

Cobalt Digital Inc.

**9992-DEC**  
**9992-DEC-4K-HEVC**  
**Software Defined Broadcast Decoder**

**Product Manual**  
**Version 0.6.26**

**COBALT**

**9992-DEC-OM**  
**Version 0.6.26**

**openGear**

---

## 9992-DEC • Software Defined Broadcast Decoder Product Manual

- Cobalt Digital Inc. Part Number: **9992-DEC**
- Document Version: **1.0**
- Printed in the United States.
- Last Author: RMS
- Printing Date: 2021

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

---

### Copyright

**Cobalt Digital Inc. © 2021** 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.

---

# 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 within the product's power supplies and power supply area, 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

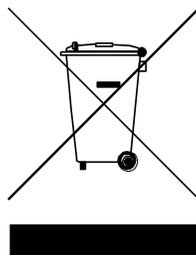
Routine maintenance to this Cobalt Digital Inc. product is not required. This product contains no user serviceable parts. If the frame does not appear to be working properly, please contact Technical Support using the numbers listed under the “Contact Us” section on the last page of this manual. All 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

Contents .....	5
Introduction.....	8
Features: .....	8
9992-DEC Base Unit Features:.....	8
9992-DEC-4K-HEVC Base Unit Features: .....	8
Optional Licenses: .....	9
Rear I/O Modules:.....	9
Product Overview .....	11
Video Decoding .....	11
Audio Decoding.....	11
Ancillary Data Support .....	11
Inputs.....	12
Outputs.....	12
Decoder Block Diagram .....	12
Indicators and Switches .....	13
Rear I/O Panel Indicators.....	13
Front Indicators.....	14
Front Switches .....	15
9992-DEC Operation and Management.....	16
Product Tab.....	18
Product Statistics Tab .....	18
Network Tab .....	20
Network Configuration Tab.....	20
Network Configuration Interfaces Tab .....	21
Network Configuration DNS Tab.....	22
Network Configuration RIST Tunnels Tab .....	23
Network Configuration Authentication Tab .....	25
Network Statistics Tab.....	28
Network Statistics Interfaces Tab .....	28
Network Statistics DNS Tab.....	29
Network Statistics RIST Tunnels Tab .....	30
Network Statistics Authentication Tab .....	32
Network Statistics Tunnel Stats Tab.....	33
Network Statistics Remote Info Tab.....	34
Video Ports Tab .....	36
Video Ports Configuration Tab.....	36
Video Ports Statistics Tab.....	36
Video Ports Statistics External Outputs Tab.....	36
Video Ports Statistics Reference Inputs Tab.....	37
Video Ports Statistics Mainboard Inputs Tab .....	37
Decoder Mode Tab .....	39
Decoder Mode Configuration Tab.....	39
Decoder Mode Statistics Tab .....	39
Decoder 1-2 Tabs.....	40
Decoder Configuration Tab .....	40

---

Decoder Config Tab.....	40
Config Tab – Decoder Input Configuration.....	40
Config Tab for UDP/RTP Protocols.....	42
Config Tab for UDP/RTP+RIST Protocols.....	43
Config Tab for ASI Inputs.....	45
Config Tab for RTMP.....	45
Config Tab for RTSP Client.....	48
Config Tab for SRT.....	50
Config Tab – Decoder Video Configuration.....	51
Config Tab – Ancillary Data Injection Configuration.....	55
Config Tab – Audio Configuration.....	56
Decoder Audio Config Tab.....	56
Decoder Audio Config Tab – Standard Stereo Service.....	57
Decoder Audio Config Tab – Standard Surround Service.....	58
Decoder Audio Config Tab – Dolby-E Mode.....	58
Decoder Audio Config Tab – Dolby Passthrough.....	59
Dolby AC-4 Configuration.....	59
Decoder Audio Routing Tab.....	60
Decoder Program Tab.....	61
Decoder Program Tab – Transport Streams.....	61
Decoder Program Tab – RTMP Mode.....	62
Decoder Audio Metadata Tab.....	62
Decoder Apply/Cancel Buttons.....	64
The Apply/Cancel Buttons.....	64
Decoder Statistics Tab.....	65
Status Tab.....	65
Audio Status Tab.....	66
Network Tab.....	67
Network Tab for UDP/RTP Stream.....	67
Network Tab for UDP/RTP+FEC Stream.....	67
Network Tab for UDP/RTP+RIST Stream.....	69
Network Tab for ASI Input.....	70
Network Tab for RTMP Client and Server.....	70
Network Tab for RTSP Client.....	71
Network Tab for SRT.....	72
Multi-Link Tab.....	73
Ancillary Data Tab.....	73
ASI Ports Tab.....	75
ASI Ports-Configuration Tab.....	75
ASI Ports - Statistics Tab.....	77
Monitor Tab.....	78
Monitoring Configuration Tab.....	78
PID Monitor Configuration Tab.....	78
Monitor Configuration- PID Alarms Tab.....	80
Monitor Statistics Tab.....	81
Monitor Statistics - PID Monitor Tab – PID Alarms.....	81

---

Admin Tab .....	82
Admin General Configuration Tab .....	82
Admin General Statistics Tab .....	83
Admin Firmware Tab.....	84
Uploading a Firmware Upgrade.....	84
Admin Config Files Tab .....	85
User-Saved Configurations .....	86
Clear Current Configuration Button .....	88
Admin License Keys Tab .....	88
Admin Event Log Tab .....	90
Support Tab.....	94
RIST Main Profile Authentication.....	95
Technology Overview.....	95
Certificate Validity and Expiration.....	96
Blacklists.....	96
Signing a Certificate .....	96
Cipher Suites.....	97
RIST Main Profile Encryption and Authentication in Cobalt Devices .....	98
Encryption options .....	98
Authentication Options .....	99
Authentication Security Model .....	99
Configuring the Local Credentials in the Device .....	100
Uploading Keys and Certificates .....	101
Obtaining a CSR for the Built-In Keys.....	102
Authenticating Remote Devices .....	103
Option 1: Use an External Certificate Authority .....	103
Option 2: Using one of the Cobalt Devices as the Certificate Authority.....	105
Option 3: Using the same CA Key in all Cobalt Devices.....	108
Creating a Blacklist.....	109
Creating a Certificate Authority with OpenSSL.....	110
Generating the CA Key and Certificate .....	110
Generating Device Keys .....	111
Generating CSRs.....	111
Generating Signed Certificates from the CSRs .....	112

