls whether or not link aggregation is enabled. The options are:
 - **Single-Link:** if this is selected, the DEC-MPEG will receive a single network stream for the content. Primary/Backup operation is still supported, and is configured exactly as described in the UDP/RTP Stream section.

- **Multi-Link:** if this is selected, the DEC-MPEG will receive multiple network streams for the content. This applies both to bonding, where the stream is split into multiple paths and reassembled at the decoder, or seamless switching, where multiple copies of the stream are sent simultaneously, and they are merged at the decoder – if one copy stops coming, the other(s) are still available. The DEC-MPEG will automatically detect the mode of operation. If **Multi-Link** is selected, the following controls become available:

	Address	UDP Port	Interface	Source
Link 1	0.0.0.0	1024	Eth1	0.0.0.0
Link 2	0.0.0.0	1026	Eth1	0.0.0.0

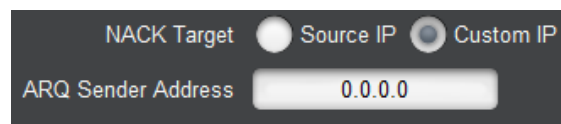
- **Number of Links:** enter the desired number of links (network flows). The DEC-MPEG supports up to 8 flows. A configuration table for the selected number of flows is automatically created.
- **Address:** enter a multicast address if desired. For unicast operation, leave at 0.0.0.0.
- **UDP Port:** enter the UDP port for the network flow.
- **Interface:** select the desired interface.
- **Source:** if you leave this at 0.0.0.0, the DEC-MPEG will accept packets from any source IP address. If you enter a unicast address here, packets will only be accepted from that address.

The remaining parameters represent the RIST-specific configuration:

- **NACK Window (ms):** enter the window, in milliseconds, for the NACK packets. The value entered here should be at least equal to the round-trip delay between the encoder and the decoder multiplied by the value of the **Packet Retries** setting. Note that the value of the NACK window adds to the end-to-end (glass-to-glass) latency.
- **Packet Retries:** enter how many times the DEC-MPEG should retry a dropped packet.
- **Reorder Buffer (ms):** enter the number of milliseconds the DEC-MPEG should wait for out-of-order packets to arrive. If the unit is not configured for multi-link operation, it is safe to leave this parameter at zero. If it is configured for multi-link, it should be at least the delay differential between the links.
- **Min Buffer (Pkts):** normally, the decoder will automatically compute its buffer size based on the RTP timestamps. This is the behavior if this control is left at 0 (zero). However, for non-compliant sources, the default buffer can be overridden by entering a non-zero value here.
- **NACK Mode:** VSF TR-06-1 defines two types of NACK messages:
 - **Bitmask** messages are the Generic NACK message defined in RFC 4585.
 - **Range** messages are defined in VSF TR-06-1.

Cobalt encoders support either type, so either setting can be used when interoperating with them. For third-party encoders, consult the vendor for the recommended setting.

- **NACK Target:** this parameter controls to which IP address the decoder will send the NACK packets. The options are:
 - **Source IP:** if this is selected, the decoder will send the NACK packets to the source IP address of the received bitstream. This is the most common case, when there are no firewalls between the encoder and decoder, or when the firewall at the encoder is configured to forward the packets transparently.
 - **Custom IP:** if this is selected, a custom IP address can be specified for the NACK packets. The decoder will send NACK packets to this IP address. When this is selected, the following field appears:

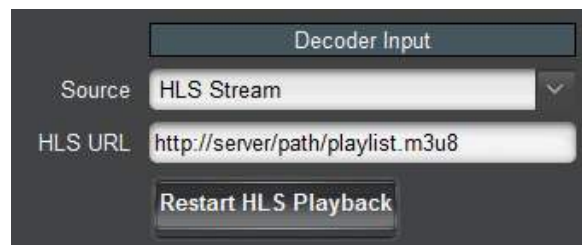


- **ARQ Sender Address:** send the NACK packets to this IP address instead of the source IP address of the received bitstream packets.
- **Reset Network Statistics** button: when clicked, this button causes the RTP/ARQ statistics shown in the Network Tab on the Statistics area to be cleared. This is useful to manage network performance (i.e., packet loss) from a known state.

RIST mode is also compatible with plain UDP streams, but no packet recovery will be possible.

HLS Stream

In this mode, the decoder can access and play a stream from a web server with an HTTP Live Streaming service. Access to the server can be either from the control or streaming ports. The configuration parameters are:



- **HLS URL:** Enter a valid HLS URL. The URL must start with **http://**⁶ and must end with either **.m3u** or **.m3u8**. In order to use a server name instead of an IP address, the decoder must have at least one DNS server configured and accessible. DNS servers can be specified in the Network Configuration Tab.

⁶ The BBG-1190-DEC-MPEG is not able to play HLS URLs that start with **https://**

-
- **Restart HLS Playback:** HLS content in the server may be a continuously-running live stream or a VOD stream. If it is a VOD stream, the decoder will stop at the end of the stream. Clicking on this button makes it play it again. The type of stream (Live or VOD) is reported in the Network Status Tab in the Statistics area.

RTMP Client

In this mode, the decoder can access and play a Flash stream from an RTMP Server such as the Adobe Media Server or similar. Note that not all Flash streams are supported. The DEC-MPEG will only support the following types of streams:

- Video Compression: H.264
- Audio Compression: MPEG-1 Layer III or AAC-LC.

An RTMP access point is defined by the following:

- An RTMP URL, of the form:

`rtmp[t][e][s]://servername/app`

- A stream name

The first part of the URL defines the protocol, as follows:

- **`rtmp`**: standard RTMP with no security
- **`rtmpt`**: RTMP tunneled over HTTP
- **`rtmpe`**: encrypted RTMP using proprietary security
- **`rtmps`**: encrypted RTMP over SSL
- **`rtmpte`**: encrypted RTMP using proprietary security, tunneled over HTTP
- **`rtmpts`**: encrypted RTMP over SSL, tunneled over HTTP

The **`servername`** field is the host name or IP address of the RTMP server to be contacted. The **`app`** field is the application in the server that should receive the data being transmitted. Note that, depending on the service, the **`app`** field may contain a complete path or even a set of parameters.

The RTMP Client configurable parameters are:

Decoder Input

Source: RTMP Client

RTMP Protocol: rtmp

RTMP Server: server

RTMP Port Selection: ☒ Use Default ☐ Specific Port

RTMP App: app

RTMP Server URL: rtmp://server/app

RTMP Stream: livestream

Authentication: ☒ No ☐ Yes

- **RTMP Protocol:** Select the protocol variant, as discussed above.
- **RTMP Server:** Enter the host name or IP address of the RTMP server to be contacted. If you want to use host names instead of IP addresses, make sure to configure at least one DNS server. DNS servers can be specified in the Network Configuration Tab.
- **RTMP Port Selection:** If your RTMP server is using the default TCP ports for the protocol variant, select **Use Default**. If your server is using a non-standard port, select **Specific Port**. When **Specific Port** is selected, an additional field is displayed:

RTMP Port Selection: ☐ Use Default ☒ Specific Port

RTMP Port: 1935

- **Port:** This field is only displayed if **RTMP Port Selection** is set to **Specific Port**. Configure a non-standard TCP port here.
- **RTMP App:** Enter the application name in the server, as discussed above. Consult your CDN or server documentation to find out what should be entered in this field.
- **RTMP Server URL:** This informational field is automatically updated as you configure the RTMP parameters. It displays the full RTMP URL for the primary server.
- **RTMP Stream:** Enter the stream name for the server. Consult your server documentation or CDN to find out what should be entered here. Some servers allow arbitrary stream names, while others use this field for authentication and thus require specific names.
- **Authentication:** Some RTMP servers require username/password authentication for access. If your server does not require authentication, select **No**, otherwise select **Yes**. If you select **Yes**, additional fields are presented:

Authentication: ☐ No ☒ Yes

Username: Cobalt

Password: *****

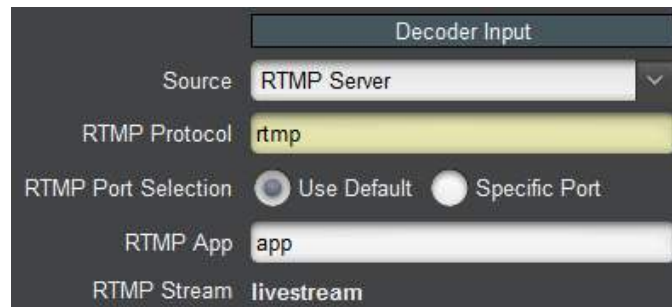
- **Username:** Enter the username to be used for authentication.

-
- **Password:** Enter the password to be used for authentication.

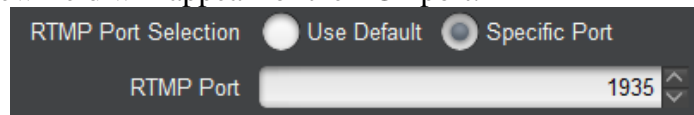
RTMP Server

In RTMP Server mode, the decoder waits for a publishing RTMP client to connect to it and publish a stream, which the decoder will then play. Please note that this mode requires a separate license.

The configuration parameters are as follows:



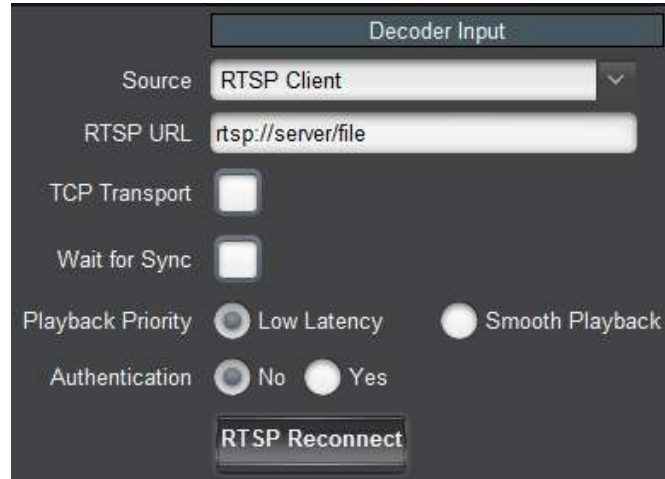
- **RTMP Protocol:** This is an informational field. The only supported variant is `rtmp://`.
- **RTMP Port Selection:** If **Use Default** is selected, the decoder will listen on the default RTMP Port (TCP Port 1935). If a custom, non-standard port is desired, select **Specific Port**, and a new field will appear for the TCP port.



- **Port:** This field is only displayed if **RTMP Port Selection** is set to **Specific Port**. Configure a non-standard TCP port here.
- **RTMP App:** any arbitrary name can be used here. Configure the exact same name in the encoder.
- **RTMP Stream:** this field is fixed at **livestream**. Configure this name in the encoder.

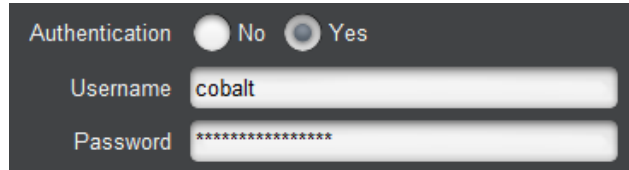
RTSP Client

In RTSP Client mode, the decoder will connect to an RTSP server (specified by an `rtsp://` URL), request a stream, and play the stream. This mode is intended primarily to support devices such as IP Cameras. The configuration parameters are as follows:



The parameters are:

- **RTSP URL:** Enter the full RTSP URL to access the RTSP server. Please consult the RTSP server vendor to find out what to enter here. A comprehensive list of URLs from the various IP Camera manufacturers can be found in [this link](#).
- **TCP Transport:** Standard RTSP uses a TCP connection to negotiate the streaming, and RTP/UDP on a dynamically-allocated port for the video content. This mode of operation is compatible with all RTSP devices, but it does not work well over the Internet nor can it go across most firewalls. Many RTSP cameras support tunneling the video over the control TCP connection, which works a lot better in complex networks, at the expense of increased latency. If this box is checked, the DEC-MPEG will request this tunnel mode. If this mode works with your camera, it is preferred.
- **Wait for Sync:** a few seconds after the stream start, the RTSP server may send a synchronization message, which is primarily intended to synchronize audio and video. Some RTSP cameras will send this even if they do not support audio. If you check this box, the decoder will only start playing after the synchronization message is received. Please keep in mind that some RTSP devices never send this message. It is suggested that this be disabled at first, and only enabled if there are startup problems.
- **Playback Priority:** this parameter controls the amount of buffering in the decoder, as follows:
 - **Low Latency:** the decoder will try the least amount of buffering, but if there are network issues, the video may stutter.
 - **Smooth Playback:** the decoder will buffer a fair amount of data (several seconds), so the playback is smooth, but at the expense of significantly more latency.
- **Authentication:** Some RTSP devices can be configured to require username/password authentication. Select **Yes** if this is the case. The following additional options are displayed:

A dark-themed dialog box for RTSP authentication. It features two radio buttons at the top: 'No' (unselected) and 'Yes' (selected). Below the buttons are two text input fields. The first field is labeled 'Username' and contains the text 'cobalt'. The second field is labeled 'Password' and contains a series of asterisks '*****'.

- **Username:** enter the username expected by the RTSP device.
- **Password:** enter the password expected by the RTSP device.
- **RTSP Reconnect:** if this button is clicked, the DEC-MPEG drops the RTSP connection and re-creates it.

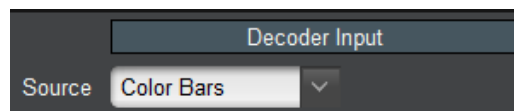
The decoder will automatically generate RTSP Keep-Alive messages once a minute, for RTSP servers that require it.

RTSP support in the DEC-MPEG has the following limitations:

- For audio, only AAC compression with sample rates of 48 kHz, 44.1 kHz, 32 kHz, 24 kHz, 22.05 kHz and 16 kHz are supported.
- Both elementary streams and transport streams are supported.
- For video, only H.264 compression is supported.
- No support for encrypted passwords.

Color Bars

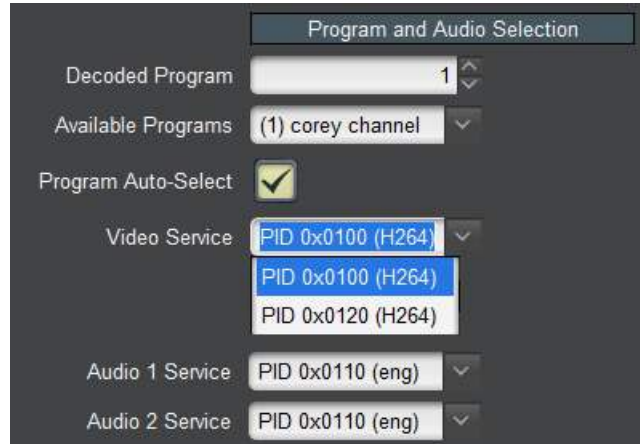
No additional parameters are required for Color Bars. Use the Decoder Output Configuration controls to specify the desired output, frame rate, and other video output parameters.

A dark-themed dialog box for Decoder Input Configuration. It has a title bar that says 'Decoder Input'. Below the title bar, there is a label 'Source' followed by a dropdown menu. The dropdown menu is currently open, showing 'Color Bars' as the selected option.

Decoder Program and Audio Selection

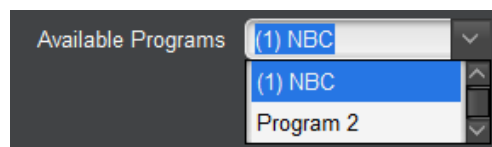
This section is only displayed if the **Source** parameter in Decoder Input Configuration is set to either **ASI Input**, or **UDP/RTP Stream**, or **RIST**. It allows the following selections to be made:

- If the stream being received by the decoder is a Multi-Program Transport Stream (MPTS), the program to be decoded can be chosen here.
- If the program being played by the decoder has multiple audio PIDs, the audio PIDs being decoded can be selected here.
- If the stream has multiple Video PIDs (e.g., multi-angle), the **Video Service** select drop-down allows selecting the desired video PID (in the example below, PID 0x100 and 0x120). For each available video PID, the type (MPEG-2 or H-264) is also shown in the drop-down.



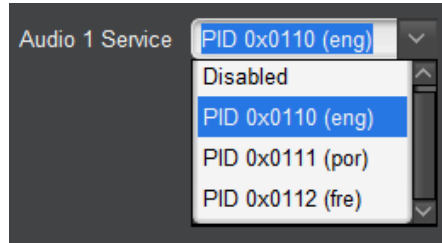
The parameters are:

- **Decoded Program, Available Programs:** These two parameters work together, and are used to select the program to be decoded in an MPTS. The program can be specified by number in the **Decoded Program** field, or selected in the **Available Programs** drop-down menu. If **Program Auto-Select** is checked, and a non-existing program number is entered in the **Decoded Program** field, the decoder will ignore the setting and stay on the current program.
- **Available Programs:** This control is pre-populated with a drop-down list of the programs available in the transport stream. If the program name can be determined, it will be shown, with the program number in parenthesis. If not, the program is shown as **Program X**, where **X** is the actual program number. In the example below, Program 1 has a name (NBC), so it shown as “**(1) NBC**”, and Program 2 does not have a name, so it is shown as **Program 2**.



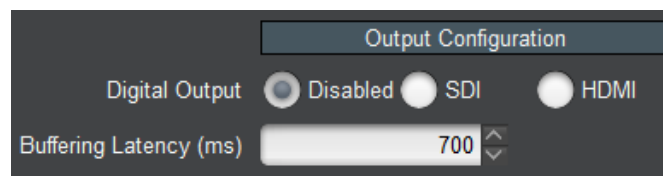
- **Program Auto-Select:** If checked, if the decoder does not find the configured program, it will automatically play the first program in the MPTS. Otherwise, it will not play any programs⁷.
- **Audio 1 Service, Audio 2 Service:** The DEC-MPEG has two independent audio decoders. These controls allow the selection of the audio service for each of the audio decoders. The selection is a drop-down menu with the audio PID values. If a language descriptor can be found for the audio service, the language code is displayed here as well. It is also possible to disable audio decoding altogether, by selecting the **Disabled** option. An example with three audio services (English, Portuguese and French) is shown below.

⁷ In the current firmware version, this control is not available and is always checked.



Decoder Output Configuration

This set of controls configures the video outputs. The appearance of the controls depends on the selection made on the **Digital Output** parameter:



The following parameter is always available:

- **Buffering Latency (ms):** the buffering latency through the decoder can be configured using this parameter. The range is from 200 to 700 milliseconds. It can be used to reduce overall end-to-end latency depending on stream delivery conditions. If this value is set too low for the network and encoding conditions, **the DEC-MPEG will stop decoding audio**. Increase the value in this case.

Digital Output: Disabled

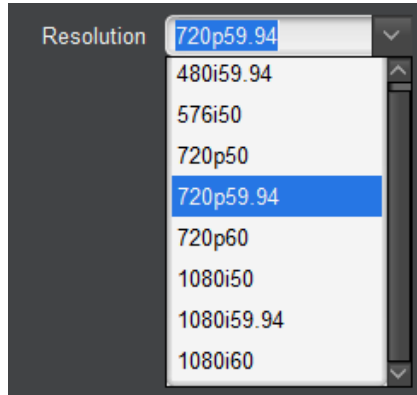
No additional parameters are displayed in this case. Both the SDI and the HDMI outputs will be disabled, and video will be present only in the composite output. The composite output will present either an NTSC or PAL signal depending on the program being decoded.