---

## Introduction

This manual covers the **9992-DEC** and the **9992-DEC-4K-HEVC Software Defined Broadcast Decoders**. These are broadcast-grade decoders supporting up to two channels, designed to meet the most stringent requirements for today's broadcasters. Decoders support MPEG-2 (H.262), AVC (H.264) and HEVC (H.265), with resolution up to 4K, and a full complement of audio decoding capabilities. The 9992-DEC is an industry standard openGear® card and provide an ideal platform for transitioning to state-of-the-art decoding capabilities.

### Features:

- **Future-Proof** — Software-defined architecture supports MPEG-2 (H.262), MPEG-4 AVC (H.264) and HEVC (H.265).
- **Industry Standard Form-Factor** — The 9992-DEC is offered in the industry-standard openGear format, and is compatible with existing deployed openGear frames.
- **High Density** — Supports up to two independent 1080p60 input streams, or a single UHD 4Kp60 input stream. One openGear frame can support up to 10 cards, for a total of 20 HD or 10 UHD 4K channels.
- **Full Audio Support** — The 9992-DEC supports MPEG-1 Layer II, AAC-LC, HE-AAC, Dolby AC-3/EAC-3/AC-4, Dolby-E and LPCM (SMPTE-302M), as well as Dolby AC-3/EAC-3/AC-4 pass-thru.
- **Low Latency** — Low latency modes available.

### 9992-DEC Base Unit Features:

- Support for one decode channel up to 1080p60
- Support for MPEG-2 (H.262) and MPEG-4 AVC (H.264)
- Support for 4:2:0 8-bit/10-bit decoding
- Full ancillary data support
- Support for 2 stereo pairs (4 audio channels) in any combination of MPEG-1 Layer II, AAC-LC, and HE-AAC (v1/v2) modes
- Supports ASI and UDP, RTP, RTMP (Client), and RTSP. Other protocols available as options.
- Remote control/monitoring via Dashboard™ software
- Hot-Swappable
- Supports all popular formats: 480i, 576i, 720p, 1080i, 1080p
- Five-year warranty

### 9992-DEC-4K-HEVC Base Unit Features:

- Support for two decode channels up to 1080p60, or one 4K channel
- Support for MPEG-2 (H.262), MPEG-4 AVC (H.264), and HEVC (H.265)
- Support for 4:2:0 8-bit/10-bit decoding
- Full ancillary data support
- Support for 4 stereo pairs (8 audio channels) in any combination of MPEG-1 Layer II, AAC-LC, and HE-AAC (v1/v2) modes
- Supports ASI and UDP, RTP, RTMP (Client), and RTSP. Other protocols available as options.

- 
- Remote control/monitoring via Dashboard™ software
  - Hot-Swappable
  - Supports all popular formats: 480i, 576i, 720p, 1080i, 1080p and 4K
  - Five-year warranty

### Optional Licenses:

- **+HEVC-DEC** Enables HEVC decoding on one AVC encode engine (up to 2 licenses max per unit).
- **+AVC-DEC** Additional 1080p60 decoder channel with MPEG-2, MPEG-4 AVC, HEVC (up to one additional channel, for a total of 2 channels per unit). Includes support for two additional stereo pairs in MPEG-1 Layer II, AAC-LC, and HE-AAC (v1/v2) modes.
- **+4K-DEC** 4K support. Requires +AVC-DEC and +HEVC-DEC license on card.
- **+422** 4:2:2 decoding support per unit.
- **+DEC-2.0** Adds one Dolby Digital/Dolby Digital Plus stereo audio decoding license.
- **+DEC-5.1** Adds one Dolby Digital/Dolby Digital Plus 5.1 Surround Sound audio decoding license.
- **+DEC-D** Dolby E audio decode license.
- **+FEC-DEC** Add SMPTE-2022 support (per unit).
- **+TSMON** Monitoring license, per channel. Adds continuous monitoring of current transport stream being decoded. Provides a list of all PIDs available in the transport stream, their current individual bit rates, and keeps numerical track of any continuity counter errors. Can also be configured to watch up to 8 PIDs and issue an alarm if PID disappears for a configurable amount of time. (If SNMP is available, this alarm is also provided as a trap.)
- **+GENLOCK** Add Genlock support (license is per channel).
- **+MP1L2-AAC-DEC** Adds one MPEG-1 Layer II, AAC-LC, or HE-AAC audio decoding per pair. Three AAC licenses can be combined to allow one 5.1 surround decode.
- **+DEC-RTMP-SVR** RTMP Server license option
- **+SRT-DEC** SRT support (per unit)
- **+RIST/ARQ-DEC** Adds RIST RTP/ARQ support (per unit)
- **+RIST/ENCRP-DEC** Adds RIST encryption and authentication support (per unit). (Requires the +RIST/ARQ-DEC license to also be present on the decoder.)

### Rear I/O Modules:

- RM20-9992-DEC-B-HDBNC 20-Slot Frame Rear I/O Module (Standard-Width)
- (2) 12G/6G/3G/HD-SD-SDI Video Out
- (2) 3G/HD/SD-SDI Video Out
- (4) SDI Video Copy Out
- (2) ASI In BNCs
- (2) GigE Media Ports
- GPIO Port

(All SDI coaxial connectors HD-BNC.)

---

Note: Mates to card in odd slot.