Digital Output: SDI

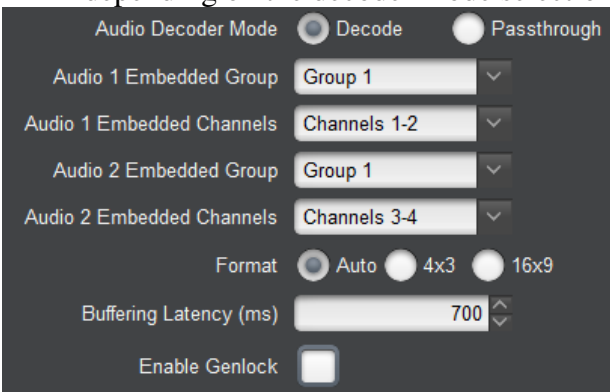
This selection enables the SDI output. The HDMI output will be disabled. The composite output will have an SD version of the signal. **Note that, in this mode, the decoder may output a garbled signal on the HDMI output. Do not use the HDMI output when SDI is selected, even if there is a signal present.**

The available parameters are:

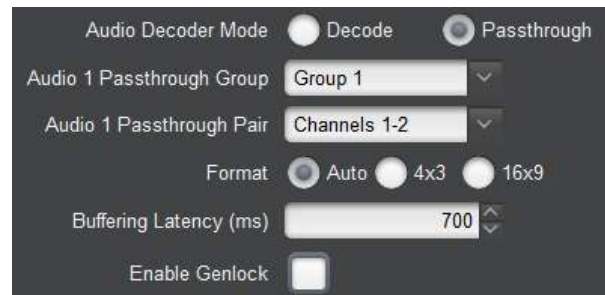
- **Resolution:** Select the SDI output resolution. The decoder can convert between formats and frame rates, so this selection can be made independent of the decoded signal. The available formats are:



- **Audio Decoder Mode:** The DEC-MPEG can either decode the audio PID, or pass the compressed bitstream directly into the SDI signal⁸. The remaining controls change depending on the decoder mode selection:



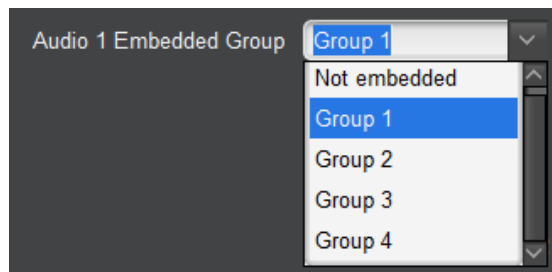
Audio Decode Mode options



Audio Passthrough Mode options

The BBG1190-DEC-MPEG can only pass-through only one audio PID. Therefore, in pass-through mode, only one Group/Pair selection is available. Note also that the **Audio 2 Service** selection in the Decoder Program and Audio Selection section will disappear in pass-through mode.

- **Audio 1 Embedded Group:** Select the group to embed the first decoded audio service. Groups 1 through 4 can be selected, or audio embedding can be disabled:



⁸ If the incoming audio is Dolby, no license is required for the pass-through function as the bitstream is not decoded.

- **Audio 1 Embedded Channels:** Select the channels to embed the first decoded audio. The available choices are **Channels 1-2** or **Channels 3-4**.
- **Audio 2 Embedded Group, Audio 2 Embedded Channels:** These controls are similar to the corresponding Audio 1 controls. They select the embedding of the second decoded audio pair.
- **Format:** This selects the output format. It is only relevant if the Decoder is decoding a Standard Definition (SD) signal and up-converting it to HD. Setting format to **4x3** will produce a pillarbox image (a 4x3 image with black bands on both sides). Setting format to **16x9** will stretch the image to full screen – this is recommended if the SD signal is anamorphic.
- **Enable Genlock:** If this box is checked, the SDI output can be genlocked to a reference signal. The following controls become available:



- **Genlock Line Offset:** By default, the Decoder will align the beginning of the video frames between the genlock reference and the SDI output. This control allows the offset to be changed by an integral number of lines. The available range for this parameter depends on the SDI output selection, as follows:

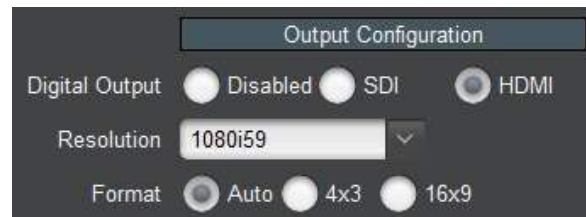
SDI Standard	Line Offset Range
480i	0 to 524
576i	0 to 624
720p	0 to 749
1080i	0 to 1124

- **Genlock Sample Offset:** By default, the Decoder will align the beginning of the video frames between the genlock reference and the SDI output. This control allows the offset to be changed by an integral number of samples (pixels) on either direction (negative or positive offset). The available range for this parameter depends on the SDI output selection, as follows:

SDI Standard	Line Offset Range
480i59.94	0 to 1715
576i50	0 to 1727
720p50	0 to 1979
720p59.94	0 to 1649
720p60	0 to 1649
1080i50	0 to 2639
1080i59.94	0 to 2199
1080i60	0 to 2199

Digital Output: HDMI

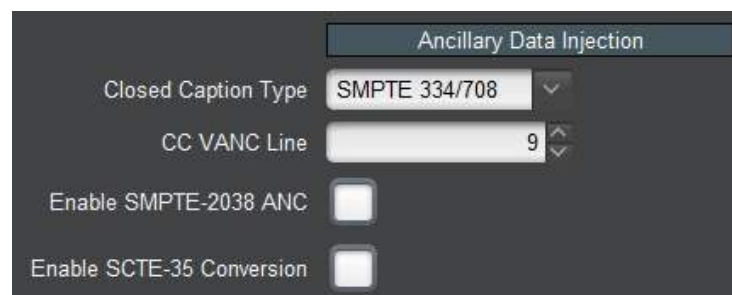
This setting enables the HDMI output. The SDI output will be disabled. Depending on the HDMI resolution settings, an SD version of the signal may be present in the composite output.



- **Resolution:** select the desired HDMI output resolution. You can choose a specific resolution, or select **Auto**. In **Auto** mode, the decoder will communicate with the HDMI monitor, determine its optimum resolution, and provide a signal of that resolution. Note the following for **Auto** mode:
 - If the monitor requests a non-standard resolution, the decoder will comply, but the composite signal will be turned off. If a composite signal is required, select one of the standard modes.
 - If the monitor does not complete the negotiation with the decoder, **no video will be displayed**. Select a standard resolution in this case.
- **Format:** This selects the output format. It is only relevant if the **DEC-MPEG** is decoding a Standard Definition (SD) signal and up-converting it to HD. Setting format to **4x3** will produce a pillarbox image (a 4x3 image with black bands on both sides). Setting format to **16x9** will stretch the image to full screen – this is recommended if the SD signal is anamorphic.

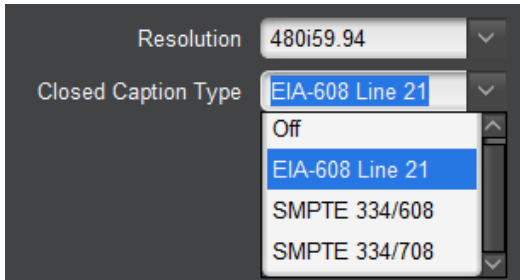
Decoder Ancillary Data Injection Configuration

This section is displayed only if the **Digital Output** control is set to **SDI**. It is depicted below.

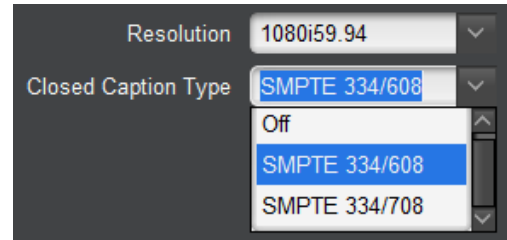


- **Closed-Caption Type:** The decoder supports Closed-Caption injection if the incoming bitstream has captions. The options are a function of output resolution:
 - **Off:** no Closed-Captioning injection.
 - **EIA-608 Line 21:** This option is only available if the resolution is set to 480i59.94. Closed captioning is inserted in Line 21.

- **SMPTE 334/608:** Inject Closed-Captioning using SMTE-334M in EIA-608 format.
- **SMPTE 334/708:** Inject Closed-Captioning using SMPTE-334M in EIA-708 format.

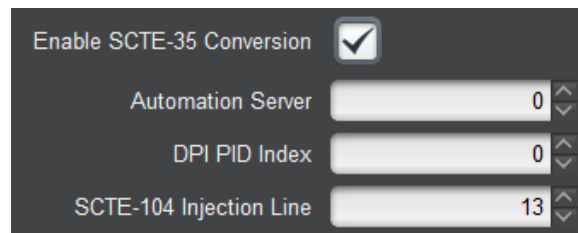


Closed-Caption options for 480i59



Closed-Caption options for all other resolutions

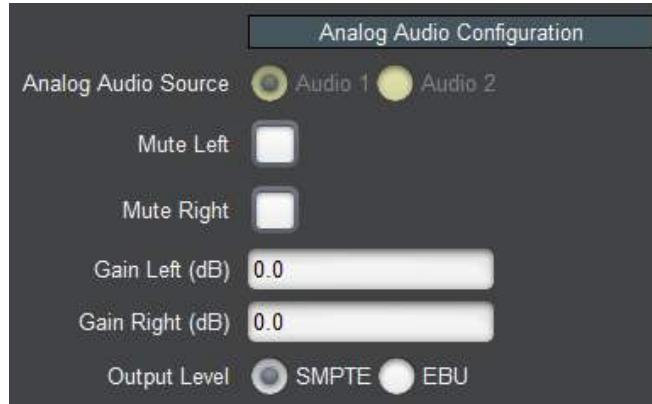
- **CC VANC Line:** This control is only displayed if **Closed-Caption Type** is set to one of the SMPTE 334 modes. It determines in which VANC line the closed-captioning is injected. The defaults are line 9 for HD and line 12 for SD.
- **Enable SMPTE-2038 ANC:** Where non-specific ANC has been included in the stream, the decoder can retrieve the encoded ANC and re-insert it into the outputted SDI stream (line location is the same as the line the encoder noted when integrating the ANC in the transport stream).
- **Enable SCTE-35 Conversion:** The decoder converts transport stream SCTE-35 sections back to SCTE-104 VBI ANC and re-inserts this data when the box is checked and applied. Once this box is checked, the following additional controls become available:



- **Automation Server:** This field is copied directly into the SCTE-104 message. It may or may not be relevant to your installation. Its usage is dependent on the equipment downstream to the decoder.
- **DPI PID Index:** This field is copied directly into the SCTE-104 message. It may or may not be relevant to your installation. Its usage is dependent on the equipment downstream to the decoder.
- **SCTE-104 Injection Line:** this field determines the line to be used to inject SCTE-104 messages. It is usually not necessary to change it from the default of 13.

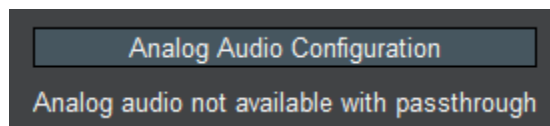
Decoder Analog Audio Configuration

This area configures the analog audio stereo output. It includes the following controls:



- **Analog Audio Source:** Selects between the first and the second decoded audio services for the analog output. This version of the firmware only supports the decoding of one service, so this control is not available. A future firmware update will enable this functionality.
- **Mute Left, Mute Right:** these controls will mute the corresponding audio analog output.
- **Gain Right, Gain Left:** these controls can provide independent audio gain or attenuation for the left/right channels. The range for these controls is from -12 dB to +12 dB, in steps of 0.5 dB.
- **Output Level:** This control is only displayed if the decoder is fitted with balanced audio outputs. Select between **SMPTE** and **EBU** output levels.

Note that if the DEC-MPEG is in SDI output mode (**Digital Output** set to **SDI** in the Decoder Output Configuration and **Audio Decoder Mode** is set to **Passthrough** (see Digital Output: SDI), analog audio decoding is not supported, and this section will disappear as follows:



Decoder Apply/Cancel Buttons

When the **Apply** button is clicked, the decoder configuration takes effect. All changes cause interruption to the video stream, except for changes related to audio – namely any changes in the Analog Audio Configuration or the Audio Service Selection.

If there are no errors, the Decoder configuration area closes. If any errors are detected, an error message is displayed by the **Apply** button. The possible error messages are:

- **Error: no available IP License:** the **Source** parameter in the Decoder Input Configuration is set to one of the IP protocols, and the unit does not have the IP License (check the Admin License Keys Tab). Contact Cobalt Digital Inc. if you need to acquire this license.
- **Error: no available RTMP Server License:** the **Source** parameter in the Decoder Input Configuration is set to RTMP Server, and the unit does not have the RTMP Server

License (check the Admin License Keys Tab). Contact Cobalt Digital Inc. if you need to acquire this license.

- **Error: no available Dolby License:** the incoming stream has Dolby audio, and the unit does not have the Dolby decoding license (check the Admin License Key Tab). If the program has other audio services, select an alternate audio PID in the Decoder Program and Audio Selection area. Contact Cobalt Digital if you need to acquire this license.
- **Error: no available Genlock License:** the **Enable Genlock** parameter in the Decoder Output Configuration is enabled, and the unit does not have the Genlock License (check the Admin License Keys Tab). Contact Support if you need to acquire this license

If the **Cancel** button is clicked, all changes are discarded, and the parameters return to their original values.

Decoder Program Info Tab

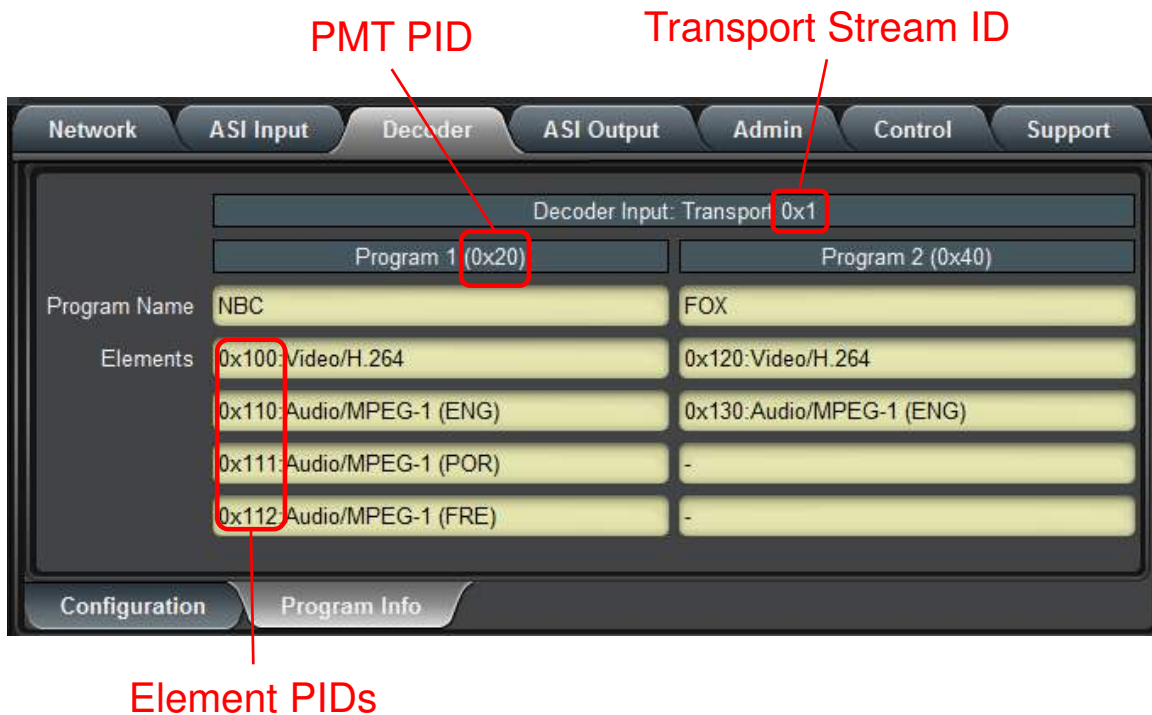
The information available in the **Program Info** tab depends on the setting of the **Source** parameter in the Decoder Input Configuration.



Program Info Tab for ASI Input and UDP/RTP Stream

For ASI Inputs and UDP/RTP Streams, the Program Info tab displays the information about the transport stream being received:

- **Header Information:** The top header indicates the Transport Stream ID (TSID). For each program, an individual header is provided, showing the Program Number and the PMT PID.
- **Program Name:** If available, the Program Name is displayed. If the transport stream contains a Service Description Table (SDT), the Service Name is displayed here. If the transport stream contains a Virtual Channel Table (VCT – used in terrestrial ATSC broadcasts), this field will show the major and minor channel numbers, and the short channel name (as depicted above).
- **Elements:** For each program, a list of elements is provided. The list contains the Element PID, the element type (Audio/Video/other), and the type of compression if appropriate. For audio streams, if a language code is present, it is displayed here as well.



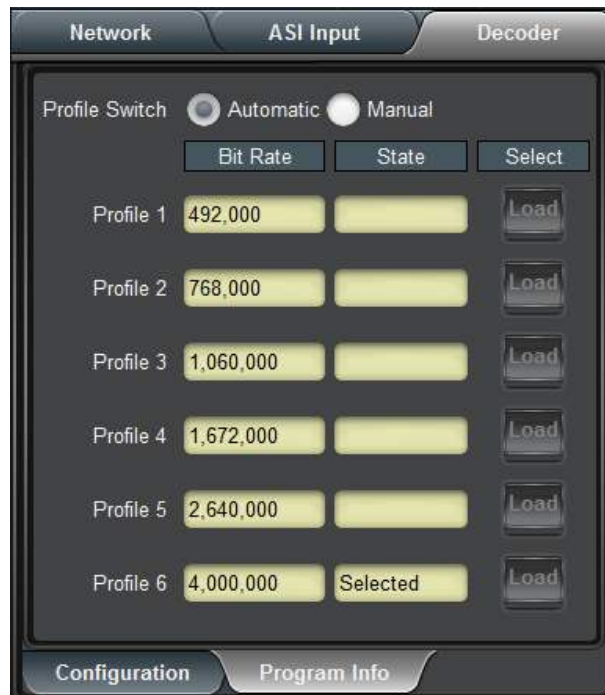
Program Info Tab for HLS Stream

For HLS Streams, the Program Info Tab shows the available profiles and their bit rates. It also shows which profile the decoder is currently downloading.

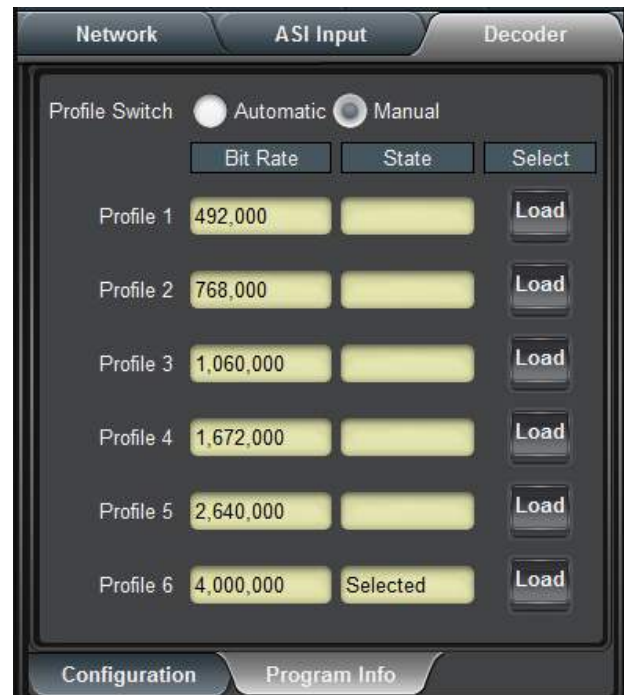
The controls available in this tab are:

- **Profile Switch:** If this is set to **Automatic**, the decoder will select the highest bit rate profile supported by its Internet connection. If this is set to **Manual**, the **Load** buttons in the **Select** column will become available, and a specific profile can be selected.
- **Load:** these buttons can be used to manually select one of the available profiles. If a button is pressed, the **State** entry next to it will indicate **Requested** until the decoder starts downloading that profile.

The table will also show the bit rate for each profile (as informed by the HLS server) and will indicate which profile is currently being downloaded – marked as **Selected** in the **State** column.



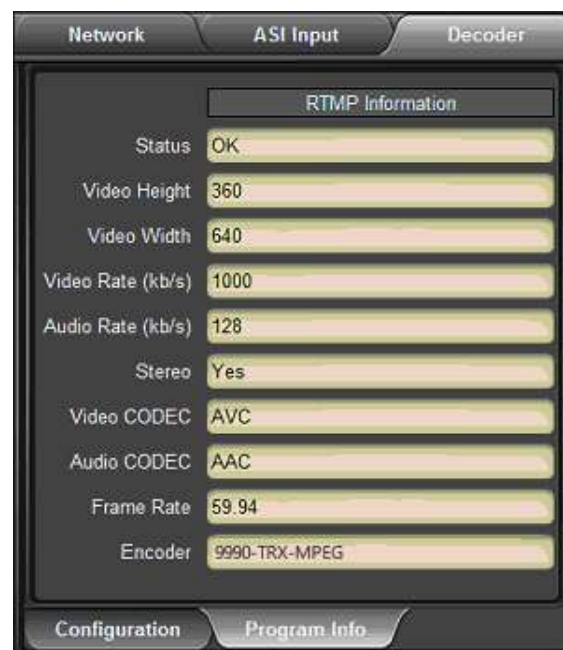
Automatic Profile Selection



Manual Profile Selection

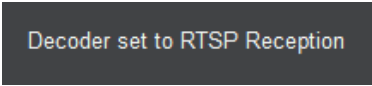
Program Info Tab for RTMP Client and Server

For RTMP Streams, the Program Info Tab shows the RTMP Metadata, if it has been provided by the client or the server.