---

## **Product Overview**

### **Video Decoding**

Decoding Standards:

- MPEG-2 (H.262)
- MPEG-4 AVC (H.264)
- HEVC (H.265)
- Support for up to two independent 1080p60 decode sessions
- Support for UHD decoding in AVC and HEVC modes (Maximum resolution 4096x2160p60)
- Support for 4:2:0 and 4:2:2 (option) color spaces in all modes
- Support for 8-bit / 10-bit decoding in all modes
- Low Latency decoding supported

### **Audio Decoding**

Decoding Standards:

- MPEG-1 Layer II
- AAC-LC
- HE-AAC (v1/v2)
- Dolby AC-3
- Dolby EAC-3
- Dolby AC-4
- Dolby E
- LPCM (SMPTE-302M)
- Dolby AC-3/EAC-3 pass-through support  
(5.1-Surround decoding available for AAC-LC, HE-AAC, Dolby AC-3 and Dolby EAC-3; subject to licensing)

Maximum number of channels supported (subject to licensing):

- MPEG-1 Layer II: 16 stereo pairs (32 audio channels)
- Dolby AC-3: 16 stereo pairs (32 audio channels)
- Dolby EAC-3: 8 stereo pairs (16 audio channels)
- AAC-LC: 8 stereo pairs (16 audio channels)
- HE-AAC (v1/v2): 8 stereo pairs (16 audio channels)
- Dolby E: 4 services, each with up to 8 channels.

Optional support for 5.1 Surround Sound encoding, in AAC and Dolby modes.

### **Ancillary Data Support**

- Closed-Captioning: SMPTE-334M (EIA-608 and EIA-708 supported), Line 21 (SD sources)
- AFD: SMPTE-2016, Line 20/22 WSS (SD sources)
- SCTE-104 to SCTE-35 conversion
- SMPTE ST 2038 generic ancillary data transport (timecode, KLV, etc.)
- SMPTE ST 2108 HDR metadata

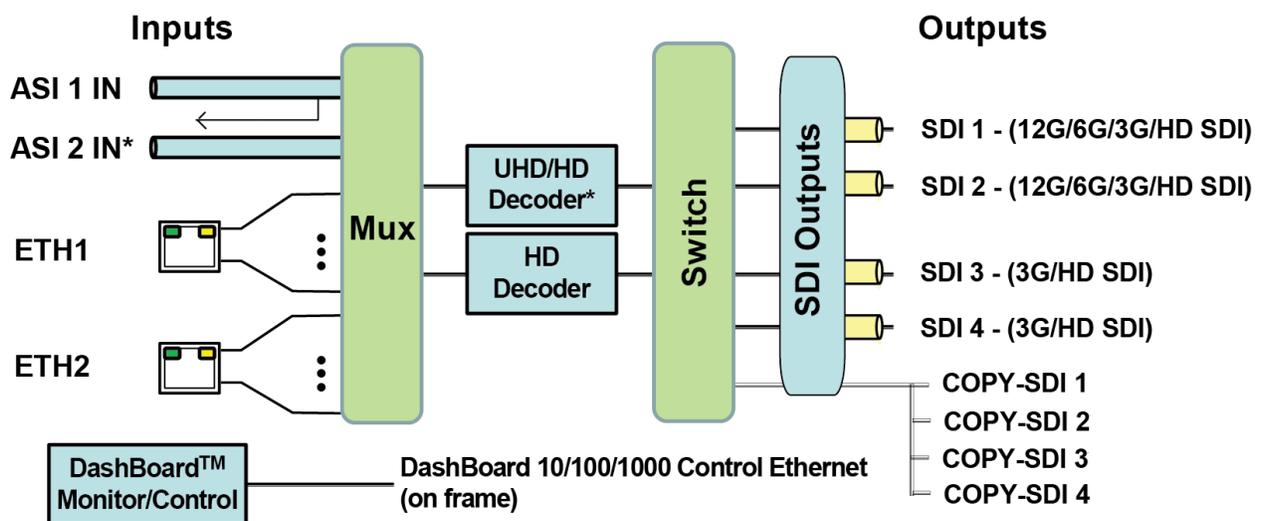
## Inputs

- (2) 75Ω DVB-ASI inputs
- (2) Gigabit Ethernet ports for IP input, supporting the following protocols:
  - UDP unicast/multicast
  - RTP unicast/multicast with optional SMPTE-2022 FEC
  - RTMP Client or Server
  - RTSP Client
  - SRT for legacy applications
  - RIST for contribution over the Internet

## Outputs

- (2) SDI outputs each supporting 12G-SDI, 3G-SDI, HD-SDI and SD-SDI
- (2) SDI outputs each supporting 3G-SDI, HD-SDI and SD-SDI
- Support for all standard frame rates (interlaced and progressive): 23.98, 24, 25, 29.97, 30, 50, 59.94, 60

## Decoder Block Diagram



\* ASI 2 IN BNC selectable as ASI 2 IN stream decode source (default mode) or as alternate which instead provides a loop-thru ASI 1 output copy.

For the remainder of this manual, the term *port* for a physical output/input port (such as ASI or Ethernet), and *stream* for a transport stream present in the port. ASI ports support only one stream. Ethernet ports support multiple streams.

---

## Indicators and Switches

The 9992-DEC card and its rear module are intended for installation only in 20-slot openGear<sup>®</sup> frames such as the 20-slot OG3/OGX frame or the Cobalt HPF-9000 frame. Prior to installing the card, first install the corresponding rear panel I/O module.

### ***Rear I/O Panel Indicators***

The 9992-DEC rear I/O panel is depicted below. It includes the following:

- (2) 12G/6G/3G/HD/SD-SDI Video Out
- (2) 3G/HD/SD-SDI Video Out
- (4) SDI Video Copy Out
- (2) ASI In BNCs
- (2) GigE Media Ports
- COMM/GPIO

(All SDI coaxial connectors HD-BNC)

**Note:** Output ports marked as “(12G)” can output 12G and lower SDI media. Output ports marked as “(3G)” are compatible only with 3G or lower SDI media.

**Note:** ASI IN 2 BNC can be DashBoard selected to function as an ASI copy of ASI IN 1.

Each of the video outputs has a green indicator LED, with the following states:

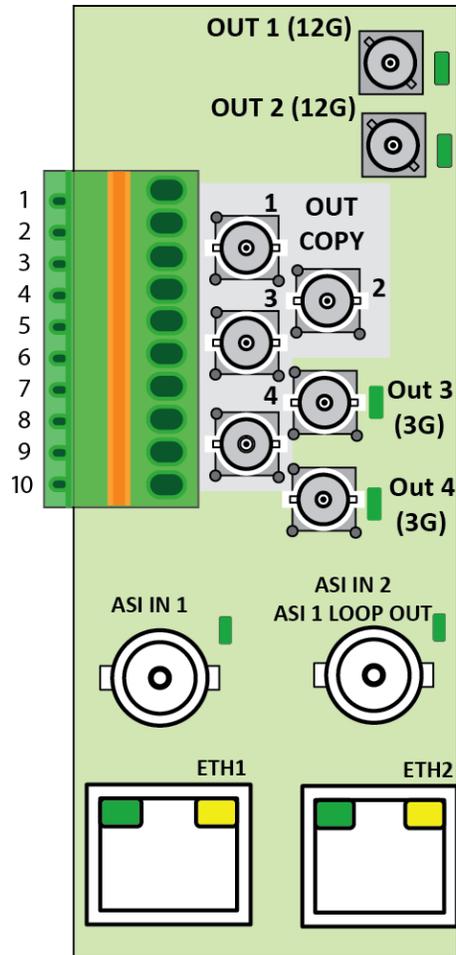
- **LED off:** no video signal present, or output not configured.
- **LED ON:** video output locked to the video signal.

Each of the ASI input ports has a green indicator LED, with the following states:

- **LED off:** No ASI signal detected at the input.
- **LED ON:** Input locked to an ASI signal.

Each of the Gigabit Ethernet ports has two indicator LEDs, with the following states:

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

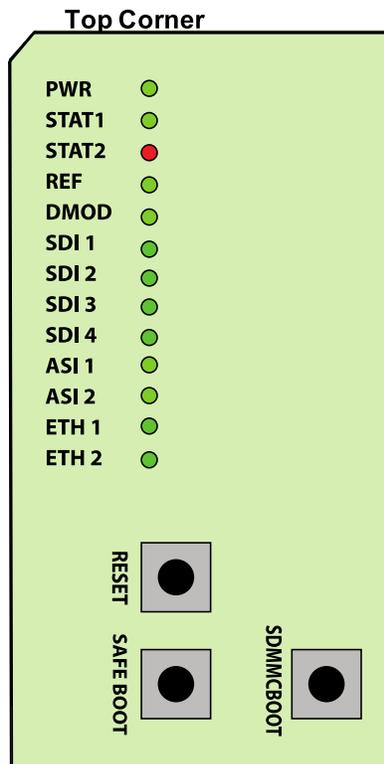


## Front Indicators

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:

- **PWR 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)
- **Status LED:** indicates the overall status of the board.
  - **STAT1:** is Green no active alarm
  - **STAT2:** is Red at least one critical alarm present
- **REF and DMOD:** are unused at this time.
- **SDI 1, SDI 2, SDI 3, and SDI 4 LEDs:** these behave the same as the corresponding rear I/O panel indicators.
- **AS1 1 and ASI 2 LEDs:** these behave the same as the corresponding rear I/O panel indicators.
- **ETH1 and ETH2 LEDs:** these indicate the status of the corresponding Ethernet connection.
  - **Off:** no link
  - **On:** link OK, port is transmitting and/or receiving packets



The 9992-DEC board has other LEDs that may or may not be illuminated. They are intended for engineering debug only.