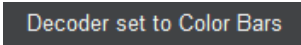
Program Info Tab for RTSP Streams

No additional information is presented for RTSP streams in the Program Info Tab:

A dark gray rectangular button with the text "Decoder set to RTSP Reception" in a light gray font.

Program Info Tab for Color Bars

No additional information is presented in the Program Info Tab when the decoder is in Color Bars mode:

A dark gray rectangular button with the text "Decoder set to Color Bars" in a light gray font.

Decoder Statistics Tab

The Decoder Statistics Tab is divided into four bottom tabs:



- The **Status** tab displays the current decoding status and information.
- The **Network** tab displays network statistics. It changes according to the decoder source selection.
- The **Ancillary Data** tab displays Closed Captioning and SMPTE-2038 presence. It also shows SCTE-104 insertion number and count of SCTE-35 errors detected..
- The **Configuration** tab is a mirror of the Configuration Tab and displays the current decoder configuration.

Status Tab

The Status Tab includes the following information:

- **Decoder State:** if this indicator is green, the content is being decoded normally. Otherwise, it will be red and the state of the decoder will be displayed.
- **Program Information:** this section contains general program information: program number, name (if available), and the PMT and PCR PIDs.
- **Video Information:** this section contains information about the video stream: PID, CODEC (H.264 or MPEG-2), resolution, and whether it is progressive or interlaced.
- **Audio Information:** if audio decoding is enabled, this section contains information about the stream being decoded. There are two audio information sections, one for each audio decoder. If the audio decoder is enabled, it contains the PID, CODEC, and language code (if present in the stream).

Decoder State	● Playing
Program Information	
Program Number	1
Program Name	NBC
PMT PID	0x20
PCR PID	0x101
Video Information	
Video PID	0x100
Video CODEC	H264
Video Resolution	1280x720
Video Mode	Progressive
Audio 1 Information	
Audio 1 PID	0x110
Audio 1 CODEC	MPEG
Audio 1 Language	eng
Audio 2 Information	
Audio 2 PID	0x111
Audio 2 CODEC	MPEG
Audio 2 Language	por

If the **Enable Genlock** control in the Digital Output: SDI section of the decoder configuration is checked, two additional information items are included in the Status Tab:

Decoder State	● Playing
Genlock Status	● OK
Genlock Signal	720x480i59.94
Program Information	
Program Number	1

- **Genlock Status:** this field can show the following values:
 - ● **OK:** The genlock function is operating normally, and the output is genlocked to the reference.
 - ● **Incompatible Reference:** The Decoder has detected a valid genlock signal, but the decoder output is incompatible with this genlock signal. Please consult the

genlock compatibility matrix below to confirm the supported combinations. The SDI output is **NOT** genlocked to this signal and is free-running.

- **Unlocked:** The Decoder is not detecting any genlock signal. The SDI output is free-running.
- **Genlock Signal:** this field indicates the resolution and frame rate of the detected genlock signal.

Not all combinations of SDI output standard and genlock signal are supported. The matrix below indicates what combinations are legal.

Genlock Compatibility Matrix

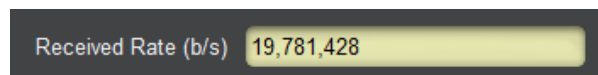
		SDI Output Signal							
		576i50	720p50	1080i50	480i59	720p59	1080i59	720p60	1080i60
Genlock Signal	576i50	√	√	√					
	720p50		√						
	1080i50	√	√	√					
	480i59				√	√	√		
	720p59					√			
	1080i59				√	√	√		
	720p60							√	
	1080i60							√	√

Network Tab

The Network Tab contains protocol-specific statistics and changes according to the decoder source selection.

Network Tab for ASI Input

The only parameter displayed is the measured input bit rate from the ASI port. This is the same value also displayed in the ASI Input: Statistics Tab.



Network Tab for UDP/RTP Stream

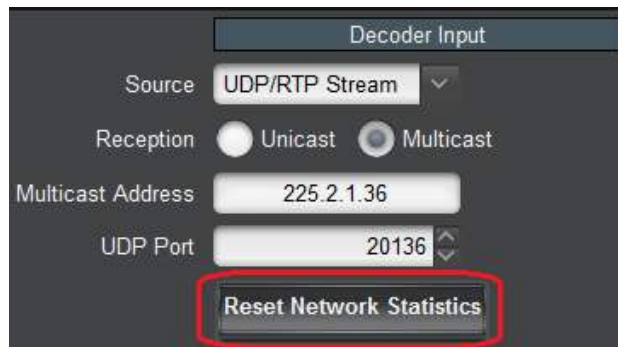
The following statistics are displayed for UDP/RTP:

Received Rate (b/s)	6,002,482
Protocol	RTP
Stream Source IP Address	10.10.9.75
Current Source	Primary
SMPTE 2022 FEC	Row and Column
Columns	10
Rows	10
Received Packets	794193870
Lost Packets	0
Recovered Packets	0
Unrecovered Packets	0
Invalid FEC Packets	0

- **Received Rate (b/s):** indicates the measured rate in bits/second at the input of the decoder. This does not include FEC bit rate or UDP/IP overhead – it is the transport stream rate.
- **Protocol:** indicates the detected protocol, either UDP or RTP.
- **Current Source:** indicates **Primary** or **Backup**.
- **Stream Source IP Address:** indicates the current IP address from which the stream is being received.
- **SMPTE 2022 FEC:** Indicates the detected FEC mode, as follows:
 - **None:** SMPTE 2022 FEC transmission is not being detected by the **DEC-MPEG**.
 - **Column Only:** The DEC-MPEG is detecting SMPTE 2022 FEC in Column Only mode.
 - **Row and Column:** The **DEC-MPEG** is detecting SMPTE 2022 FEC in Row and Column mode.
 - **Not Licensed:** The SMPTE 2022 functionality is not licensed in this unit (see the Admin License Keys Tab). If SMPTE 2022 FEC is present, it is being ignored by the DEC-MPEG.
- **Columns:** If SMPTE 2022 FEC is being received, this indicates the number of columns detected.
- **Rows:** If SMPTE 2022 FEC is being received, this indicates the number of rows detected.
- **Received Packets:** Indicates the number of packets received since the last time the statistics were reset. This count does not include the FEC packets, if any.
- **Lost Packets:** Indicates the total number of lost packets since the last time the statistics were reset. Note that the DEC-MPEG can only detect lost packets if the incoming protocol is RTP. It is not possible to detect lost packets with UDP as it lacks a sequence number.

-
- **Recovered Packets:** Indicates the total number of packets recovered with SMPTE 2022 FEC since the last time the statistics were reset.
 - **Unrecovered Packets:** Indicates the total number of lost packets that could not be recovered with SMPTE 2022 FEC (either because of excessive loss or because SMPTE 2022 is not present).
 - **Invalid FEC Packets:** Indicates the count of received FEC packets which have invalid protocol fields. If this count is non-zero we recommend you contact your encoder vendor.

The counts for Received Packets, Lost Packets, Recovered Packets, Unrecovered Packets and Invalid FEC Packets can be reset at any time by clicking on the **Reset Network Statistics** button in the configuration area of the Decoder Input configuration, also reproduced below:



Network Tab for RIST Stream

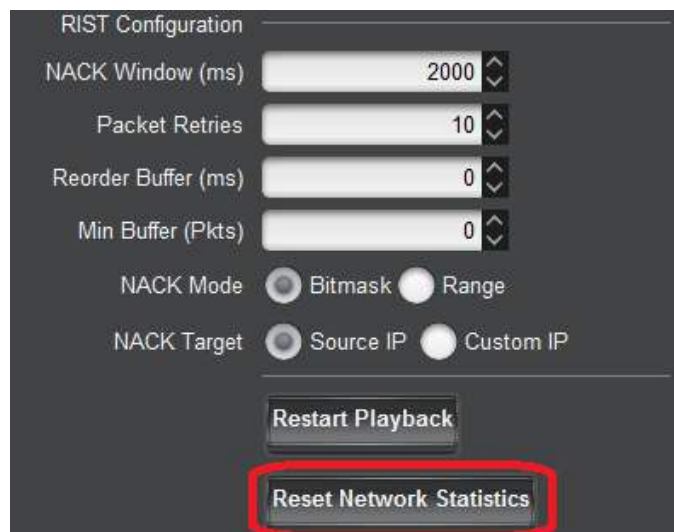
The following statistics are displayed for RIST:

Received Rate (b/s)	4,705,911
Protocol	RTP
Stream Source IP Address	10.10.9.82
Current Source	Primary
Received Packets	28282
Retransmissions Received	98
Lost Packets	1638
Recovered Packets	0
Unrecovered Packets	0
NACKs Sent	78
Late Packets	0
Duplicate Packets	98
RTCP Received	695
RTCP Source IP Address	10.10.9.82
RTCP Source Port	2001
RTT	1 ms
Buffer (Pkts)	852

- **Received Rate (b/s):** indicates the measured rate in bits/second at the input of the decoder. This does not include FEC bit rate or UDP/IP overhead – it is the transport stream rate.
- **Protocol:** indicates the detected protocol, either UDP or RTP.
- **Current Source:** indicates **Primary** or **Backup**.
- **Stream Source IP Address:** indicates the current IP address from which the stream is being received.
- **Received Packets:** indicates the number of packets received since the last time the statistics were reset.
- **Lost Packets:** indicates the total number of lost packets since the last time the statistics were reset. Note that the Decoder can only detect lost packets if the incoming protocol is RTP. It is not possible to detect lost packets with UDP as it lacks a sequence number.
- **Recovered Packets:** indicates the total number of packets recovered with RIST since the last time the statistics were reset.
- **Unrecovered Packets:** indicates the total number of lost packets that could not be recovered with RIST because a retransmission for them was never received.
- **NACKs Sent:** indicates the number of retransmission requests sent. Note that one retransmission request can ask for up to 17 packets, and a packet may be requested multiple times, so this number may be more or less than the number of lost packets.

- **Late Packets:** indicates the number of packets successfully received, but too late to be used (after the time they were supposed to be consumed). A non-zero count in this field indicates that the **NACK Window** should be increased.
- **Duplicate Packets:** indicates the number of packets that were received more than once. Duplicate packets do not create glitches or issues. A count of duplicate packets means that either there is delay variation in the network or packets are being received out-of-order.
- **RTCP Received:** indicates the number of RTCP packets received so far. The RIST transmitter will send RTCP packets to establish state in firewalls for the NACK packets from the receiver. A count of zero indicates that there may be a networking problem on the RTCP port (which is the stream port plus one), and that the packet loss protection may not be working.
- **RTCP Source Address:** indicates the source IP address for the RTCP packets. It is usually the same as the **Stream Source IP Address**.
- **RTT:** This indicates the round-trip time between the DEC-MPEG and the RIST sender. The RIST sender must implement support for the optional RTT Echo messages defined in VSF TR-06-1, otherwise this indicator will be blank.
- **Buffer (Pkts):** this indicates the current buffer size in packets.

The statistics can be reset at any time by clicking on the **Reset Network Statistics** button in the RIST Stream area of the Decoder Input configuration, also reproduced below:



Network Tab for HLS Stream

The Network Tab statistics for the HLS Stream are shown below:

Stream Source IP Address	172.231.63.91
Type	Live Stream
Profiles	10
Profile Rate (b/s)	2,305,600
Segments Loaded	14
Segment Duration (s)	10.0

- **Stream Source IP Address:** This field indicates the server IP address for the HLS top level URL. Note that the top-level manifest may point to different servers for the actual stream; this field only shows the server for the top-level manifest.
- **Type:** This field will contain the following values:
 - **Unknown:** the stream type is unknown.
 - **VOD:** the stream is VOD content. This means that it is finite, it has a well-defined end. The DEC-MPEG will stop playing the content at the end, use the **Restart HLS Playback** button in the HLS Stream configuration area to play it again.
 - **Live Stream:** the stream is live.
 - **Event:** the stream is an event. This means that it is finite, it has a well-defined end. The DEC-MPEG will stop playing the content at the end, use the **Restart HLS Playback** button in the HLS Stream configuration area to play it again.
- **Profiles:** indicates the number of profiles advertised by the server. You can get more information about the profiles in the Program Info Tab for HLS Stream.
- **Profile Rate:** indicates the bit rate of the current profile being downloaded, as advertised by the server.
- **Segments Loaded:** indicates the number of segments downloaded from the server since the connection was made.
- **Segment Duration (s):** Indicates the segment duration, in seconds, advertised by the server.

Network Tab for RTMP Client and Server

The Network Tab Statistics for the RTMP Client and Server modes is depicted below:

Received Rate (b/s)	905,467
Stream Source IP Address	192.168.129.48
RTMP Connection	● OK

- **Received Rate (b/s):** indicates the measured rate in bits/second at the input of the decoder.
- **Stream Source IP Address:** if there is an RTMP connection, it indicates the IP address of the source. In RTMP Client mode, this is the IP address of the RTMP Server from

which the decoder is pulling the stream. In RTMP Server mode, this is the IP address of the publishing client.

- **RTMP Connection:** this shows the RTMP connection state, as follows:
 - **Connected:** The decoder has established a connection with the RTMP server or client and is transferring data.
 - **Not Connected:** The decoder has not been able to connect to the RTMP server, or there is no RTMP client connected to it. If the decoder is in RTMP client mode, check the Admin Event Log Tab for possible reasons why it is unable to connect.

Network Tab for RTSP Client

The Network Tab Statistics for the RTSP Client is depicted below:

Received Rate (b/s)	1,593,211
Stream Source IP Address	98.100.155.39
RTSP Connection	 OK
Video Protocol	RTP
Video UDP Port	60694
Video CODEC	H264
Video Frame Rate	30
Audio Protocol	RTP
Audio UDP Port	33852
Audio CODEC	AAC

- **Received Rate (b/s):** indicates the measured rate in bits/second at the input of the decoder.
- **Stream Source IP Address:** if there is an RTSP connection, it indicates the IP address of the source.
- **RTSP Connection:** this shows the RTSP connection state, as follows:
 - **Connected:** The decoder has established a connection with the RTSP server and is transferring data.
 - **Not Connected:** The decoder has not been able to connect to the RTSP server.
- **Video Protocol:** RTSP creates a separate connection to transfer the video bitstream. This field contains a textual representation of the protocol name, obtained from the RTSP server.
- **Video UDP Port:** RTSP creates a separate connection to transfer the video bitstream, and the UDP port used in this transfer is dynamically negotiated with the server. This field

reports the UDP port number being used. Note that if the protocol is RTP, two consecutive ports are used. In the example above, port 59970 is being used for the video, and port 59971 is being used for RTCP.

- **Video CODEC:** This field contains a textual representation of the video CODEC, as reported by the server. The DEC-MPEG only supports H.264 in RTSP mode, but this field will always be updated.
- **Video Frame Rate:** This field contains the video frame rate, as measured by the decoder.
- **Audio Protocol:** RTSP creates a separate connection to transfer the audio bitstream. This field contains a textual representation of the protocol name, obtained from the RTSP server. This field will be empty if the RTSP stream does not have audio.
- **Audio UDP Port:** RTSP creates a separate connection to transfer the audio bitstream, and the UDP port used in this transfer is dynamically negotiated with the server. This field reports the UDP port number being used. Note that if the protocol is RTP, two consecutive ports are used. In the example above, port 33852 is being used for the audio, and port 33853 is being used for RTCP. This field will have a value of 0 (zero) if the RTSP stream does not have audio.
- **Audio CODEC:** This field contains a textual representation of the audio CODEC, as reported by the server. The BBG-1190-DEC-MPEG only supports AAC in RTSP mode, but this field will always be updated. This field will be empty if the RTSP stream does not have audio.

Network Tab for Color Bars

No additional information is presented in the Network Tab when the decoder is in Color Bars mode:

Decoder set to Color Bars

Ancillary Data Tab

The Ancillary Data Tab shows the current running status of received ANC such as closed captioning, SMPTE-2038, and SCTE-35 errors/SCTE-104 insertions. These indicators are only valid if the decoder is configured for SDI output.

Closed Captions	Not Present
SMPTE-2038	Present
SMPTE-2038 Inserted	111900
SCTE-104 Inserted	0
SCTE-35 Errors	0

- **Closed Captions:** indicates if closed-captions are present or not present in the SDI output.
- **SMPTE-2038:** indicates if SMPTE-2038 ANC packets are being inserted in the SDI output. Note that if the rate of SMPTE-2038 messages is low (i.e., 1 message/sec or

less), this indicator will show **Not Present**. Use the **SMPTE-2038 Inserted** count to monitor insertion.

- **SMPTE-2038 Inserted:** indicates the count of SMPTE-2038 ANC packets inserted so far.
- **SCTE-104 Inserted:** indicates the count of SMPTE-104 ANC packets inserted so far.
- **SCTE-35 Errors:** indicates the number of invalid SCTE-35 messages received. If this count is non-zero, please contact the vendor of the device generating the messages. Note that the decoder does not support DPI component mode, and will flag these as errors.

Configuration Tab

The Configuration Tab shows the current running configuration of the decoder. When the **Apply** button is pressed, the changes made in the configuration area are reflected here. It follows the same layout as the Decoder Configuration Tab. An example is shown below:

The image displays two screenshots of a decoder configuration interface, separated by three vertical dots. The left screenshot shows the 'Decoder' tab, and the right screenshot shows the 'Configuration' tab.

Decoder Tab Configuration:

- Decoder Input:**
 - Source: UDP/RTP Stream
 - On Input Loss: Go to Black
 - Primary Reception: Unicast
 - Primary UDP Port: 1026
 - Redundant Reception: No
- Program and Audio Selection:**
 - Decoded Program: 1
 - Available Programs: (1) corey channel
 - Program Auto-Select: Yes
 - Video Service: PID 0x0100 (H264)
 - Audio 1 Service: PID 0x0110 (eng)
 - Audio 2 Service: Disabled
- Output Configuration:**
 - Digital Output: SDI
 - Resolution: 1080i59.94
 - Audio Decoder Mode: Decode
 - Audio 1 Embedded Group: Group 1
 - Audio 1 Embedded Channels: Channels 1-2
 - Audio 2 Embedded Group: Group 1
 - Audio 2 Embedded Channels: Channels 3-4
 - Format: Auto
 - Buffering Latency (ms): 700
 - Enable Genlock: No

Configuration Tab Configuration:

- Ancillary Data Injection:**
 - Closed Caption Type: SMPTE 334/608
 - CC VANC Line: 9
 - Enable SMPTE-2038 ANC: Yes
 - Enable SCTE-35 Conversion: No
- Analog Audio Configuration:**
 - Analog Audio Source: Audio 1
 - Mute Left: No
 - Mute Right: No
 - Gain Left (dB): 0.0
 - Gain Right (dB): 0.0
 - Output Level: SMPTE

IP Outputs Tab

The DEC-MPEG is capable of doing ASI to IP turnaround, if it equipped with the optional IP Output license (see the Admin License Keys Tab). The output streams can be sent using UDP or RTP, and, if the unit has the SMPTE 2022 FEC license, it can also transmit a FEC stream.

The DEC-MPEG can also operate as a single-stream gateway for RIST streams, and retransmit a received RIST stream as a standard UDP or RTP stream.

The IP Output function is independent of the decoder source selection and is always available. For example, the decoder may be displaying a stream received from Ethernet, and at the same time transmitting an ASI stream over IP.

The IP Output function of the DEC-MPEG has the following capabilities:

- Protocol support: UDP, RTP and SMPTE-2022 FEC (if licensed)
- Full transport transmission
- MPTS splitting into multiple SPTS streams
- NULL-padding of SPTS streams
- Support for up to 16 IP flows
- Transmission always uses the streaming Ethernet port

IP Outputs Configuration Tab

The IP Outputs configuration tab is depicted below. It contains 16 pre-defined IP output streams, managed as follows:

- Stream 1 is always the full transport stream received from the ASI input.
- Streams 2 to 16 are SPTS streams, automatically pre-populated with the programs present in the ASI input, in the order they appear in the PAT.