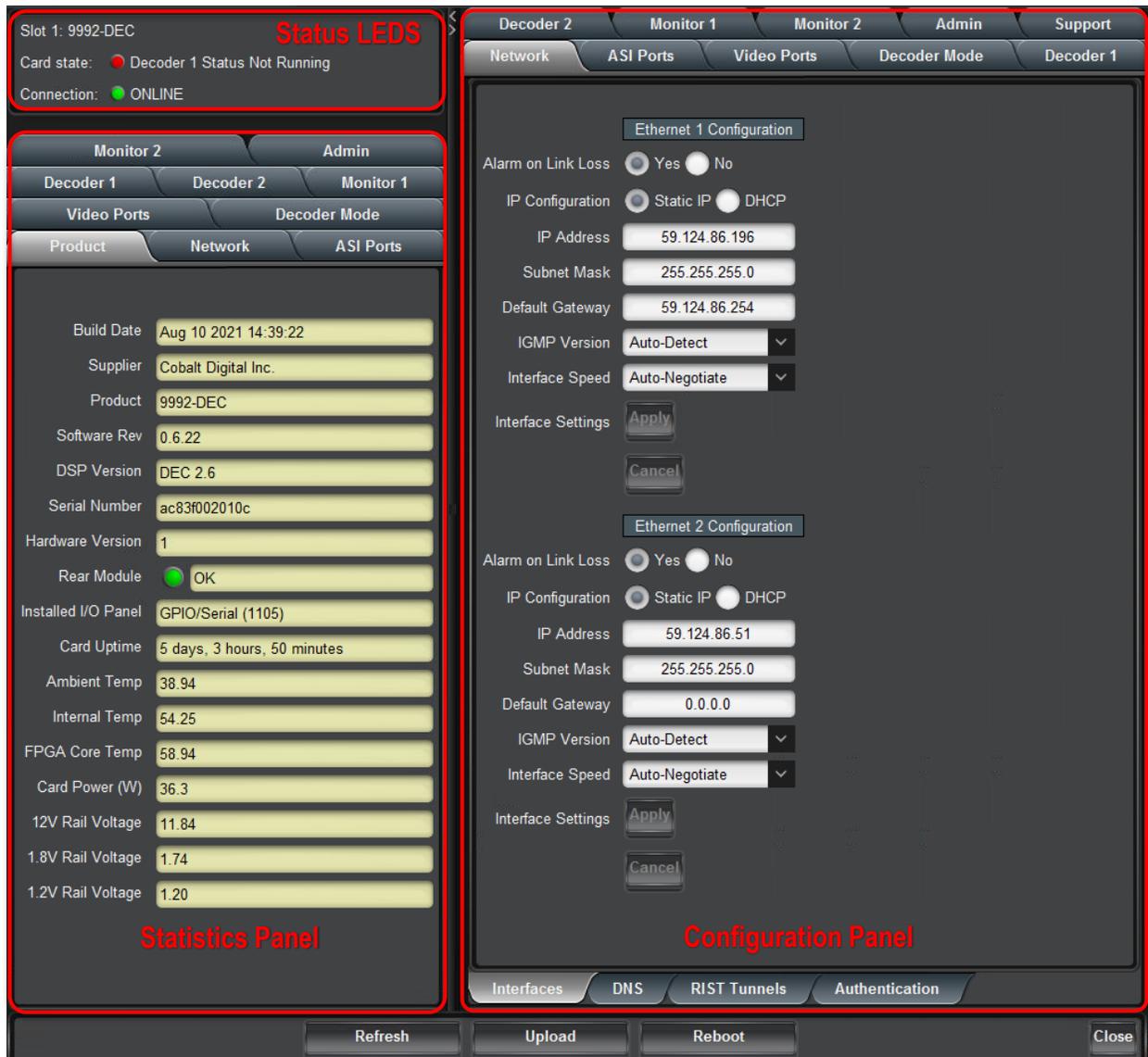
### **Front Switches**

The 9992-DEC has three pushbutton-type switches in the front, just below the LEDs, as depicted below. Their operation is as follows:

- **Reset Switch:** Pressing this pushbutton switch causes the card to reset.
- **Safe Boot:** This switch is used to recover the board in the unlikely case of a corrupted or broken firmware update. In most cases, the 9992-DEC 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 green and red Status LEDs light up simultaneously. This action causes the card to revert to the factory-default firmware and remove the persistent configuration.
- **SDMMC BOOT:** DO NOT USE. For engineering use only.

## 9992-DEC Operation and Management

The 9992-DEC is configured using the free Dashboard™ application, which is available for Windows, Apple OS X, and Linux. The graphic user interface (GUI) for the 9992-DEC is described in detail. As with any openGear™ card, 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. The **Card State** indicator in the **Status LEDs** area mirrors the **STAT1/STAT2** LEDs in the front of the card. If this indicator is green or yellow, the green **STAT1** LED will be lit; if this indicator is red, the red **STAT2** LED will be lit.



The following Statistics and Configuration panel 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 Ports:** this tab is used to configure/monitor the ASI ports.
  - **Video Ports:** this tab provides status information on the video outputs. In the configuration area, it can be used to configure some output port parameters.
  - **Decoder Mode:** this tab is used to configure some common parameters for all decoding sessions.
  - **Decoder 1-2:** these tabs are used to configure the individual settings for each decoder session. Only one tab will be shown if the decoder is in single-channel mode.
  - **Monitor 1-2:** these tabs are used to configure up to two audio services for a given decoder. The number of such tabs presented is a function of the number of configured audio services.
  - **Admin:** this tab is used for general administrative functions, such as firmware upgrades, licensing, logs, and configuration management.
  - **Support:** this tab provides customer support information. It appears only on the Configuration panel.

---

## Product Tab

The Product Tab contains basic information about the 9992-DEC and is only available in the statistics panel.

Product	Network	ASI Ports
Build Date	Aug 10 2021 14:39:22	
Supplier	Cobalt Digital Inc.	
Product	9992-DEC	
Software Rev	0.6.22	
DSP Version	DEC 2.6	
Serial Number	ac83f002010c	
Hardware Version	1	
Rear Module	<span style="color: green;">●</span> OK	
Installed I/O Panel	GPIO/Serial (1105)	
Card Uptime	5 days, 3 hours, 50 minutes	
Ambient Temp	38.94	
Internal Temp	54.25	
FPGA Core Temp	58.94	
Card Power (W)	36.3	
12V Rail Voltage	11.84	
1.8V Rail Voltage	1.74	
1.2V Rail Voltage	1.20	

### ***Product Statistics Tab***

The following information is available:

- **Build Date:** Date the firmware image was built.
- **Supplier:** Cobalt Digital Inc.
- **Product:** 9992-DEC<sup>1</sup>.
- **Software Rev:** This indicates the firmware revision currently running. The format is Major Version • Minor Version • Build Number.
- **DSP Version:** This indicates the version of the firmware loaded in the device's DSP.

---

<sup>1</sup> This field will show 9992-DEC even if the device is licensed as a 9992-DEC-4K-HEVC

- 
- **Serial Number:** This is the serial number of this particular 9992-DEC card.
  - **Hardware Version:** This indicates the version of the encoder hardware.
  - **Rear Module:** This indicates the status of the Rear I/O Module. It can have one of the following states:
    - **Green OK:** The Rear Module is the correct module for the 9992-DEC.
    - **Yellow Not Installed:** The 9992-DEC 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.
    - **Red Wrong Module:** The 9992- DEC 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 chance of damage to the 9992-DEC. It is recommended that this situation be rectified immediately. This alarm will cause the front status LED to turn red.
  - **Installed I/O Panel:** This indicates what type of I/O panel is installed.
  - **Card Uptime:** Indicates how long the card has been running since it was last rebooted.
  - **Ambient Temperature:** Indicates the temperature, in degrees Celsius, of the air intake of the card (measured at the front edge of the card).
  - **Internal Temperature:** Indicates the temperature, in degrees Celsius, at the back of the card.
  - **FPGA Core Temp:** Indicates the temperature at the FPGA processing element.
  - **Card Power (W):** Indicates the current card power consumption
  - **12V Rail Voltage:** Indicates the voltage at this rail.
  - **1.8V Rail Voltage:** Indicates the voltage at this rail.
  - **1.2V Rail Voltage:** Indicates the voltage at this rail.