The **Source** selection indicates whether the IP Outputs are being driven from the **ASI Input** or the **Current IP Input**. Note that IP Output turnaround is only available for RIST and UDP streams.

The most common settings and statistics for each stream are shown in the table below. Note that changes in the table take effect immediately. The columns are:

- **Program:** This column shows the program number for the specific stream. The possible values are:
 - **All:** this will only be shown for Stream 1, to indicate that it is the full transport.
 - **1 to 65535:** these are program numbers, read from the PMT.
 - **None:** this will be displayed for streams for which there are no available programs. These streams can be configured, but will only actually transmit if the transport changes and more programs appear.
- **Enable:** Checking this box enables transmission of a particular stream. This operation will fail if the DEC-MPEG does not have an IP Output license.

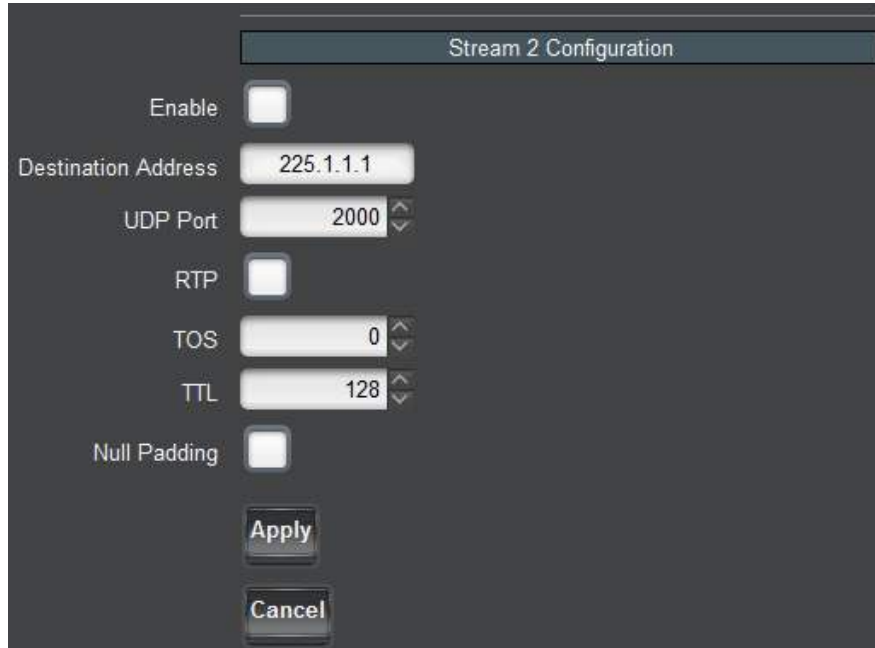
-
- **Destination Address:** Enter the desired destination IP address for the stream. Both multicast and unicast are supported.
 - **UDP Port:** Enter the desired UDP port for the stream.
 - **RTP:** If this box is checked, the RTP protocol is used. If not checked, the UDP protocol is used. Note that RTP requires that the UDP port be an even number. Checking this box will change the UDP port to the next even number if it is an odd number.
 - **NULL Pad:** If this box is checked, the stream is made CBR by padding it with NULL packets. The padding rate can be controlled by using the **Advanced Edit** button. This function is not available for Stream 1 as it is already padded from the ASI source.
 - **Input Rate:** This field reports the instantaneous measured input rate for the stream.
 - **Peak Rate:** If the stream is enabled, this field reports the peak rate observed in the stream since it was enabled.
 - **Output Rate:** This field reports the output rate of the stream. If NULL padding is disabled, it will match the input rate. If NULL padding is enabled, it will correspond to the padding rate.
 - **Advanced Edit:** When the **Edit** button is clicked, the **Advanced Edit** area opens at the bottom of the table. This allows for detailed configuration of the port, including the NULL padding parameters, IP parameters, and FEC parameters. A more detailed description of the edit area is provided below.

Source	☒ ASI Input		☐ Current IP Input								
	Program	Enable	Destination	UDP	RTP	Null	Input	Peak	Output	Advanced	
			Address	Port		Pad	Rate(b/s)	Rate(b/s)	Rate(b/s)	Edit	
Stream 1	All	☐	225.1.1.0	2000	☐	☐	36,740,877	0	0	Edit	
Stream 2	3	☐	225.1.1.1	2000	☐	☐	11,770,803	0	0	Edit	
Stream 3	4	☐	225.1.1.2	2000	☐	☐	5,279,702	0	0	Edit	
Stream 4	5	☐	225.1.1.3	2000	☐	☐	2,217,136	0	0	Edit	
Stream 5	None	☐	225.1.1.4	2000	☐	☐	0	0	0	Edit	
Stream 6	None	☐	225.1.1.5	2000	☐	☐	0	0	0	Edit	
Stream 7	None	☐	225.1.1.6	2000	☐	☐	0	0	0	Edit	
Stream 8	None	☐	225.1.1.7	2000	☐	☐	0	0	0	Edit	
Stream 9	None	☐	225.1.1.8	2000	☐	☐	0	0	0	Edit	
Stream 10	None	☐	225.1.1.9	2000	☐	☐	0	0	0	Edit	
Stream 11	None	☐	225.1.1.10	2000	☐	☐	0	0	0	Edit	
Stream 12	None	☐	225.1.1.11	2000	☐	☐	0	0	0	Edit	

When the **Edit** button is clicked for a stream, the following message appears at the top of the table:

Advanced config for Stream 2 open below										
Program	Enable	Destination	UDP	RTP	Null	Input	Peak	Output	Advanced	
		Address	Port		Pad	Rate(b/s)	Rate(b/s)	Rate(b/s)	Edit	

At the bottom of the table, the Advanced Configuration area opens:



The image shows a 'Stream 2 Configuration' dialog box with the following fields and controls:

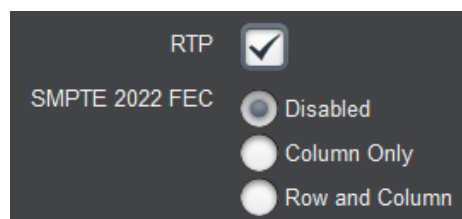
- Enable:** An unchecked checkbox.
- Destination Address:** A text field containing '225.1.1.1'.
- UDP Port:** A spin box set to '2000'.
- RTP:** An unchecked checkbox.
- TOS:** A spin box set to '0'.
- TTL:** A spin box set to '128'.
- Null Padding:** An unchecked checkbox.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

Changes made in this configuration area only take effect when the **Apply** button is clicked. If the **Cancel** button is clicked, the changes are discarded. The configuration area closes when either button is clicked.

The **Enable**, **Destination Address**, **UDP Port**, **RTP** and **NULL Padding** fields correspond to the fields in the table, described above. The following additional parameters are available:

- **TOS:** This parameter allows the configuration of the Type-Of-Service (TOS) byte in the IP header (also known as the Differentiated Services – DS – field). Valid values are between 0 and 255. Configuring this is only useful if the downstream router is configured to honor the field.
- **TTL:** This parameter allows the configuration of the Time-To-Live (TTL) byte in the IP header. Valid values are between 0 and 255. If not explicitly configured, it defaults to 128. This field controls how many hops the packet can traverse before it is dropped by a router. The default value of 128 is suitable for virtually all applications.

If the **RTP** box is checked, the following additional control becomes available:



The image shows a sub-dialog for RTP configuration with the following controls:

- RTP:** A checked checkbox.
- SMPTE 2022 FEC:** Three radio button options:
 - Disabled:** Selected (indicated by a blue dot).
 - Column Only:** Unselected.
 - Row and Column:** Unselected.

- **SMPTE 2022 FEC:** Select the FEC mode, as follows:
 - **Disabled:** No SMPTE 2022 FEC packets are transmitted.

- **Column Only:** The DEC-MPEG will send a single FEC flow, corresponding to the column protection data, using a UDP port number corresponding to the media UDP port number plus 2.
- **Row and Column:** The DEC-MPEG will send two FEC flows, the first corresponding to the column protection data, and the second corresponding to the row protection data. The row protection data will be sent using a UDP port number corresponding to the media UDP port number plus 4. Note that not all receivers support Row and Column mode; such receivers will only use the FEC Column data and discard the FEC Row data.

If either **Column Only** or **Row and Column** are selected, the following additional controls are displayed:

RTP ☒

SMPTE 222 FEC ☐ Disabled ☐ Column Only ☒ Row and Column

Columns

Rows

- **Columns:** Number of columns in the FEC matrix. This variable must be between 1 and 20 if **SMPTE 222 FEC** is set to **Column Only**, and between 4 and 20 if it is set to **Row and Column**.
- **Rows:** Number of rows in the FEC matrix. This variable must be between 4 and 20.

If the **NULL Padding** box is checked, the following additional control is displayed:

Null Padding ☒

Auto Bit Rate ☒

- **Auto Bit Rate:** If this box is checked, the DEC-MPEG will automatically determine the NULL padding rate for the stream, based on the measured peak rate. The auto rate may change over time if the stream peaks at higher rates. The current auto bit rate can be read in the **Output Rate** column of the table. If this box is unchecked, the following additional control is displayed:

Null Padding ☒

Auto Bit Rate ☒

Bit Rate

-
- **Bit Rate:** Enter the desired NULL padding bit rate, in bits/second. Note that if the stream data rate peaks over the configured value, data can be dropped, depending on the peak duration (the DEC-MPEG will buffer the data for short periods of time, but the MPEG buffer models may be compromised).

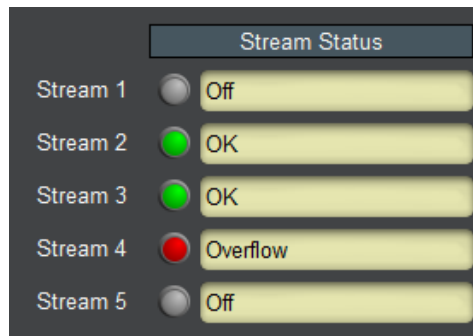
When the **Apply** button is clicked, the changes entered in the Advanced Configuration area are implemented, if the DEC-MPEG is licensed to support them:

- Enabling a stream requires an IP Output license.
- Enabling SMPTE 2022 FEC requires a FEC license.

An error message is displayed at the top of the table if either or both licenses are not available.

IP Outputs Status Tab

The IP Outputs Status tab is depicted below. It has one entry for each available stream:



The following status are reported:

- **Off:** The stream is not enabled (and is not transmitting).
- **OK:** The stream is enabled and is transmitting correctly.
- **Overflow:** The stream is set for NULL Padding with Auto Bit Rate disabled, and the configured padding rate is not high enough to support the current stream rate. Packets are being dropped. Either increase the padding rate, or set the port to Auto Bit Rate, or disable NULL padding.
- **Overrun:** The overall IP output capacity of the DEC-MPEG has been exceeded, and packets are being dropped. This will happen if too many output flows are enabled, especially if NULL padding is also enabled. Turn off unneeded streams, reduce the NULL padding rate, or disable NULL padding if possible.

Monitoring Tab

The DEC-MPEG is capable of doing basic stream monitoring, if it equipped with the optional Monitoring license (see the Admin License Keys Tab). It will monitor the stream being decoded. This function is only available for transport streams received from ASI or UDP/RTP (with or without SMPTE-2022 FEC).

The Monitoring function of the DEC-MPEG has the following features:

- Capable of displaying instantaneous bit rate for up to 32 PIDs in the incoming transport stream.
- Capable of tracking and monitoring Continuity Counter errors for up to 32 PIDs in the incoming transport streams.
- Up to 8 configurable PID alarms – the device will generate an alarm and send an SNMP trap if a given PID disappears for more than a configurable amount of time.

Monitoring Configuration Tab

The Monitoring Configuration Tab is divided into two sub-tabs:



- The **PID Monitor** sub-tab displays the PID monitoring function.
- The **PID Alarms** sub-tab configures up to 8 PID alarms.

PID Monitor Configuration Tab

If PID monitoring is disabled, the only control displayed is:



Set **Monitoring** to **Enabled** to start the PID Monitor function. Note that this operation will fail with the message **Error: No Monitoring License** if the unit is not licensed for this function. Contact Support if you would like to purchase this license.

Once PID monitoring is enabled, the unit starts reporting the PID list from the incoming transport stream that is being decoded, with the individual PID bit rates and CC (Continuity Counter) error counts.

Monitoring ☐ Disabled ☒ Enabled

PID Display ☒ Hexadecimal ☐ Decimal

PID	Bit Rate	CC Errors
0x0	15605	0
0x11	743	0
0x20	15605	0
0x100	6167161	0
0x101	50532	0
0x110	188009	0
0x111	188009	0
0x1FFF	589295	0

Reset PID Statistics

The following controls are available:

- **PID Display:** selects **Hexadecimal** or **Decimal** display for the PID values. Hexadecimal PID displays are prefixed with “0x”.
- **Reset PID Statistics:** if this button is clicked, the CC Error counts are reset to zero. Also, the list of detected PIDs is also reset, and PIDs are re-discovered from the stream.

The PID monitoring results are displayed in a table with the following columns:

- **PID:** discovered PID value. Only PIDs present in the stream are displayed. If a PID is initially present and then disappears, it will remain in the table until the **Reset PID Statistics** button is clicked.
- **Bit Rate:** current PID bit rate, in bits/second. Bit rates are averaged every 2 seconds.
- **CC Errors:** number of Continuity Counter errors detected in this PID.

PID Alarms Configuration Tab

The PID Alarms function is only available if PID Monitoring is enabled. If PID Monitoring is disabled, the PID Alarms sub-tab will only contain this message:

PID Monitor disabled

Go to the PID Monitor Configuration Tab and enable PID Monitoring to configure the alarms.

Once PID monitoring is enabled, the alarms are available:

PID	Trigger (s)	Enable	Elapsed (s)	Alarm
0x100	5	☒	0	● OK
257	10	☒	0	● OK
300	8	☒	15	● Alarm
0	10	☐	0	● Off
0	10	☐	0	● Off
0	10	☐	0	● Off
0	10	☐	0	● Off
0	10	☐	0	● Off

This table allows up to 8 alarms to be configured, as follows:

- **PID:** Enter the desired PID value to be monitored. This field accepts both decimal and hexadecimal entries. For example, the PID value 256 can be entered either as 256 or as 0x100.
- **Trigger (s):** Enter the desired timeout for the PID, in seconds. If the PID disappears for a period of time greater than what is configured in this field, the alarm is raised.
- **Enable:** Check this box to enable the alarm. If the PID is not actually present in the stream, the alarm will only be raised when the elapsed time from the enable moment exceeds the trigger.
- **Elapsed (s):** This field indicates the number of seconds since the PID in this alarm was last seen. It is only active if the alarm is enabled. In the example above, PID 0x100 is present, but PID 300 has not been seen in 15 seconds.
- **Alarm:** This field contains the alarm state for the entry, as follows:
 - ● **Off:** This alarm is disabled.
 - ● **OK:** The alarm is enabled, and the PID was last seen within the trigger period.
 - ● **Alarm:** The PID has not been seen for a period of time that exceeds the configurable trigger. The actual time is displayed in the **Elapsed** field.

Monitoring Status Tab

The Monitoring Status Tab is just a subset of the Configuration tab.



Monitoring

PID	Bit Rate	CC Errors
0x0	16317	0
0x11	741	0
0x20	15575	0
0x100	6173919	0
0x101	50435	0
0x110	189133	0
0x111	188392	0
0x1FFF	582235	0

PID Monitor

PID Alarms

PID	Trigger (s)	Enable	Elapsed (s)	Alarm
0x100	5	Enabled	0	 OK
257	10	Enabled	0	 OK
300	8	Enabled	113	 Alarm
0	10	Disabled	0	 Off
0	10	Disabled	0	 Off
0	10	Disabled	0	 Off
0	10	Disabled	0	 Off
0	10	Disabled	0	 Off

PID Monitor

PID Alarms

Admin

The Admin tab contains a number of general administrative functions, each on its own tab. The general layout is shown below:



The Admin tabs are:

- **General:** Manages a number of general card parameters; provides an SNMP MIB download.
- **Firmware:** Manages firmware images.
- **Config Files:** The DEC-MPEG has the ability to store multiple configurations, and it has a number of pre-set configurations as well. These are managed in this tab.
- **License Keys:** Contains the current licensing state of the DEC-MPEG, and allows for new license keys to be entered.
- **Event Log:** The DEC-MPEG contains a non-volatile event log. It can be inspected and downloaded from this tab.

The Admin Statistics tabs are simplified read-only versions of the corresponding Admin Configuration tabs. They will not be explicitly described here.

Admin General Tab

The Admin General Tab includes the following parameters:

- **Card Name:** This field defaults to DEC-MPEG but can be set to any descriptive name. The name provided here will also appear in the Dashboard™ Tree View.
- **SNMP Traps:** This allows SNMP traps to be enabled or disabled⁹. Note that this setting does not take effect immediately – it will become active the next time the card is rebooted.

⁹ SNMP is an optional feature in the openGear™ frame controller. The BBG-1190-DEC-MPEG SNMP functions are only available if SNMP is licensed in the frame controller.

-
- **Enable LCD Screensaver:** Default mode has box checked (enabled). When enabled, the LCD will turn off after one minute of inactivity. If the screen saver is disabled, the LCD will remain lit indefinitely.
Note: To protect the LCD from “burn-in” damage, it is recommended that the screen saver Disable mode not be used for long or indefinite periods.
 - **MIB File Download:** The DEC-MPEG provides an up-to-date copy of its MIBs. If you click on the **Save** button, a zip file with the relevant MIBs will be downloaded to your computer. This zip file contains the card MIBs, as well as the Ross Video and openGear MIBs required to compile the card MIBs.

The Admin General Tab is depicted below:



The screenshot shows a web-based configuration interface for a DEC-MPEG card. It includes the following elements:

- Card Name:** A text field containing "BBG-1190-DEC-MPEG".
- SNMP Traps:** Two radio buttons, with "Enabled" selected.
- Enable LCD ScreenSaver:** A checkbox that is checked.
- MIB File Download:** A text field containing "CARD-MIBS.ZIP" and a "Save" button.

Admin Firmware Tab

The DEC-MPEG can hold up to three distinct firmware images: a **Factory** image, and two upgrade images, called **Image 1** and **Image 2**. The Factory image can never be overwritten, and will always be available as a fall-back in case of problems or failed updates. Image 1 and Image 2 can be updated at will. Since the card offers two upgrade images, it is always possible to fall back to the previous image if there are any problems with the current one. The card will also automatically fall back to the factory image if it detects a corrupted firmware image.

The DEC-MPEG has one additional firmware image, called the **DSP Image**. The unit can hold up to 4 DSP images. DSP images will be rarely updated by Cobalt Digital Inc.. The decoder will only accept a firmware upgrade if the corresponding DSP image is already loaded in the unit; if Cobalt Digital Inc. releases a new DSP image, it must be loaded first. DSP images are automatically managed – the unit will never replace a DSP image required by any of the loaded firmware images.

DEC-MPEG firmware and DSP images are updated in the same fashion as with any standard openGear™ card. Once you obtained the upgrade image from Cobalt Digital Inc., place it anywhere in your computer and click on the **Upload** button, as shown below. A dialog box allows you to select the upgrade file. Note that you can simultaneously upgrade all of your DEC-MPEG cards over multiple chassis if you wish. For more detail, consult the **Dashboard User Manual**, chapter 6, section **Upgrading Device Software**. The Dashboard manual can be downloaded from:

<https://www.opengear.tv/frame-and-control/control-system/download/>

Note that uploading firmware to the DEC-MPEG does not affect its operation in any way and does not introduce any glitches in the inputs/outputs.



Click here to start firmware update

The fields in the Firmware Image Management tab are:

- **Factory Image, Image 1, and Image 2:** These contain version and release date information for the corresponding firmware images. If no image is present, this field will indicate **No Image**. This field also shows the required DSP image for each of the firmware images.

-
- **Upload Location:** This field contains the location where the image upload will go. The DEC-MPEG automatically chooses a location that will not overwrite the currently running image.
 - **Boot Location:** This field indicates which image will be used in the next boot. If an image is successfully uploaded through Dashboard, this automatically changes to point to that image. It can also be manually changed.
 - **Auto-Reboot After Update:** This field controls whether or not the DEC-MPEG will automatically reboot after a successful firmware upload through Dashboard. By default, the DEC-MPEG will **not** reboot after an update. You can upload the firmware at any time, and reboot later during a maintenance window.
 - **Available DSP Images:** this field has a list of loaded DSP images.

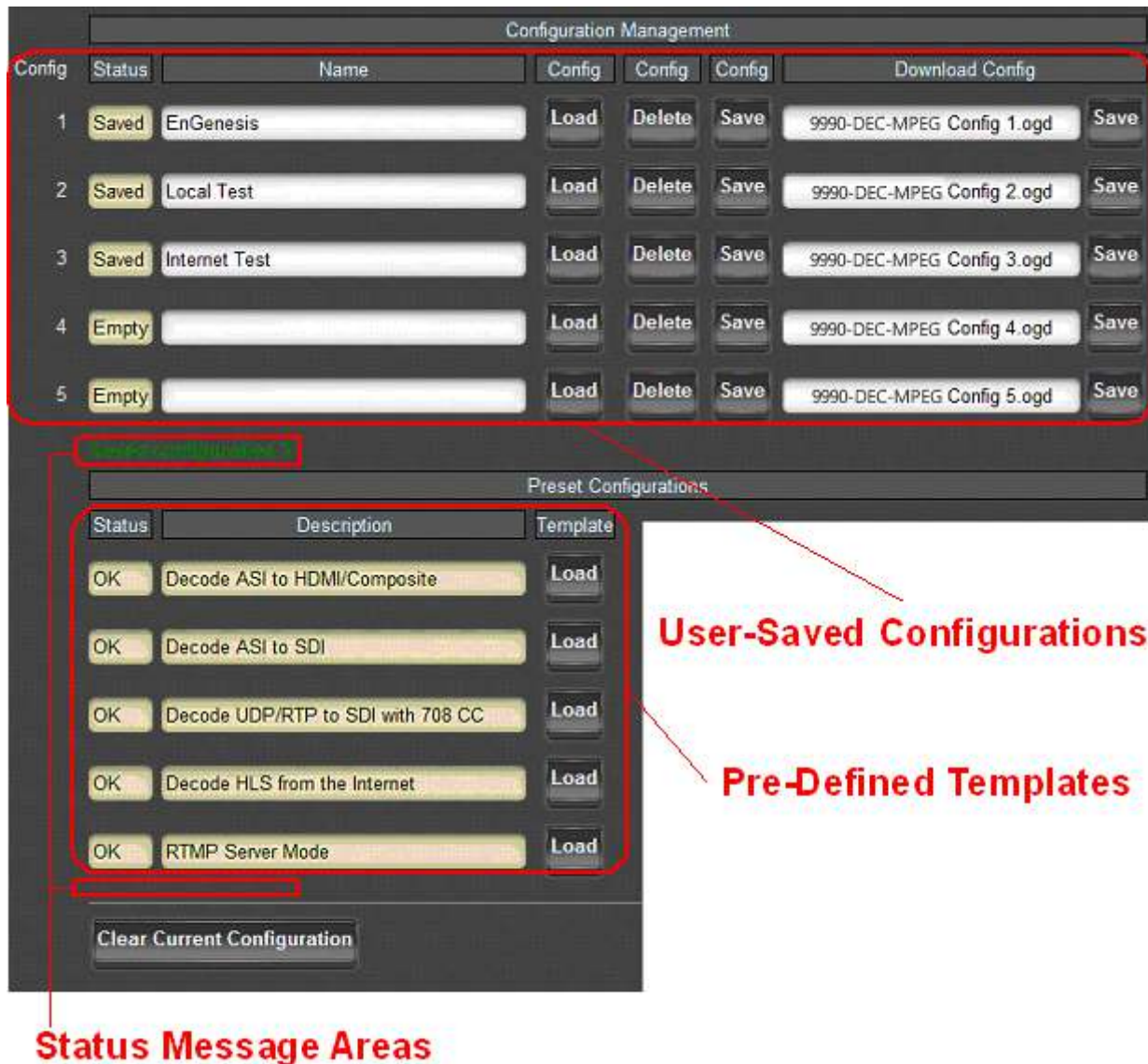
Admin Config Files Tab

As you make configuration changes to the DEC-MPEG, they are automatically persisted in non-volatile storage. If the card is rebooted or power-cycled, it will come back in the same configuration.

In addition to automatic configuration persistency, the DEC-MPEG also offers the ability to save up to 5 complete configurations, load them, and even export them. This can be used to quickly configure it for different scenarios, or for saving configuration “checkpoints” as a complex configuration is built. Since configurations can be exported, they can be archived outside the card as well.

Finally, the DEC-MPEG also offers 5 pre-saved configuration templates for some common scenarios.

The layout of the Admin Config Files tab is shown below.



User-Saved Configurations

The fields in the user-saved configuration are:

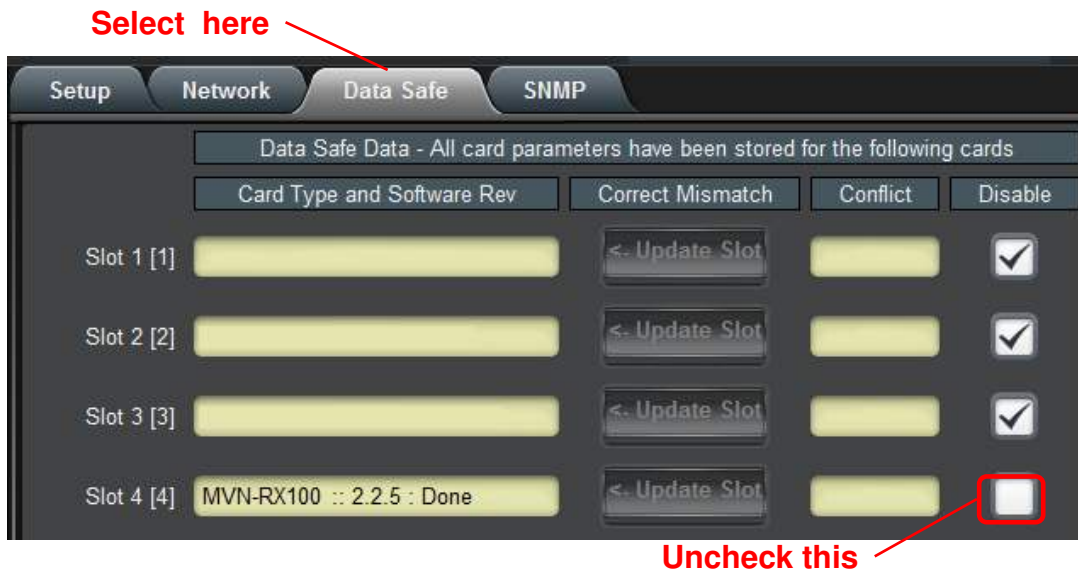
- **Status:** This indicates whether there is a saved configuration on that particular slot. It will contain the words **Saved** or **Empty**.
- **Name:** This is an optional name for the configuration. It is not required but highly advisable. The name can be edited at any time (even when there is no saved configuration).
- **Config Load Button:** If you click on this button, the corresponding configuration is loaded in the DEC-MPEG card. It will replace the currently-running configuration. Dashboard™ will take a few seconds to reload (longer if you are accessing over a wide-

area network), but the actual configuration in the DEC-MPEG is virtually instantaneous. The Status Message Area will indicate the result of the operation.

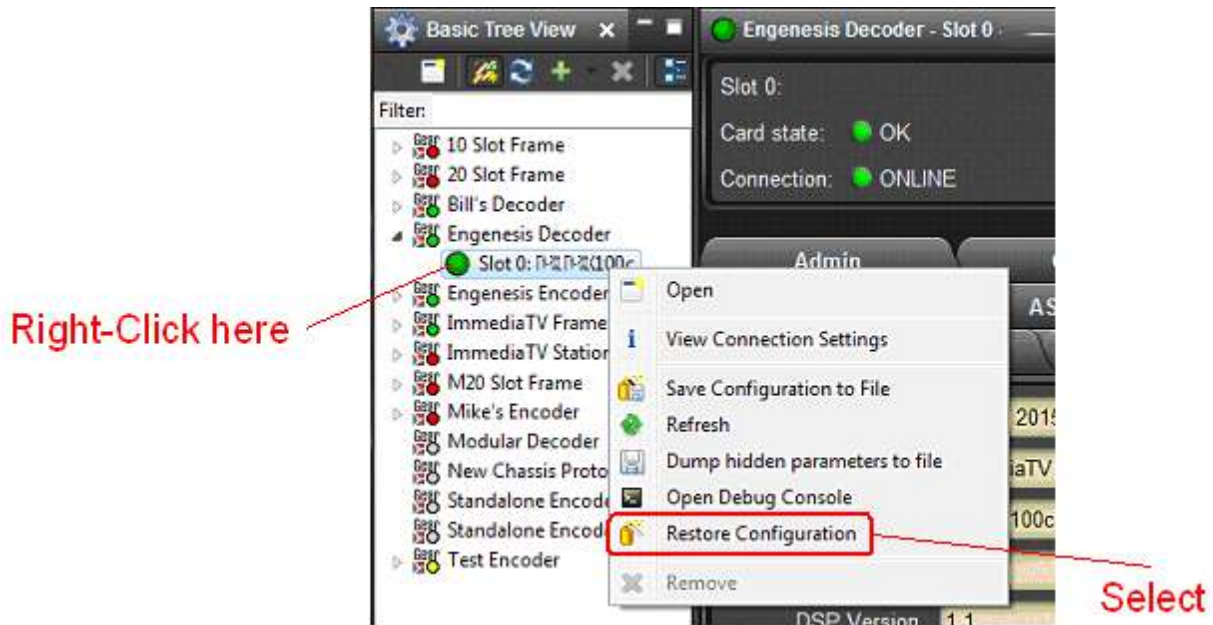
- **Config Delete Button:** If you click on this button, the corresponding configuration and its description are deleted.
- **Config Save Button:** If you click on this button, the current card configuration is saved on the corresponding slot, possibly replacing the configuration saved there if it is not empty.
- **Download Config:** If you click on the **Save** button, the corresponding file is downloaded to your computer. This feature is provided to allow configuration backups.

If you save a configuration to your computer, and later wish to restore it to the DEC-MPEG, use the following procedure:

1. For BBG-1090/1190-ENC, you can skip to step 5. Otherwise, continue to step 2.
2. On Dashboard™, open the user interface for the frame controller (slot 0).
3. Select the **Data Safe** tab in the configuration area.
4. Uncheck the **Disable** checkbox corresponding to the card you wish to restore the configuration. This step is depicted below.



5. On the Dashboard™ Tree View, right-click on the card, and select **Restore Configuration**. Follow the prompts and navigate to the file you wish to restore. This process is illustrated below



This process is discussed in further detail in the **Dashboard User Manual**, chapter 5, section **Restoring Configurations to Devices**.

Pre-defined Templates

The DEC-MPEG offers 5 pre-defined configuration templates, as indicated below.

Status	Description	Template
OK	Decode ASI to HDMI/Composite	Load
OK	Decode ASI to SDI	Load
OK	Decode UDP/RTP to SDI with 708 CC	Load
OK	Decode HLS from the Internet	Load
OK	RTMP Server Mode	Load

To load a template, just click on the **Load** button next to it. The pre-defined templates are;

- **Decode ASI to HDMI/Composite:** This template assumes a signal present in the ASI Input, decode it, and simultaneously outputs it to the HDMI and composite ports.
- **Decode ASI to SDI:** This template assumes a signal present in the ASI Input, decode it, and simultaneously outputs it to the SDI port.

-
- **Decode UDP/RTP to SDI with 708 CC:** This template assumes a multicast stream present in the Ethernet streaming port, and decodes it to the SDI output. If the input stream has closed-captions, these are passed through as SMPTE-334M captions.
 - **Decode HLS from the Internet:** This template loads a public HLS feed from the Internet and decodes it. If the decoder has access to the Internet via either the streaming port or the control port, and is configured with a DNS address, there may be actual video being displayed¹⁰.
 - **RTMP Server Mode:** This template puts the decoder in RTMP Server Mode. It will wait for a connection from an RTMP publishing client and display the stream.

Clear Current Configuration Button

The **Clear Current Configuration** button clears all the configured ports and streams as follows:

- The ASI Ports are enabled. The ASI Output is configured in automatic mode.
- The decoder is configured to decode from ASI.
- All decoder parameters are reset to their defaults.

The button does not affect the following areas:

- The settings in the **Network** tab are not changed.
- The settings in the **Admin General** tab are not changed.
- Saved configurations are not modified in any way.

Dashboard™ will take a few seconds to reload (longer if you are accessing over a wide-area network), but the actual configuration in the DEC-MPEG is virtually instantaneous. The Status Message Area will indicate the result of the operation.

Admin License Keys Tab

The DEC-MPEG has a number of optional licensable features. The Admin License Keys Tab is used to manage these features. Using this tab, you can see how many licenses you have for each optional feature, and how many you are currently using.

The DEC-MPEG has the concept of a temporary license. If you want to try out a certain feature, contact Cobalt Digital Inc.. You will receive a license key that enables that feature for a specific period of running time (license time does not “count” when the device is off).

The Admin License Keys Tab includes a License Status table, and a configuration area, as shown below. The table rows are license counts, and the columns correspond to different licensable features. The rows are:

- **Permanent Licenses:** This is the number of non-expiring licenses for each feature.
- **Temporary Licenses:** This is the number of temporary licenses for each feature. Once the license period expires, they are removed.
- **Total Licenses:** This is the total number of licenses for each feature.

¹⁰ Since the server is not operated by Cobalt Digital Inc., we cannot guarantee that video will actually play.

- **Used Licenses:** This is the number of licenses in use for each feature by the current card configuration.

If you have temporary licenses, the **Time Remaining** field indicates how long until they expire. If you do not have temporary licenses, this field has the message “No active temporary licenses”.

The table columns correspond to the licensable features, as follows:

- **IP Protocols:** This field indicates whether or not the DEC-MPEG is licensed to accept content on its Ethernet port. Without this license, the unit will only decode from ASI.
- **Dolby Decoding:** This field indicates whether the unit is licensed to decode Dolby AC3/EAC3 audio. Without this license, if the DEC-MPEG is presented with a stream with Dolby, no audio decoding will be performed.
- **Genlock:** This field indicates whether or not the unit is licensed for output genlock.
- **SMPTE 2022 FEC:** This field indicates whether the unit is licensed to decode SMPTE 2022 FEC. Without this license, the unit will still decode the RTP flow containing the bitstream, but will ignore the SMPTE 2022 FEC packets.
- **IP Output:** This field indicates whether the unit is licensed for ASI to IP Output. If it has the SMPTE 2022 FEC license, it will also be able to generate FEC on the output streams.
- **Monitoring:** This field indicates whether or not the unit is licensed for stream monitoring
- **RIST:** This field indicates whether or not the unit is licensed for RIST operation also requires the **IP Protocols** license.
- **RTMP Server:** This field indicates whether or not the RTMP Server feature is licensed.
- **Encryption:** This field indicates whether or not RIST Main Profile Encryption and Authentication feature is licensed.

Feature	License Status								
	IP Protocols	Dolby Decoding	Genlock	SMPTE 2022 FEC	IP Output	Monitoring	RIST	RTMP Server	Encryption
Permanent Licenses	1	1	1	1	1	1	1	1	1
Temporary Licenses	0	0	0	0	0	0	0	0	1
Total Licenses	1	1	1	1	1	1	1	1	1
Used Licenses	1	0	0	0	0	1	1	0	0
Time Remaining	1 week, 6 days, 23 hours								
License Key									
	<button>Apply License Key</button>								
Serial Number	ac83f00090bc								

To request a license key from Cobalt Digital Inc., you will need to provide the card serial number. It can be found in the Product Tab and in the Admin License Key Tab as well. Once you receive the key from Cobalt Digital Inc., enter it in the **License Key** field shown above, and click on the **Apply License Key** button. If the key is accepted, you will see the message *License*

Key Installed OK, as illustrated above. If there are any problems, you will see an error message in the same location. The following are the possible error messages:

- **Invalid key: missing characters:** the key you entered is too short. Double-check that you entered all the characters.
- **Invalid/Corrupted Key:** the key you entered has the correct number of characters, but it is invalid. Double check what you entered.
- **Serial number mismatch: this key is for serial xxxxxxxxxxxx:** DEC-MPEG license keys are specific to a unit. You entered a valid license key, but it is intended for a different unit, whose serial number is displayed in the message. You must use this key on the correct unit.
- **This key has already been applied:** License keys can only be applied once. This is a valid key for this unit, but you have already applied it, and its features are already available.

Admin Event Log Tab

The DEC-MPEG includes an Event Log in non-volatile storage. This event log can be used for fault-finding, and to check for error conditions. The following information is included in each DEC-MPEG event in the log:

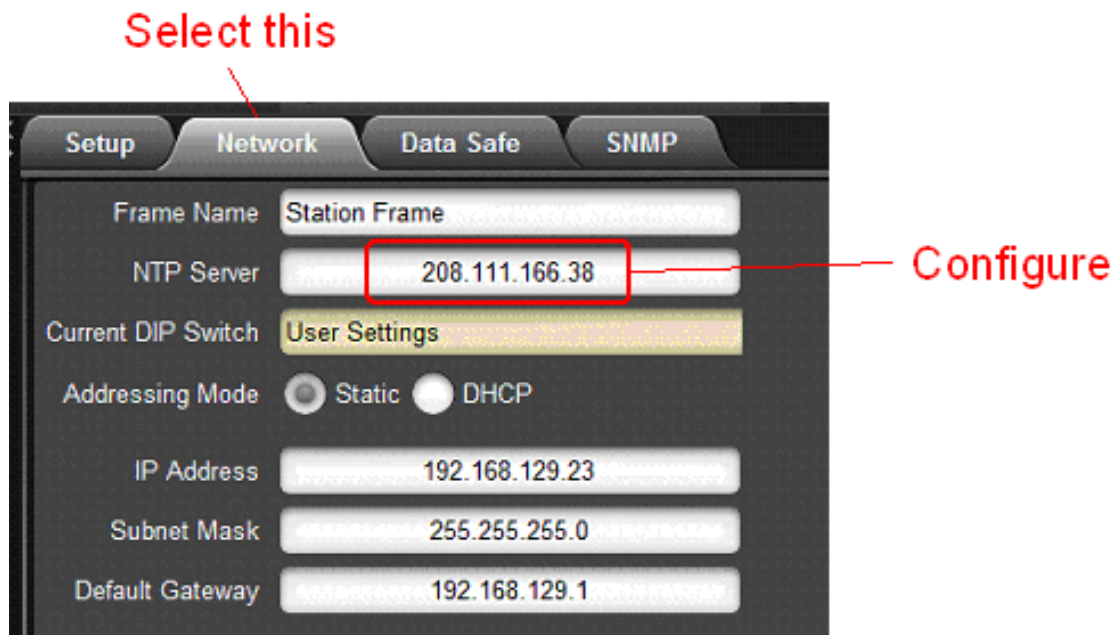
- **Date:** The calendar date in which the event occurred.
- **Time:** The time at which the event occurred.
- **Severity:** The severity of the event. The DEC-MPEG defines three severity levels:
 - **Error:** These are events that affect the operation of the device. For example, an ASI Input losing lock. An error will impact service until addressed.
 - **Warning:** These are events that may produce visible glitches, but they do not have a continuous service impact.
 - **Info:** These are informational events. All configuration actions are logged with this severity. When an error is cleared (for example, an ASI Input regains lock), the event is logged with this severity as well.
- **Subsystem:** The subsystem affected by the event. This may be a port, a stream, or the card itself.
- **Event:** This is a textual description of the event.

None of the DEC-MPEG models have a battery-backed real-time clock, so they depend on external time servers to synchronize to the current time. By default, the DEC-MPEG will initialize its internal time-of-day clock to January 1, 2010, GMT and synchronize with a time server if available.

For the BBG-1090/1190-DEC-MPEG, the NTP server IP address can be entered in the Control Tab.

The 9990-DEC-MPEG openGear card depends on the frame controller to obtain the current date and time, and the frame controller depends on an external Network Time Protocol (NTP) server to obtain current date and time.