The openGear™ frame is designed to operate in environments with up to 40°C ambient. There is typically a 5°C temperature raise from the external ambient to the “Ambient Temperature” measured by the 9992- DEC. If that measurement is at 45°C or higher, action must be taken to cool down the ambient temperature.

---

## Network Tab

The Network Tab allows for configuration/monitoring of the two Ethernet ports.

### **Network Configuration Tab**

The Network Configuration Tab is used to configure the network interfaces for the device.

- The **Interfaces** tab is used to set the parameters for each of the Ethernet ports.
- The **DNS** tab is used to optionally configure DNS servers.
- 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 displays the Network Configuration Tab with the following settings:

Section	Parameter	Value
Ethernet 1 Configuration	Alarm on Link Loss	Yes
	IP Configuration	Static IP
	IP Address	59.124.86.196
	Subnet Mask	255.255.255.0
	Default Gateway	59.124.86.254
	IGMP Version	Auto-Detect
	Interface Speed	Auto-Negotiate
	Interface Settings	Apply
		Cancel
	Ethernet 2 Configuration	Alarm on Link Loss
IP Configuration		Static IP
IP Address		59.124.86.51
Subnet Mask		255.255.255.0
Default Gateway		0.0.0.0
IGMP Version		Auto-Detect
Interface Speed		Auto-Negotiate
Interface Settings		Apply
		Cancel

Navigation tabs at the bottom: Interfaces, DNS, RIST Tunnels, Authentication.

---

## Network Configuration Interfaces Tab

This tab is used to configure the IP address and connection details for the two Ethernet ports:

- **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. It is recommended that the alarm for ports that are in use be turned on; only turn it off if you do not plan to connect that port to a network.
- **IP Configuration:** Select **Static** or **DHCP** method for configuration. If **Static** is selected, the following options are displayed:
  - **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.
- **IGMP Version:** The 9992-DEC implements the IGMP protocol for multicast reception. This parameter controls the version of the protocol to be used.
  - **Auto-Detect:** The 9992-DEC 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 9992-DEC Ethernet interfaces only support two modes: 100 Mb/s Full-Duplex and 1 Gb/s Full-Duplex<sup>2</sup>.
  - **Auto-Negotiate:** The Ethernet port will auto-negotiate the speed.
  - **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.

Notes:

- If the 9992-DEC streaming Ethernet interfaces are connected, to a 10 Mb/s switch, hub, or network feed, link will **not** be established and the port will not recognize the connection.
- If you select **100 Mb/s Full-Duplex** or **1 Gb/s Full-Duplex** and the corresponding streaming Ethernet interface is connected to a switch, hub or network feed that does not support the selected speed, link will **not** be established and the port will not recognize the connection.
- If the interface speed is set to **Auto-Negotiate**, the streaming Ethernet port will allow link to be established in 100 Mb/s Half-Duplex mode. However, this will be flagged as a warning.
- **Interface Settings:** If you make any changes to the IP Configuration, IP Address, Subnet Mask and/or Default Decoder 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.

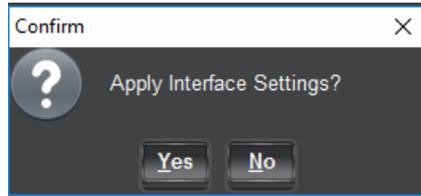
---

<sup>2</sup> Support for 10 Mb/s and Half-Duplex modes are not offered, as these are unsuitable for MPEG transport over IP applications. Moreover, any modern switch supports at least 100 Mb/s Full-Duplex.

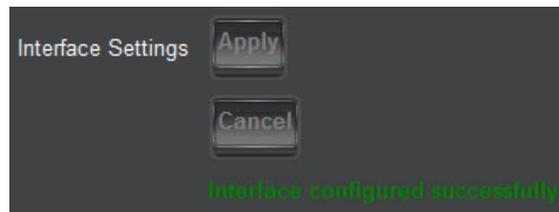
---

Note that the 9992-DEC will check the consistency of the data entered and will reject invalid combinations (i.e., combinations where the gateway is outside the interface subnet).

Once the **Apply** button is pressed, a confirm message appears, click **Yes** to apply setting or **No**.

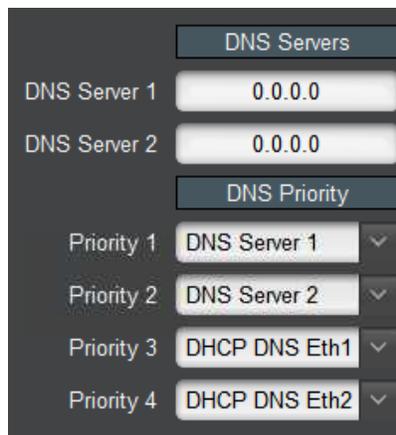


Once the setting is applied, a green success or a red error message will appear just below the **Cancel** button, as follows:



## Network Configuration DNS Tab

The DNS tab allows manual configuration of up to two DNS servers. Additional DNS servers may be acquired via DHCP, if that method is configured. The DNS servers do not need to be in the same subnetwork as the streaming ports, as long as at least one default gateway is configured. DNS is used in conjunction with the RTMP or HLS output functionality. If you are not using these functions, there is no need to configure DNS servers.



The following applies to these configuration items:

- Values entered take effect immediately.
- An unused entry should be set to 0.0.0.0.

- DNS servers will be contacted in the order defined by the **DNS Priority** list. Note that the list automatically re-sorts as changes are made.

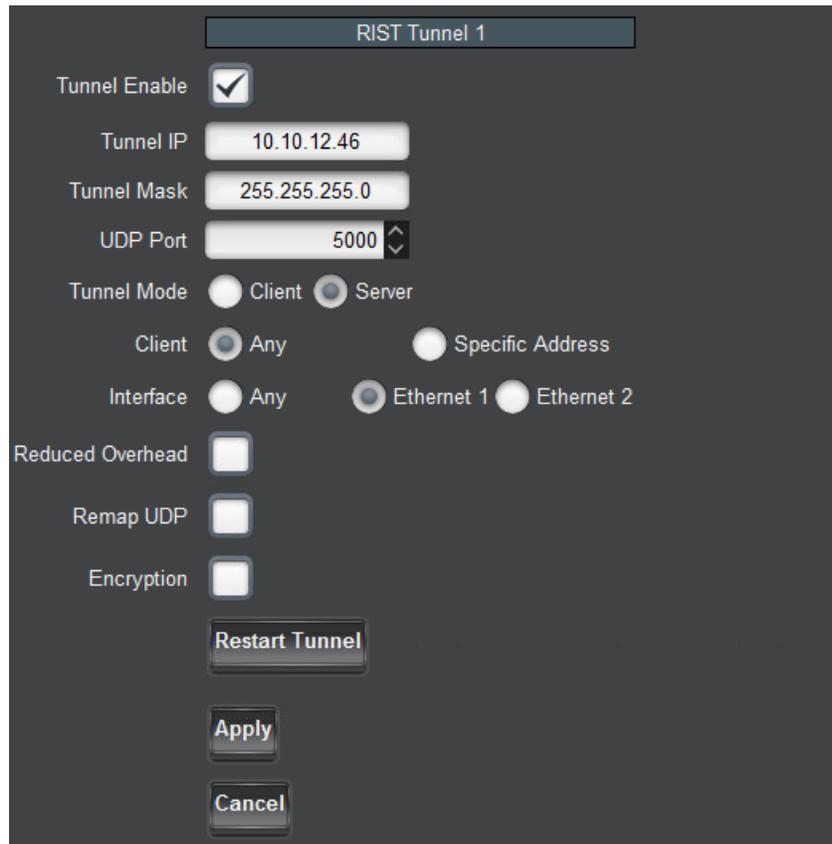
## Network Configuration RIST Tunnels Tab

This tab allows the creation and management of RIST Main Profile tunnels. The 9992-DEC supports the creation of up to two RIST Main Profile tunnels. 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:

A screenshot of the "RIST Tunnel 1" configuration window. The "Tunnel Enable" checkbox is checked. The "Tunnel IP" field contains "10.10.12.46", "Tunnel Mask" contains "255.255.255.0", and "UDP Port" is set to "5000". Under "Tunnel Mode", "Server" is selected. Under "Client", "Any" is selected. Under "Interface", "Ethernet 1" is selected. There are also unchecked checkboxes for "Reduced Overhead", "Remap UDP", and "Encryption". At the bottom are buttons for "Restart Tunnel", "Apply", and "Cancel".

- **Tunnel IP:** this is the inner IP address of the decoder 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 9992-DEC is a **Server**, it will listen on this UDP port for incoming tunnel connections.
- If the 9992-DEC is a **Client**, it will attempt to connect to this port in the server.
- **Tunnel Mode:** The 9992-DEC 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:

A screenshot of a configuration panel for Tunnel Mode. It features two radio buttons: 'Client' (selected) and 'Server'. Below them is a text input field labeled 'Server IP' containing the value '10.10.9.14'.

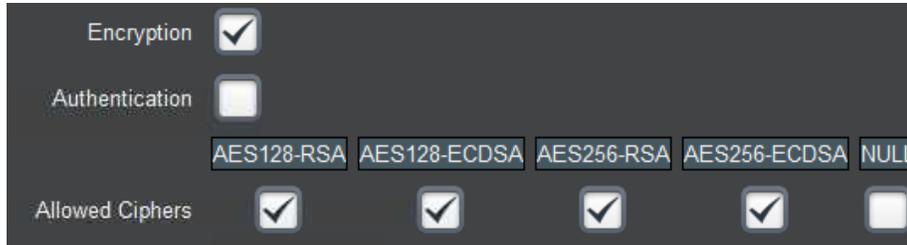
If **Server** is selected, an additional field is displayed to allow for client IP address filtering:

A screenshot of a configuration panel for Tunnel Mode. It features two radio buttons: 'Client' and 'Server' (selected). Below them are three radio buttons for client filtering: 'Client', 'Any' (selected), and 'Specific Address'.

- **Client:** This is used to configure client address filtering, as follows:
  - **Any:** The 9992-DEC will accept incoming connections from any client IP address.
  - **Specific Address:** The 9992-DEC will only accept incoming connections from one specific IP address. If this option is selected, a new field appears where the address can be configured:

A screenshot of a configuration panel for Tunnel Mode. It features two radio buttons: 'Client' and 'Server' (selected). Below them are three radio buttons for client filtering: 'Client', 'Any', and 'Specific Address' (selected). At the bottom is a text input field labeled 'Client IP' containing the value '0.0.0.0'.

- **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 9992-DEC is configured as a server, it will accept incoming connections on both 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 9992-DEC automatically detects incoming reduced overhead packets.
- **Remap UDP:** This box, if checked, causes the 9992-DEC 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-DEC** license. Once this box is checked, the following additional options become available:



- **Authentication:** If this box is not checked, the 9992-DEC 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 9992-DEC 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 9992-DEC 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 9992-DEC and the peer, the connection will fail to be established.
- The 9992-DEC 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 9992-DEC 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.