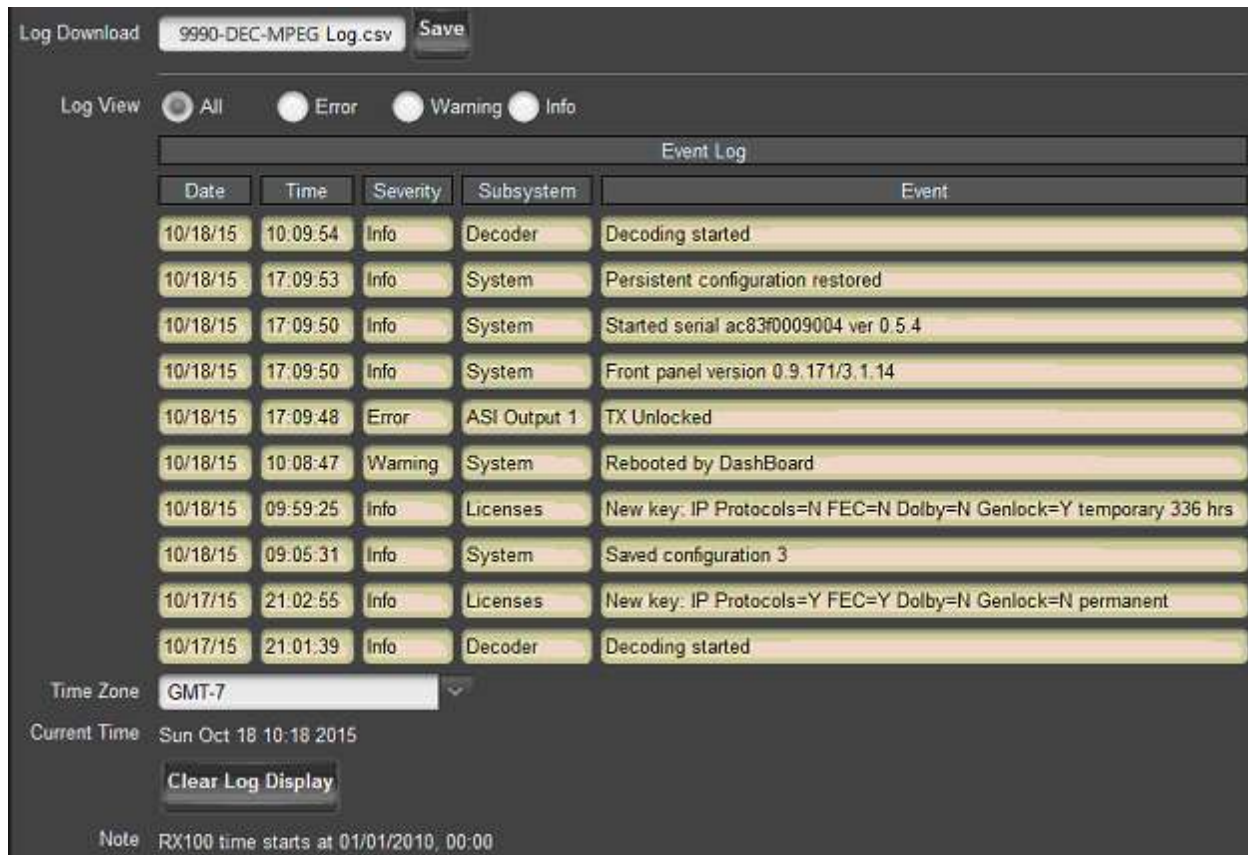
In order to configure the openGear chassis frame controller for NTP, open its configuration screen on Dashboard™, select the **Network** Tab, and enter the IP address of an available NTP server:



If your device (or frame controller in case of the 9990-DEC-MPEG) has access to the Internet, you can point it to one of the public NTP servers for your region. You can find more details on this link:

<http://psp2.ntp.org/bin/view/Servers/WebHome>

The full Admin Event Log tab is displayed below:



The fields are:

- **Log Download:** The user interface only displays the last 10 events of each type. If you would like to see the whole event log, it can be downloaded to your computer by clicking on the **Save** button. The log will be in CSV format, and it can be opened by any utility that can read text files; ideally, you should use a spreadsheet program such as Microsoft Excel or similar so it is presented in tabular format. The log will be in chronological order, oldest entry to newest.
- **Log View:** The user interface can display the last 10 events. You can choose to see the last 10 events of any kind by selecting **All**, or you can restrict the view only to **Info**, **Warning**, or **Error**.
- **Event Log:** This table presents the last 10 events of the selected type.
- **Time Zone:** To simplify the correlation of the events with your local time, you can set your time zone using this drop-down menu. Note that the DEC-MPEG presents a simplified list, with standard GMT offsets. Note that standard GMT offsets do not change back and forth with Daylight Savings; you will need to make this adjustment manually if it is relevant to you.
- **Current Time:** This field indicates the DEC-MPEG view of what the current date and time is. If your frame is not NTP-synchronized, this is useful to figure out “how long ago did this event happen”.

-
- **Clear Log Display:** If you click on this button, it clears all log views. This is useful to quickly identify any new events after the unit has been set up. Note that this action does not clear the logs stored in non-volatile memory.

The DEC-MPEG will store up to about 400 kBytes of logs in non-volatile memory. When that limit is reached, the oldest half of the stored logs will be deleted to make space for new logs.

Control Tab

The Control Tab is used to configure the management Ethernet ports in the BBG-190/1190-DEC-MPEG. This includes both the IP information, as well as the SNMP parameters. The Control Tab is only displayed for the BBG-1090/1190-DEC-MPEG.

The management port supports operation at 10, 100 and 1000 Mb/s, both half-duplex and full-duplex, with auto-negotiation and auto-crossover detection.

The Control Tab has two bottom tabs:

- **Control Port** is used to configure the IP parameters of the control port.
- **SNMP** is used to configure the SNMP parameters for the unit.

Control Port Configuration Tab

The control configuration window is depicted below:

Device Name: ENGenesis Decoder

Control Interface Configuration

IP Configuration: ☒ Static IP ☐ DHCP

IP Address: 192.168.0.97

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server: 8.8.8.8

NTP Server: 192.168.129.10

Apply

Cancel

The configuration parameters are:

- **Device Name:** This field controls the top-level name of the device in the Dashboard tree. It defaults to “Decoder”. Changes to this field take effect immediately.
- **IP Configuration:** This field selects the control port IP configuration mode, as follows:
 - **Static IP:** This option selects a static IP address, specified by the IP Address, Subnet Mask, and Default Gateway fields.

- **DHCP:** This option selects control port IP address configuration by DHCP. If this option is selected, the IP Address, Subnet Mask and Default Gateway fields are not shown.
- **IP Address:** This field is only shown if **IP Configuration** is set to **Static IP**. Enter the desired control port IP address.
- **Subnet Mask:** This field is only shown if **IP Configuration** is set to **Static IP**. Enter the desired control port subnet mask.
- **Default Gateway:** This field is only shown if **IP Configuration** is set to **Static IP**. Enter the desired control port default gateway.
- **DNS Server:** This field is only shown if **IP Configuration** is set to **Static IP**. The DEC-MPEG needs DNS for the HLS and RTMP Client protocols, if you wish to specify the server by name instead of IP address. If you do not need DNS, you can leave this field at 0.0.0.0. If your DEC-MPEG is connected to the Internet and you do not have a local DNS server, a good option is the Google public DNS at 8.8.8.8.

NTP Server: If you want the unit to be NTP-synchronized (for logging purposes), enter the IP address of an accessible NTP server in this field. If you do not need NTP, you can leave this field at 0.0.0.0

- **Apply/Cancel:** Use these buttons to apply or cancel the changes to the control port IP configuration. The IP Address, Subnet Mask and Default Gateway entries will be checked for consistency and will be rejected if invalid.

Control Port Statistics Tab

The Control Port statistics screen is depicted below. It contains the current settings for the control port. If you have configured the unit for DHCP, it will include the current IP Address, Subnet Mask, Default Gateway and DNS server obtained from the DHCP server. It also includes the link state for the control Ethernet port.

Device Name	ENGenesis Decoder
Control Interface Configuration	
IP Configuration	Static IP
IP Address	192.168.0.97
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	8.8.8.8
NTP Server	192.168.129.10
Control Link	Link OK
Control Speed	100 Mb/s Full Duplex

SNMP Configuration Tab

The DEC-MPEG includes a built-in SNMP agent with support for SNMP V1 and V2C. It will respond to SNMP transactions only on the control port, for security reasons. This tab includes the parameters for the SNMP configuration. Changes to these parameters take effect immediately.

SNMP Configuration	
Read Community	public
Write Community	private
System Contact	Contact Not Set
System Location	Location Not Set
Trap Destinations	
Trap Destination 1	0.0.0.0
Trap Destination 2	0.0.0.0
Trap Destination 3	0.0.0.0
Trap Destination 4	0.0.0.0
Trap Destination 5	0.0.0.0

The SNMP parameters are as follows:

- **Read Community:** this is the SNMP Read-Only community string.
- **Write Community:** this is the SNMP Read-Write community string.
- **System Contact:** this configures the value for the MIB-II System variable System Contact. Whatever value entered here is returned for SNMP queries to that variable.
- **System Location:** this configures the value for the MIB-II System variable System Location. Whatever value entered here is returned for SNMP queries to that variable.
- **Trap Destinations:** the DEC-MPEG supports up to 5 trap destinations. Enter the desired IP addresses here. Note that the DEC-MPEG will only generate SNMP V2C traps.

SNMP Statistics Tab

The SNMP statistics tab displays the current SNMP configuration.

SNMP Configuration	
Read Community	public
Write Community	private
System Contact	Contact Not Set
System Location	Location Not Set
Trap Destinations	
Trap Destination 1	0.0.0.0
Trap Destination 2	0.0.0.0
Trap Destination 3	0.0.0.0
Trap Destination 4	0.0.0.0
Trap Destination 5	0.0.0.0

Support Tab

If you need support with your product, you can contact Cobalt Digital Inc. by phone or e-mail:

- Phone number: +1 217 344-1243, Monday-Friday 8:00AM – 5:00PM Central Time
- E-mail: support@cobaltdigital.com

If you need to contact Technical Support, please be prepared to provide the following information:

1. A detailed description of the problem, and any actions taken to solve it.
2. A detailed description of the environment around the gateway. This includes the make and model of any connected devices being used, as well as the connection network (IP or ASI) between the gateway and any other devices.
3. The Technical Support information from the decoder itself. This is downloaded from the **Support** tab:



Select the **Support** Tab, and click on the **Save** button next to **Support Info Download**. This will create a file called **TECHSUPPORT . TXT** in the computer running DashBoard. Please e-mail this file to address shown.

The **TECHSUPPORT . TXT** file contains the following information:

- The current configuration of the unit
- A copy of the Event Log (which can also be obtained via the Admin Event Log Tab)

This file does not contain any information that would allow remote access to the unit.

RIST Main Profile Authentication

Technology Overview

RIST Main Profile security (encryption and authentication) is provided by DTLS, which is the datagram version of the TLS functionality used to secure web sites. This technology is mature and widely deployed.

DTLS authentication is based on the concept of **Key/Certificate** pairs. A **Key** must be kept secret. A **Certificate** is derived from the **Key** and is public. A certificate allows secure communication, but only with the device that holds the corresponding key.

A certificate may be signed by a third party called a **Certificate Authority (CA)**. This is a third party that is trusted; if a device is prepared to trust the Certificate Authority, that trust extends to the certificates signed by it.

The certificate-based authentication process is illustrated in Figure 1. In this figure, Device B is deciding whether or not it trusts Device A. The same process can happen independently in the other direction. Device B has decided to trust certificates signed by a certain CA, so it has a copy of its CA Certificate, which was transferred to it through some secure means. Device B then receives a certificate from Device A. Unless that certificate matches the key stored in Device A, communication cannot even start. Device B can locally check the CA signature in the certificate coming from Device A against the CA Certificate it has. If that signature matches, and if Device B is prepared to trust the CA, then it will agree to communicate with Device A.

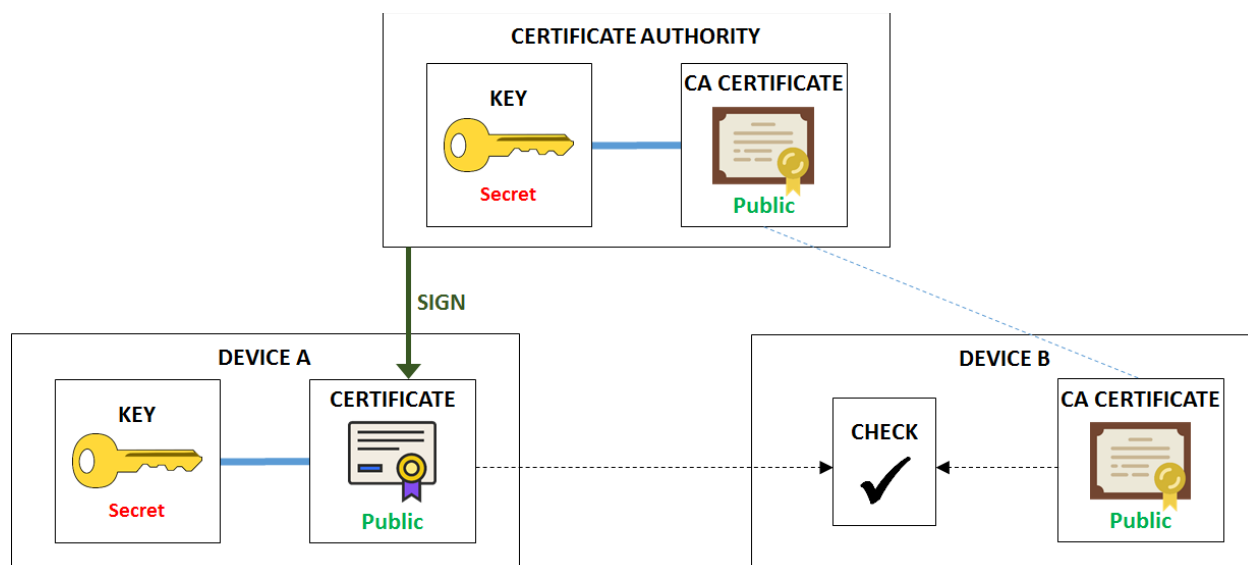


Figure 1: Certificate Checking

Security is maintained since:

- Even though the certificate from Device A is public, an unauthorized device cannot use it to establish communication because it does not have the corresponding key. Communication will not start.
- An unauthorized device may have a consistent certificate/key pair, but it will not be able to use it to start communication because the certificate is not signed by the CA trusted by Device B.

Certificate Validity and Expiration

All certificates have two dates built in:

- A starting date and time, before which the certificate is not valid.
- An ending date and time, after which the certificate is not valid.

When the certificate is generated, the user/device/process that is generating it decides on the certificate validity. There is no practical limitation on how long a certificate may be valid for. Administrators can decide on this as a tradeoff between security and convenience.

If certificate-based authentication is being used, it is important that the devices involved have a way to determine “what time is it now”. NTP synchronization is highly recommended.

Blacklists

It is possible that a device goes “rogue” – in other words, it used to be authorized, but for whatever reason, it should not be accepted anymore. In Cobalt devices, this functionality is implemented using a list of **blocked devices**. One important field in the certificate is the **Common Name** – i.e., the name of the device. In a web site, this is usually the address of the site, e.g., www.cobaltdigital.com, but it can be any text string. For Cobalt devices, the blocking is done based on the Common Name of the device. Referring back to Figure 1, Device B will execute an additional step after it verifies that the certificate from Device A is valid – it will check that the Common Name is not in a list of blocked devices. If it is, Device B will refuse to communicate, even though the certificate checks out.

Due to the nature of how certificates are generated, it is not possible to take a valid certificate and modify the Common Name (or any of the other fields encoded in it, including the validity date). Such an alteration will cause the certificate to become invalid (it is protected by a hash).

Signing a Certificate

Figure 1 shows a certificate that has been signed by a Certificate Authority. In order to be secure, the signing process must not expose the device’s secret key, not the CA’s secret key. The process uses an intermediate file called a **Certificate Signing Request**, or **CSR**. The process is illustrated in Figure 2.

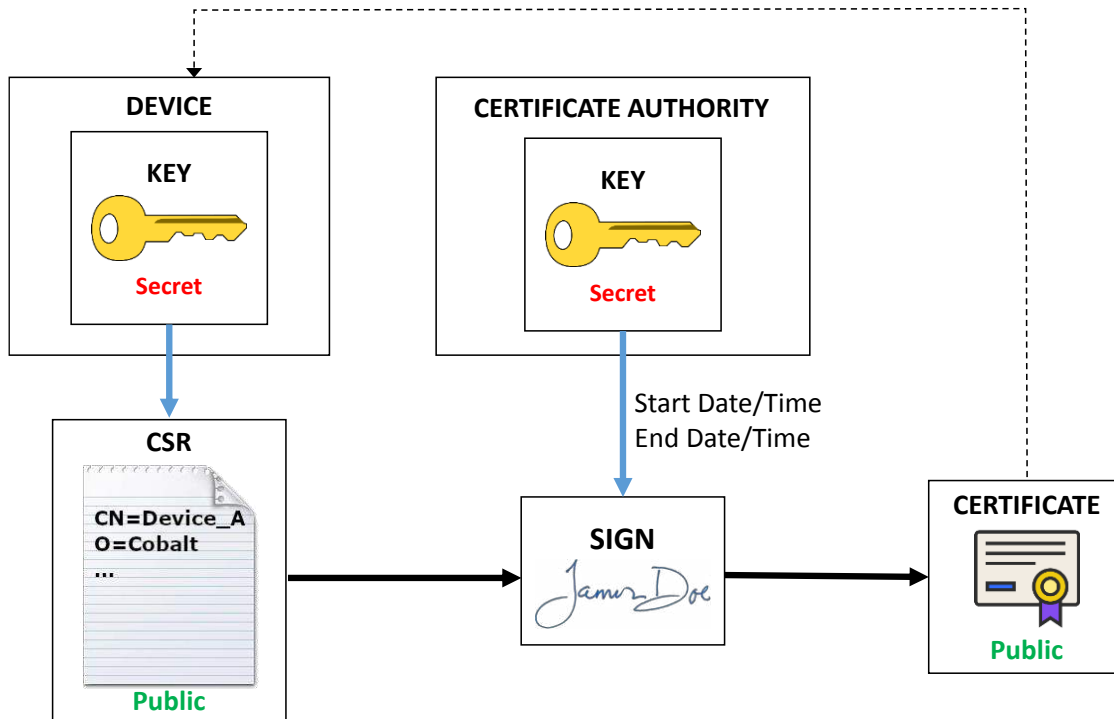


Figure 2: Certificate Signing Process

As indicated in Figure 2, the process includes the following steps:

1. A CSR is generated based on the device key (either by the device itself or by someone with access to the key). The CSR has a number of configurable items that will be transferred to the final certificate. The most important item is the Common Name, which later can be used to block access. Other fields include Organization, locality, etc. These items are not checked by Cobalt devices.
2. The CSR file (which does not need to be kept confidential) is then given to the Certificate Authority, which then “signs”, generating the desired certificate. The configurable items in the CSR are copied into the certificate. At this step, the validity dates of the certificate are also set. Normally, the start date/time is whatever the local time is at the CA, and a duration (normally expressed in days) is specified.
3. The signed certificate needs to be given back to the device, to be used when it communicates with other devices.

Cipher Suites

RIST Main Profile defines two classes of cipher suites, with different key types:

- Cipher suites that use RSA keys.
- Cipher suites that use ECDSA keys.

Cobalt devices support both types of cipher suites. Since each type has a different key, each type needs its own certificate. The whole process described in the previous sections applies to each type of key. When a RIST Main Profile device connects to another RIST Main Profile device, it will negotiate a common cipher suite that is supported on both sides. For maximum

compatibility with third-party devices, install both RSA and ECDSA keys and/or certificates in the Cobalt device. However, if you know that one type or another is not in use, you can skip the authentication files for that type.

ECDSA ciphers are considered more secure than RSA ciphers. A Cobalt device will preferably select ECDSA ciphers if supported.

RIST Main Profile Encryption and Authentication in Cobalt Devices

This section provides an overview of the encryption and authentication capabilities built into Cobalt devices. These are provided in the context of RIST Main Profile tunnels. Encryption and authentication are implemented using the DTLS protocol, which is the datagram version of the standard TLS protocol used to secure web sites in the Internet.

Encryption options

RIST Tunnels are configured in the **Network** top tab, **RIST Tunnels** bottom tab. The number of tunnels offered varies by device, and is set to the maximum number of channels that device can support. For example, since the DEC-MPEG encoder can support 4 simultaneous encoding sessions, it can support up to 4 RIST Tunnels. Encryption is invoked simply by checking the **Encryption** box. Once that box is checked, other options appear, as illustrated in Figure 3. The device will offer a list of available cipher suites. When negotiating the DTLS connection, it will accept any of the allowed ciphers. The full name of the offered cipher suites is:

- **AES128-RSA:** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- **AES128-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- **AES256-RSA:** TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- **AES256-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- **NULL:** TLS_RSA_WITH_NULL_SHA256

The **NULL** cipher provides **no encryption**, only optional authentication, and is disabled by default. It is provided for testing purposes and its use in production is strongly discouraged.

The screenshot shows the 'RIST Tunnel 1' configuration window. The 'Encryption' checkbox is checked and highlighted with a red rectangle. Other settings include: Tunnel Enable (checked), Tunnel IP (10.254.241.2), Tunnel Mask (255.255.255.252), UDP Port (5000), Tunnel Mode (Server), Interface (Ethernet 1), Reduced Overhead (unchecked), Remap UDP (unchecked), Authentication (unchecked), and Allowed Ciphers (AES128-RSA, AES128-ECDSA, AES256-RSA, AES256-ECDSA, NULL).

Figure 3: Configuring Encryption

The –RSA ciphers (and the NULL cipher) use RSA keys and certificates, and the –ECDSA ciphers use ECDSA keys and certificates.

The actual cipher to be finally used when the tunnel is established is negotiated at connection time, and is reported in the DashBoard GUI. Please note that if the tunnel endpoints are configured in such a way that there is no allowed common cipher, the tunnel will fail to connect. If the **Authentication** checkbox in Figure 3 is not checked, the device will agree to connect to any other device (regardless of whether it actively starts the connection as a client, or it waits to be contacted as a server). The communication will still be encrypted.

Authentication Options

All Cobalt devices with RIST Main Profile support include the following:

- A built-in Certificate Authority (CA), which includes a key and the corresponding certificate.
- A built-in RSA key and corresponding certificate, signed by the built-in CA.
- A built-in ECDSA key and corresponding certificate, signed by the built-in CA.

Internal certificates are generated with a 10-year duration. At boot time, the device will always check if the certificates are expired or not yet valid, and will re-generate new certificates if this is the case. However, when using authentication, it is very important to have a valid date/time in the device. All Cobalt devices support NTP synchronization.

Cobalt devices offer the following features (available independently for RSA and ECDSA modes):

- Users can upload new key/certificate pairs for the device to use.
- Users can obtain CSRs derived from the built-in device keys.
- Users can upload a CSR, have it signed by the local CA, and download the corresponding certificates.

- Users can upload new certificates matching the built-in keys.
- Users can back-up and restore the local CA key.
- Users can download the local CA and encryption certificates.

While authentication can be individually enabled/disabled in a per-tunnel basis (by using the **Authentication** checkbox shown in Figure 3), the keys and certificates are shared between all tunnels.

Authentication Security Model

Authentication involves the use of two interfaces:

- The DashBoard GUI is used to configure the authentication parameters.
- A web interface is used to move files in and out of the device.

The security model assumes that the DashBoard interface is secured – i.e., the network where DashBoard communication is happening is a secure network and no further security measures are needed.

The web interface requires a password to complete all operations that involve uploading a file to the device. The web interface can also be enabled or disabled on individual network interfaces.

If the device has a management port, the web interface is always available on this port.

All common authentication functions are available in the **Network** top tab, **Authentication** bottom tab. The relevant configuration items are shown in Figure 4.



Figure 4: Web Interface Security Control

The configuration items are as follows:

- **Web Interface Password:** some web interface actions require a password. The password is set here. If the password is lost simply set another one. The default password is **Admin** and it should be changed if this function is to be used.
- **Enable Web Config:** Cobalt devices have streaming ports (usually in the openGear card I/O panel). If a streaming port is directly connected to the Internet, it is insecure to have the authentication web interface available on it, even with the password. This control allows the user to enable or disable the web interface on specific Ethernet interfaces. The number of interfaces presented here is device-dependent.

The **Authentication** tab has Apply/Cancel buttons at the bottom. Changes become effective only after the Apply button is clicked.

If the web interface is enabled for a given network interface, the following links will be available in the web page served from that interface:

[Click here for RIST Key/Certificate Management](#)

[Click here for RIST Authentication Management](#)

Configuring the Local Credentials in the Device

As illustrated in Figure 1, the device needs a matched key/certificate pair to operate. The device's certificate is its identity, presented to remote devices when connecting. Using the DashBoard interface, in the **Authentication** tab, the device can be configured to use either its built-in credentials, or credentials that have been uploaded by the user through the web interface. This is shown in Figure 5.

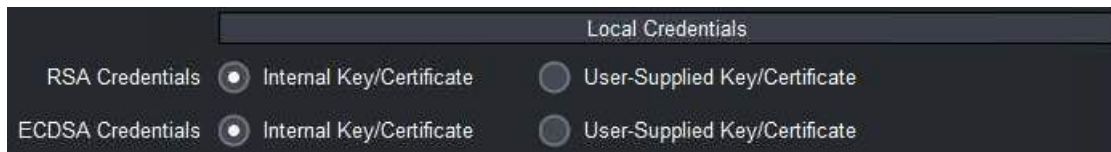


Figure 5: Configuring the Local Credentials

Note that selecting “User-Supplied Key/Certificate” prior to actually uploading a Key/Certificate will fail when the Apply button is clicked. Use the web interface to upload the files.

Uploading Keys and Certificates

In order to upload Keys and Certificates, follow the [Click here for RIST Key/Certificate Management](#) link in the web interface, as illustrated in Figure 6. For each type of encryption, you have two options:

1. Upload a matched key/certificate pair together
or
2. Upload only a certificate that is matched to the internal built-in key. In order to do this, you will need to obtain a CSR from the device itself and get it signed, as illustrated in Figure 2. This process is described in more detail below.

You do not need to provide all four files. For example, if you are only interested in ECDSA operation, you just need to provide the ECDSA Certificate (matched to the internal key) or a certificate/key pair. Certificates and keys must be in PEM format.

The **Device Password** must match the password entered in the DashBoard interface.

Click on **Upload Files** to push the selected files into the device. Note that the device will only accept the files if they are consistent, i.e.:

- Files must be in the proper format.
- If only a certificate is provided, it must match the built-in key.
- If a key and certificate are provided, they must be of the correct type (RSA or ECDSA) and must match each other.

[Click here for RIST Key/Certificate Management](#)
[Click here for RIST Authentication Management](#)

Authentication Web Interface

Web Interface Password: ****

RSA Key and Certificate

RSA Key File: No file selected.

RSA Certificate File: No file selected.

ECDSA Key and Certificate

ECDSA Key File: No file selected.

ECDSA Certificate File: No file selected.

Access Control

The device password is set using the DashBoard GUI, in the Network/Authentication Tab. Just enter the same value below.

Device Password: ●●●●

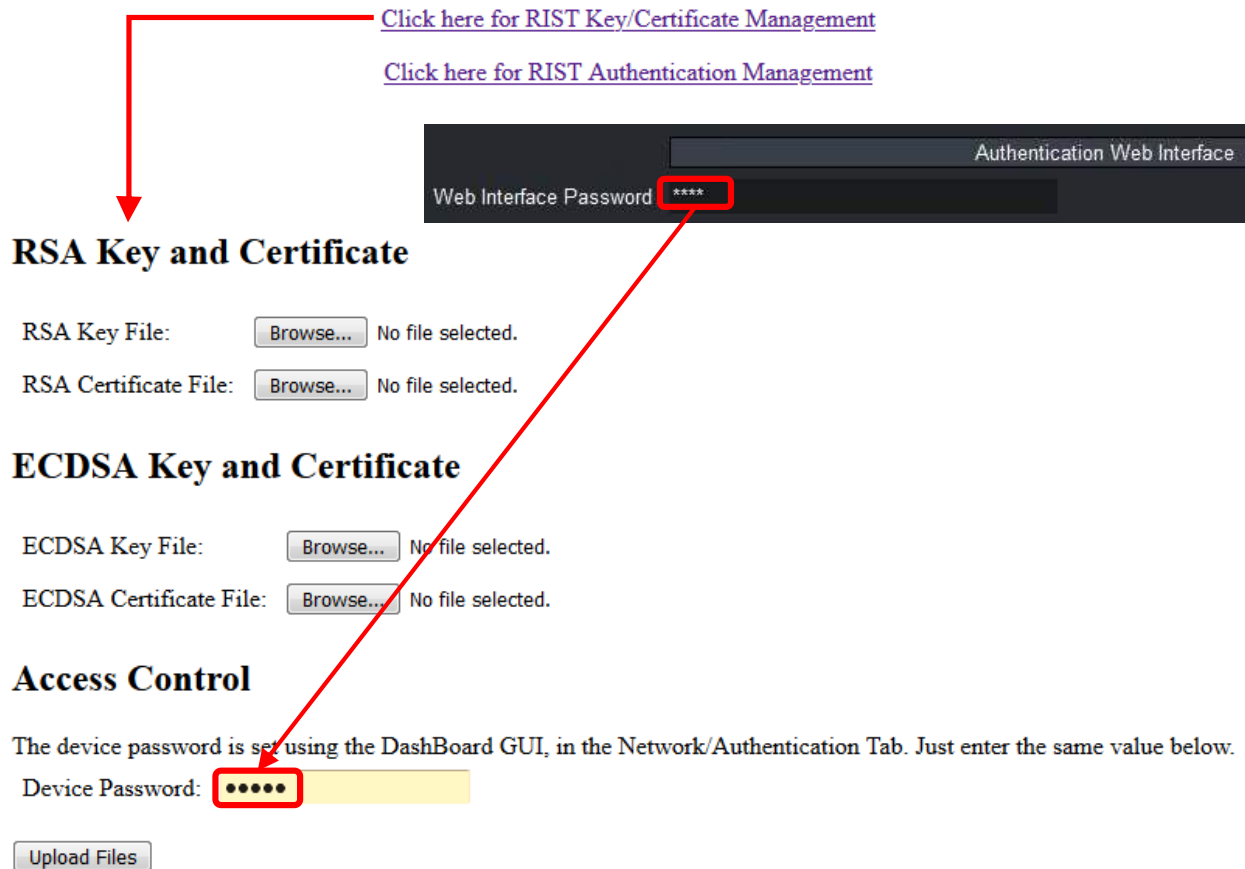


Figure 6: Uploading Keys and Certificates

Obtaining a CSR for the Built-In Keys

Figure 7 shows the process to generate a CSR for one of the built-in keys. Fill in the form and click on **Generate CSR**. A link will be provided to download the CSR, which then can be signed by an external CA, generating a certificate. The certificate will be uploaded to the device as described in the previous section.

Most fields in Figure 7 are informational and will become part of the CSR, but have no further use. The two relevant fields in this form are:

- **Key Type:** the CSR will be for either the RSA or the ECDSA key. Select which key here. If you need to generate CSRs for both keys, use this form twice.
- **Common Name:** this is what identifies the device. If later you need to block this device, the blocking will be done based on the Common Name field. It is recommended that you use unique names per device if you are generating CSRs.

No password is necessary to generate a CSR since they do not need to be kept confidential.

[Click here for RIST Key/Certificate Management](#)

[Click here for RIST Authentication Management](#)

Key/Certificate Management

Use this form to upload keys and certificates for RSA or ECDSA operation. By default, the device uses an internally-generated key and a certificate signed by its local Certificate Authority for operation. You can do the following in this form:

- Provide a certificate that matches the internal key. If you want to do that, follow [this link](#) to generate a CSR for the internal key. Use this CSR to obtain a signed certificate from your CA, and upload it here. You can leave the key field empty.
- Provide a key and certificate generated by your CA. They need to be uploaded together in the same operation.

CSR Generation

This page allows you to generate a CSR for the internal RSA or ECDSA keys. This way, you do not need to ever transmit a private key over the network. Note that separate certificates are required for RSA and ECDSA.

Key Type:	☒ RSA ☐ ECDSA
Country:	US
State:	IL
Locality:	Champaign
Organization:	Cobalt Digital
Organizational Unit:	Compression Division
Common Name:	Device
Generate CSR	

Figure 7: Generating a CSR

Authenticating Remote Devices

The previous sections described how to set the credentials for the local device, which are presented to the remote device at connection time. In other words, they are the answer to the “*who are you?*” question.

The other side of the authentication is, upon reception of the credentials, to decide if the local device is willing to communicate with the remote device. For Cobalt devices, the answer to this question is “*any device whose certificate has been signed by my trusted CA is allowed to connect, unless explicitly banned*”.

All Cobalt devices have a built-in CA, and by default will authenticate against this built-in CA. This means that if you simply enable authentication in two Cobalt devices, **they will fail to communicate** because each one is using its internal built-in CA credentials. They will need to be configured with the proper CA and credentials. There are multiple options to do so, described below.

Option 1: Use an External Certificate Authority

This is the most secure option, but it is also the most involved to set up. The steps are:

1. Create a Certificate Authority on a computer separate from the Cobalt devices, and generate a CA Certificate. An example of how to do this can be found in the section entitled “Creating a Certificate Authority with OpenSSL” later in this document.

2. Load the CA Certificate in every Cobalt device. Figure 9 shows how to do this.
3. Do one of the following:
 - a. Generate matched Key/Certificate pairs (signed by the CA) for each Cobalt device, and upload these using the process shown in Figure 6.
 - or
 - b. Generate a CSR in each Cobalt device using the process shown in Figure 7. Have the CA process the CSR to generate a certificate. Upload the certificate back into the Cobalt device using the process shown in Figure 6.
4. Configure the Cobalt device to use the user-supplied credentials, as shown in Figure 5.

The most secure is 3(3.b) above, since keys are never transmitted anywhere. However, it is the most labor-intensive. This process is illustrated in Figure 8.

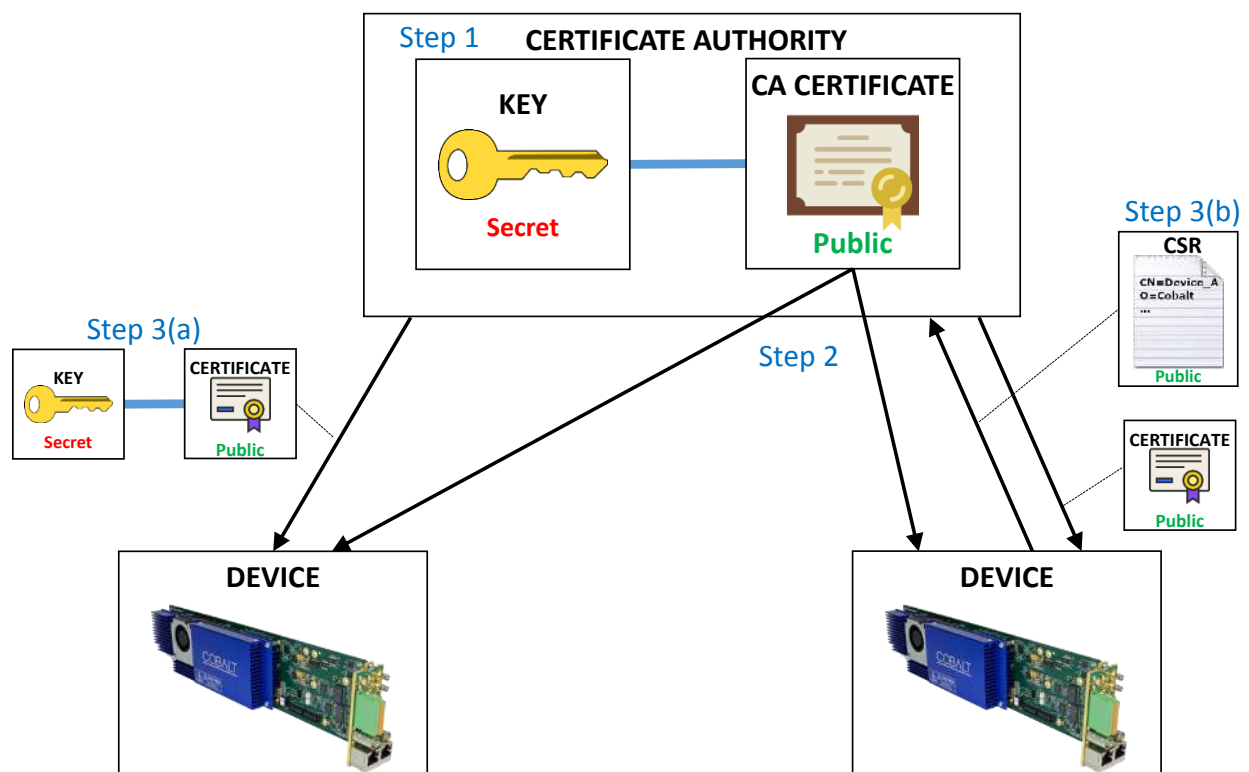


Figure 8: Using an external Certificate Authority

The process of loading an external CA certificate in the Cobalt device (Step 2) is shown in Figure 9:

- Open the device's web page and select [Click here for RIST Authentication Management](#).
- In the **Uploading an External CA Certificate**, use the **Browse** button to find the PEM file with the certificate.
- Enter the device password and click on the **Upload CA Certificate** button.

The device will check out the certificate for correctness and validity, and, if accepted, will save it. If the certificate is accepted, it can now be selected in DashBoard, as shown in Figure 9.

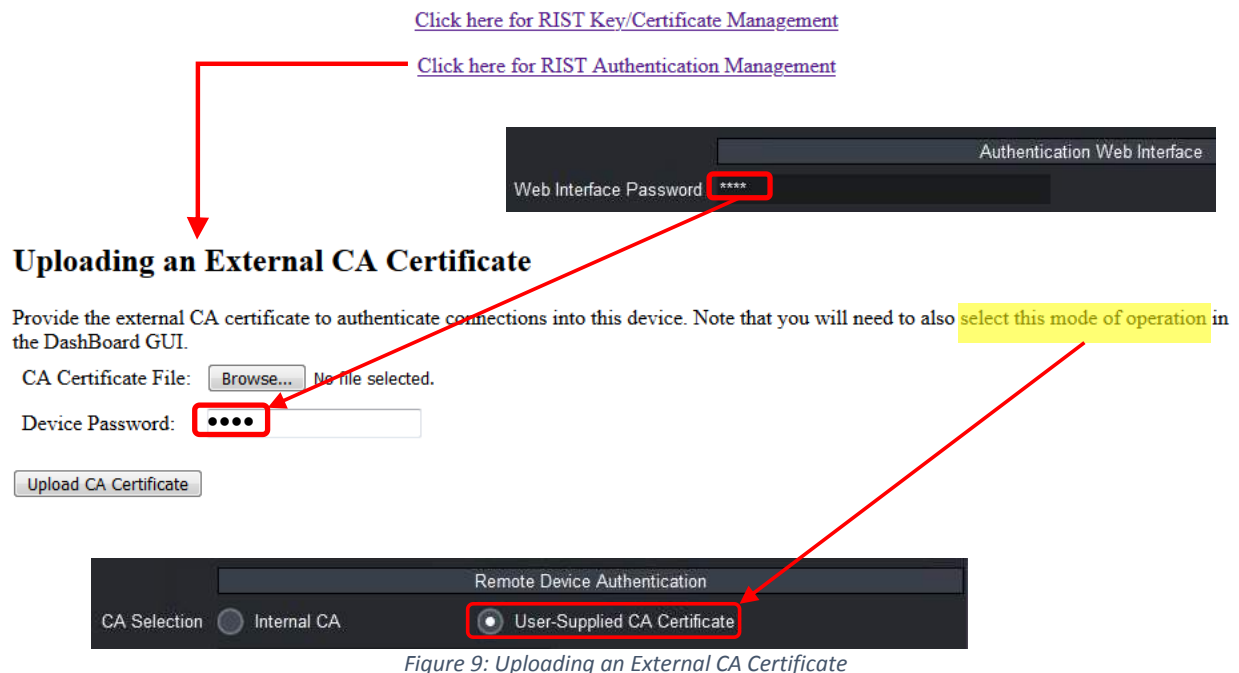


Figure 9: Uploading an External CA Certificate

Option 2: Using one of the Cobalt Devices as the Certificate Authority

This is similar to Option 1, but instead of a separate CA, one of the Cobalt devices is used as the CA. This option is less secure than Option since the CA is one of the devices participating in the network. The steps are:

1. Pick one of the Cobalt devices as the CA for your network. This device will be configured to use the internal CA and internal credentials. The CA key for this device **MUST** be downloaded and backed up.
2. Copy the CA certificate from the device chosen as the CA into all the other devices in the network. Configure all other devices to use this CA certificate.
3. Generate a CSR from each device in the network, have it signed by the CA device, and install the resulting certificate back in the device. Cobalt devices working as a CA can only sign certificates – client key generation is not supported.

Figure 10 illustrates the whole process.

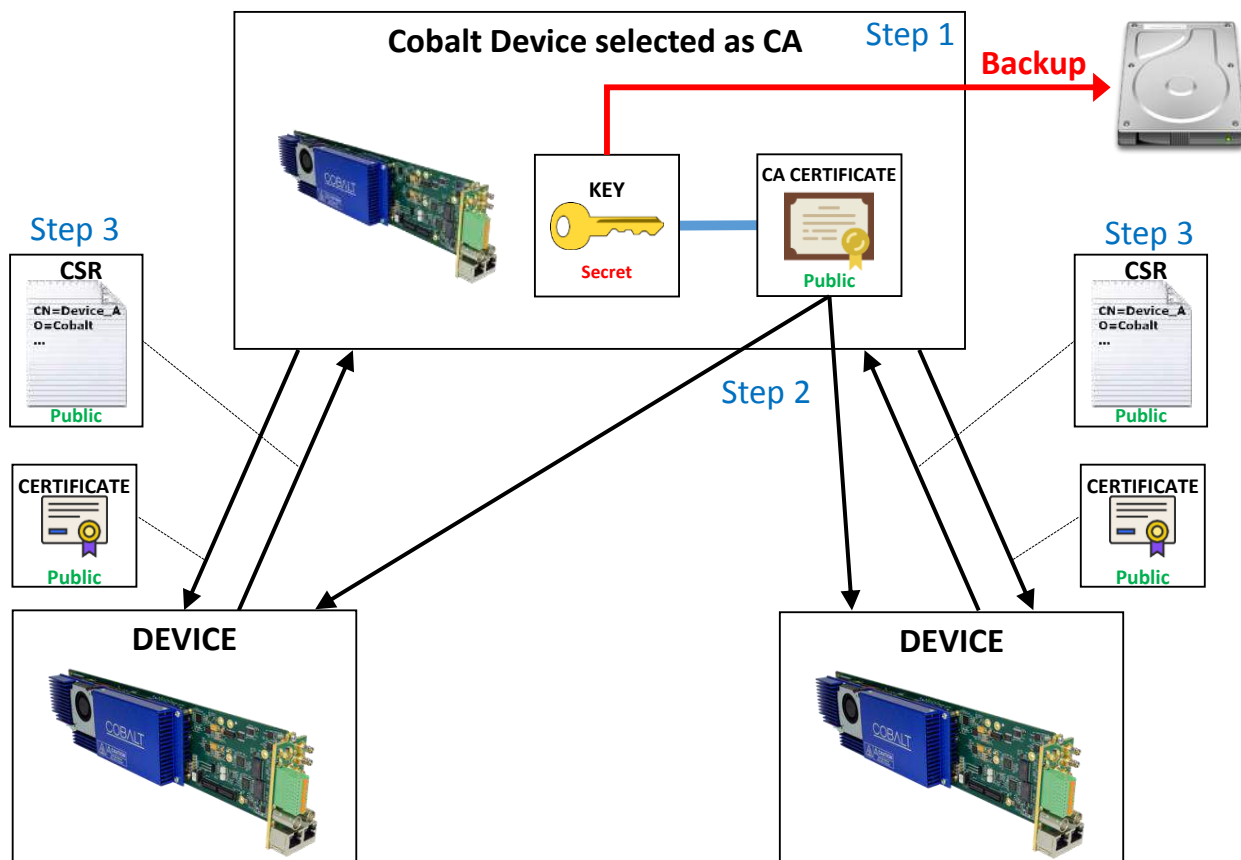


Figure 10: Using a Cobalt Device as the CA

Step 1 indicates that the CA Key for the device selected as CA must be downloaded for backup purposes. If that device is ever damaged or lost, the key can be installed on an alternate device. The CA Key can be downloaded in the DashBoard **Authentication** tab, as shown in Figure 11, by clicking on the **Save** button. Note the following:

- The default filename is **CA_KEY.BIN**, but it can be renamed as desired. Keep the extension as .BIN so as it is recognized by DashBoard.
- The file should be copied to a secure location.
- The file is encrypted and uses a proprietary format. It is not compatible with any of the usual TLS software packages. This is done as an additional level of security in case an unauthorized third-party obtains a copy of the file. However, any supported Cobalt device can use this file, so the best strategy is to keep the backup secure.

Uploading a saved key file to a Cobalt device is done through DashBoard, in a similar fashion as a firmware update. Open the device, click on the **Upload** button at the bottom of the screen, and navigate to the CA_KEY.BIN. Once the file is uploaded, the Cobalt device will automatically re-generate all the internal certificates.

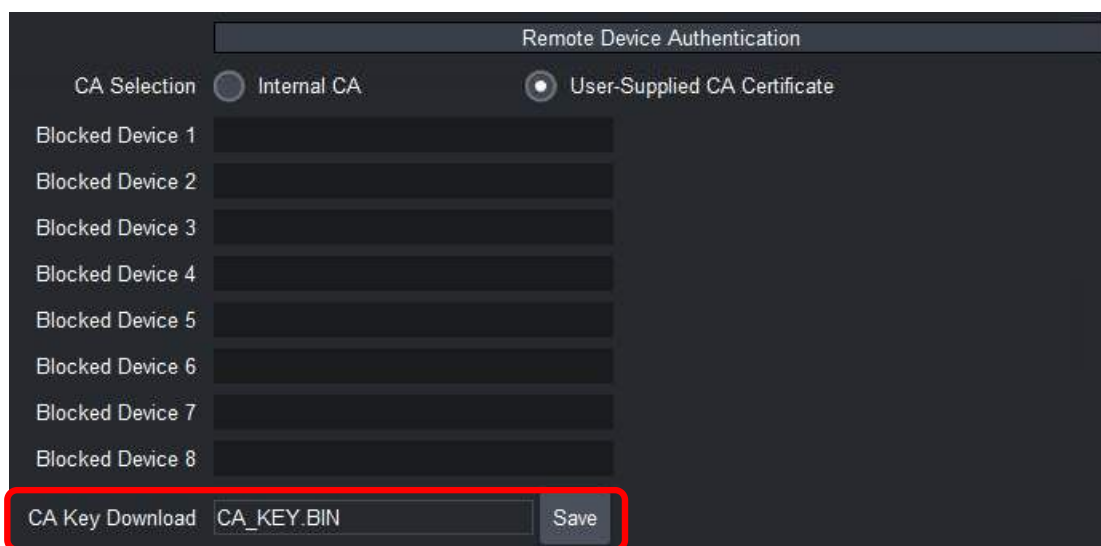


Figure 11: Downloading the device's internal CA key

The original device CA key is saved when a new key is uploaded. It can be restored at any time using the **Restore CA Key** button in the **Authentication** tab in DashBoard. This is illustrated in Figure 12.

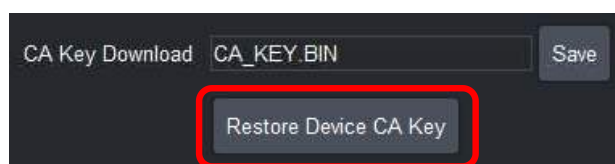


Figure 12: Restoring the original CA key

Figure 13 shows how to obtain the device's internal CA certificate for Step 2. No password is needed because the certificate does not need to be kept confidential. Use the process shown in Figure 9 to install the CA certificate in each Cobalt device.

[Click here for RIST Key/Certificate Management](#)

[Click here for RIST Authentication Management](#)



Downloading this Device's CA Certificate

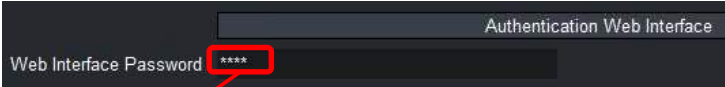
[Click here](#) to download this device's CA certificate. Upload it to all other devices that are required to authenticate connections. This file does not need to be kept confidential.

Figure 13: Downloading the internal CA Certificate

In Step 3 a CSR is generated for each device and signed by the CA device. The CSR generation for Cobalt devices is covered in the section entitled "Obtaining a CSR for the Built-In Keys". Figure 14 shows the process of signing a certificate, which is done through the web interface.

Provide the CSR file, fill in the desired certificate duration (the default is 5 years), provide the device password, and click on the **Upload CSR** button. The CSR must be in PEM format and is validated. If the CSR is valid, a certificate will be generated and a link to download it from the device will be provided. The process of uploading a certificate back to the device was described in the section entitled “Uploading Keys and Certificates”.

[Click here for RIST Key/Certificate Management](#)
[Click here for RIST Authentication Management](#)



Certificate Signing using the Local CA

Provide the CSR from the device for which you want to generate a signed certificate:

CSR File: No file selected.

Certificate validity (days):

Device Password:

Figure 14: Signing a Certificate

Option 3: Using the same CA Key in all Cobalt Devices

As with Option 2, one of the Cobalt devices is arbitrarily picked as the CA. The CA Key for this device is downloaded and installed in all the other devices, so they all become copies of the same CA. When a new CA Key is uploaded into the Cobalt device, it automatically re-generates its internal certificates to match this key. In this mode, all devices use internal credentials and internal CA, and this works because all the internal CAs are the same. This process is illustrated in Figure 15. It is still recommended that key be backed up in a secure location.

As indicated before, uploading a key to a Cobalt device is done through DashBoard. It should be noted that DashBoard can upload a file to multiple devices in parallel. This is a convenient way to distribute a key to multiple devices. DashBoard will automatically show all compatible devices to which the key can be uploaded.

This option is the least secure since a copy of the CA is in each device.

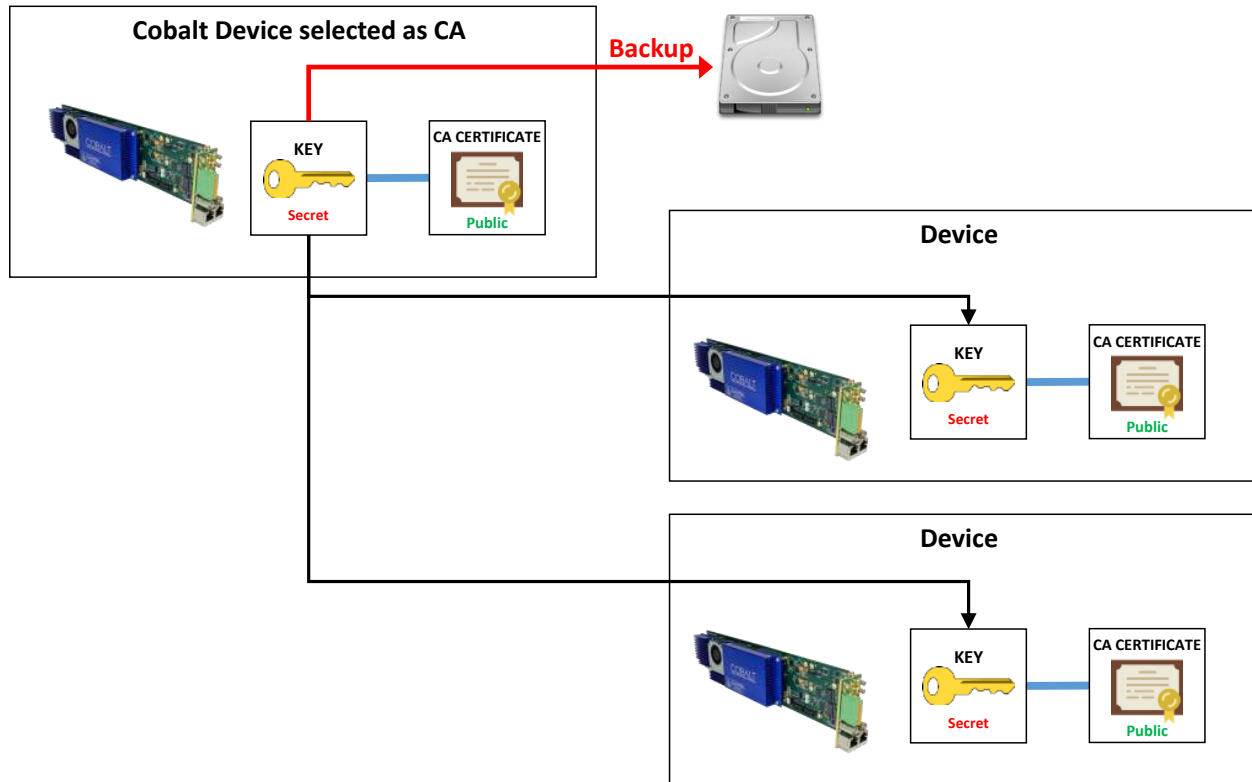


Figure 15: Copying the CA Key to all devices

Creating a Blacklist

In some situations, it may be necessary to block a device that was previously authorized to connect. The device presents valid credentials (i.e., a certificate signed by the trusted CA) but it should not be allowed to connect anymore.

This can be done in the Blocked Device list in the **Authentication** tab in DashBoard, show in Figure 16.

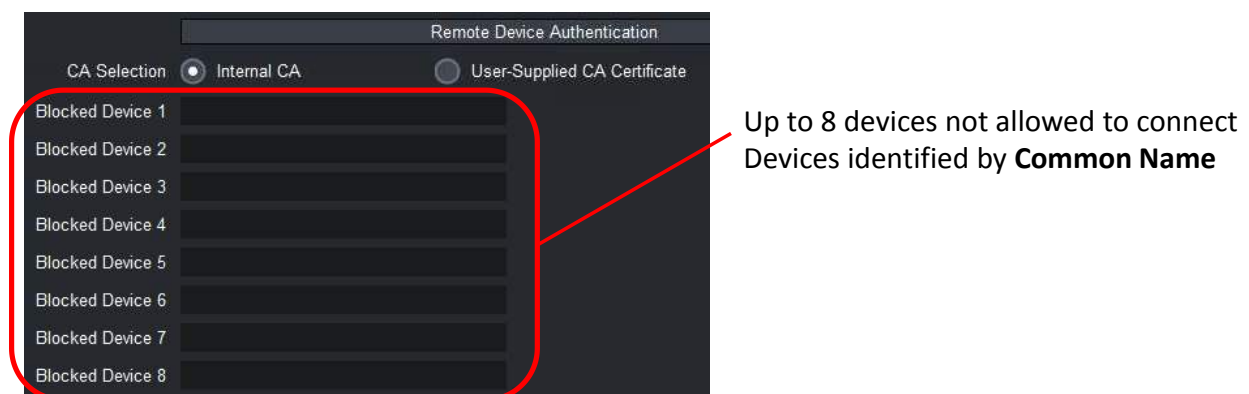


Figure 16: Blocked Device List

Devices are identified by the **Common Name (CN)** field in the certificate tied to the RSA or ECDSA keys. The Common Name is set as follows:

- If the device is using the built-in credentials, the Common Name is set to **Product_MACAddress**. For example, **DEC-MPEG_AC:83:F0:01:03:18**.
- If the device is using a certificate derived from a CSR from the device itself, the Common Name was set in the CSR, as described in the section “Obtaining a CSR for the Built-In Keys” and illustrated in Figure 7.
- If the device is using an externally-generated key/certificate pair, the Common Name is part of that certificate.

When a connection succeeds, the Common Name of the remote end is reported in the Statistics area, **Network** top tab, **Tunnel Stats** bottom tab, as indicated in Figure 17.

Product	Network	ASI Ports	Video Ports
RIST Tunnel 1 Statistics			
	TX	RX	Dropped
Full Datagram	0	0	0
Reduced Overhead	0	0	0
Keep-Alive	9467	9467	0
TX Rate (b/s)	1,354		
RX Rate (b/s)	1,354		
Remote Endpoint	10.10.9.82:51475		
Remote Name	9992-ENC_AC:83:F0:01:03:18		
Remote MAC	ac:83:f0:01:03:18		
Current Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		
RIST Tunnels	Authentication	Tunnel Stats	Remote Info

Figure 17: CN Reporting in the Statistics GUI

Creating a Certificate Authority with OpenSSL

This section shows how to create a private Certificate Authority with OpenSSL. Please note that Cobalt Digital cannot provide support for OpenSSL, these instructions are provided as-is. If you are using Linux, most distributions include OpenSSL, either by default or as an additional package. If you are using Windows, there are a number of ports available in the Internet. One such port can be found in [this link](#). Note that OpenSSL is a command-line utility that needs to run in a terminal (or a “cmd” shell in Windows).

In the sections below, commands to be typed are in **black** and responses are in **purple**.

Generating the CA Key and Certificate

The first step is to generate the CA key, which must be kept secret. In this example, the key will be written to **CA_KEY.PEM**:

```
openssl genrsa -des3 -out CA_KEY.PEM 2048
```

```

Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
...+++++
e is 65537 (0x010001)
Enter pass phrase for CA_KEY.PEM: (password is entered here)
Verifying - Enter pass phrase for CA_KEY.PEM: (password is entered here)

```

The program will ask for a passphrase (password) for the key. Enter at least 4 characters and make a note of it, because this password will be needed for signing certificates.

The next step is to generate the CA Certificate from the key. One important parameter is long the certificate validity will be. In this example, the certificate will be written to

CA_CERT.PEM, and the certificate validity will be set to 3650 days (10 years):

```
openssl req -x509 -new -nodes -key CA_KEY.PEM -sha256 -days 3650 -out CA_CERT.PEM
```

```
Enter pass phrase for CA_KEY.PEM: (password is entered here)
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

```

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Illinois
Locality Name (eg, city) []:Champaign
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cobalt Digital
Organizational Unit Name (eg, section) []:Compression
Common Name (e.g. server FQDN or YOUR name) []:CA-SERVER
Email Address []:support@cobaltdigital.com

```

You can fill the fields as you wish but do not leave the Common Name blank. The Email Address field can be left blank.

If you intend to use this as the CA for Cobalt devices, upload the **CA_CERT.PEM** file using the procedure illustrated in Figure 9.

Generating Device Keys

The following command generates an RSA key and writes it to **RSA_KEY.PEM**:

```

openssl genrsa -out RSA_KEY.PEM 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)

```

The following command generates an ECDSA key and writes it to **ECDSA_KEY.PEM**:

```
openssl ecparam -name secp521r1 -genkey -param_enc explicit -out ECDSA_KEY.PEM
```

(No output is generated in the terminal.)

Generating CSRs

In order to have certificates signed by your CA, you will need to generate a CSR for each key.

The CSR generation procedure is the same for RSA and ECDSA keys. In the example below, we are generating a CSR for the key in **RSA_KEY.PEM** and writing it to **RSA_CERT.CSR**:

```
openssl req -new -key RSA_KEY.PEM -out RSA_CERT.CSR
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Illinois
Locality Name (eg, city) []:Champaign
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cobalt Digital
Organizational Unit Name (eg, section) []:Compression
Common Name (e.g. server FQDN or YOUR name) []:Encoder-Device
Email Address []:
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The most important parameter is the **Common Name**. Select something unique for each device.
Also, leave the challenge password empty.
Repeat the same steps to generate a CSR for the ECDSA key if desired.

Generating Signed Certificates from the CSRs

The procedure here is the same regardless of where the CSRs come from. You can use CSRs from your keys generated in the previous step, or you can get CSRs from the Cobalt device as described in the section “Obtaining a CSR for the Built-In Keys”.

In the example below, we take the CSR in **RSA_CERT.CSR** and sign it with the CA Key in **CA_KEY.PEM** and the CA Certificate in **CA_CERT.PEM**, generating a certificate that is good for 3650 days (10 years), and write to **RSA_CERT.PEM**:

```
openssl x509 -req -in RSA_CERT.CSR -CA CA_CERT.PEM -CAkey CA_KEY.PEM -CAcreateserial -
out RSA_CERT.PEM -days 3650 -sha256
Signature ok
subject=C = US, ST = Illinois, L = Champaign, O = Cobalt Digital, OU = Compression, CN
= Encoder-Device
Getting CA Private Key
Enter pass phrase for CA_KEY.PEM: (password is entered here)
```

At this point, the file **RSA_CERT.CSR** is no longer necessary and can be deleted. Repeat the same step for the ECDSA CSR if desired.

You can now upload the keys and certificates to the Cobalt devices using the procedure described in section “Uploading Keys and Certificates”.