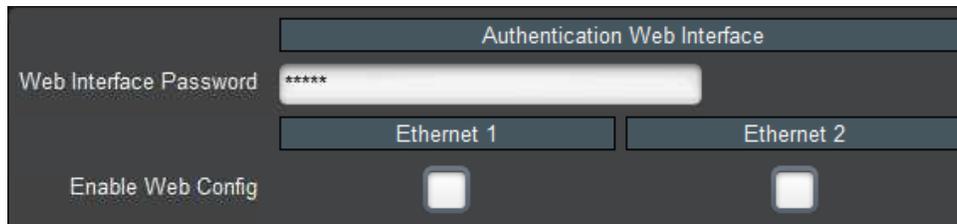
## Network Configuration Authentication Tab

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 9992-DEC. The section entitled “RIST Main Profile Authentication” later in this document provides a detailed explanation of

---

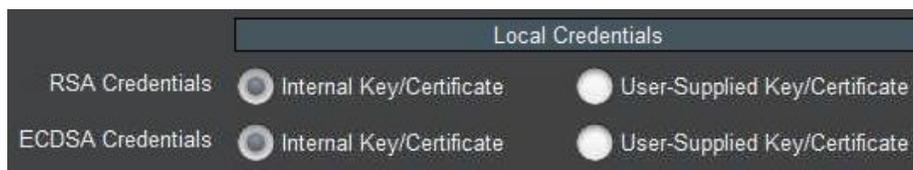
this process, and shows the relationship between the controls presented here and the web interface.

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 9992-DEC uses for itself when negotiating a connection with a peer. The 9992-DEC 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 9992-DEC 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 9992-DEC authenticates remote devices:

If authentication is enabled, the 9992-DEC will agree to communicate with any peer presenting a certificate signed by a trusted Certificate Authority (CA). The 9992-DEC 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 9992-DEC 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 9992-DEC, 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 9992-DEC 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 status of the various functions in the Network tab.

### **Network Statistics Interfaces Tab**

The following parameters are reported in the Network Statistics / Interfaces tab:

- **Alarm on Link Loss:** Reports the current setting of this parameter.
- **IP Address:** Reports the current IP Address for the port. If the port is set to DHCP and no address has been received, this will report 0.0.0.0.
- **Subnet Mask:** Reports the current Subnet Mask for the port. If the port is set to DHCP and no mask has been received, this will report 0.0.0.0.
- **Default Gateway:** Reports the current Default Gateway for the port.
- **Interface Speed:** Reports the current setting for this parameter.
- **Port 1/2 Link:** This indicator has the following states:
  - **Link OK:** The port has established link with the switch.
  - **Half-Duplex Link:** The port is set to **Auto-Negotiate**, and it has achieved 100 Mb/s Half-Duplex link with the network connection. We do not consider Half-Duplex links suitable for video communication. The port will operate, but we recommend that this be addressed. If Alarm on Link Loss is set to Yes, the Dashboard™ Card State will be yellow if there are no higher-priority alarms present.
  - **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.
- **Port 1/2 Status:** This indicator is the port overrun status. It has the following states:
  - **OK:** The port is operating normally.
  - **TX Overflow:** The 9992-DEC does not currently produce this error.

- **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 1 Configuration	
Alarm on Link Loss	Yes
IP Address	10.10.9.82
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Interface Speed	Auto-Negotiate
Port 1 Link	<span style="color: green;">●</span> Link OK
Port 1 Status	<span style="color: green;">●</span> OK
Link Speed (Mb/s)	1000
MAC Address	ac:83:f0:01:03:1a
Ethernet 2 Configuration	
Alarm on Link Loss	Yes
IP Address	10.10.9.248
Subnet Mask	255.255.255.0
Default Gateway	10.10.9.1
Interface Speed	Auto-Negotiate
Port 2 Link	<span style="color: green;">●</span> Link OK
Port 2 Status	<span style="color: green;">●</span> OK
Link Speed (Mb/s)	1000
MAC Address	ac:83:f0:01:03:1b

### Network Statistics DNS Tab

The Network Statistics DNS Tab reports the current DNS configuration, including the priority order.

---

DNS Servers	
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4
DNS Priority	
Priority 1	DNS Server 1
Priority 2	DNS Server 2
Priority 3	DHCP DNS Eth1
Priority 4	DHCP DNS Eth2
DHCP DNS Eth2	192.168.129.1

If any of the ports are set for DHCP, the DNS received from the DHCP server (if any) is displayed here. In the figure above, Ethernet 2 is set for DHCP and has received a DNS address through that process.

### **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	10.10.12.46
Tunnel Mask	255.255.255.0
UDP Port	5000
Tunnel Mode	Server
Client	Specific Address
Client IP	0.0.0.0
Interface	Ethernet 1
Reduced Overhead	No
Remap UDP	Yes
Encryption	Yes
Authentication	Yes
	<input type="button" value="AES128-RSA"/> <input type="button" value="AES128-ECDSA"/> <input type="button" value="AES256-RSA"/> <input type="button" value="AES256-ECDSA"/> <input type="button" value="NULL"/>
Allowed Ciphers	<input type="button" value="Yes"/> <input type="button" value="Yes"/> <input type="button" value="Yes"/> <input type="button" value="Yes"/> <input type="button" value="No"/>
RIST Tunnel 2	
Tunnel Enable	No

---

## Network Statistics Authentication Tab

This tab shows the current authentication configuration.

	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 9992-DEC is transmitting in the tunnel, in bits/second.
- **RX Rate (b/s):** This field shows the rate at which the 9992-DEC 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 9992-DEC 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 9992-DEC to take. This feature is not supported by the 9992-DEC. 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 9992-DEC will report “9992-DEC”.
  - **Version:** This indicates the software version currently running in the peer. The 9992-DEC will report the value found in the **Software Rev** field found in the Product Statistics Tab.

---

## Video Ports Tab

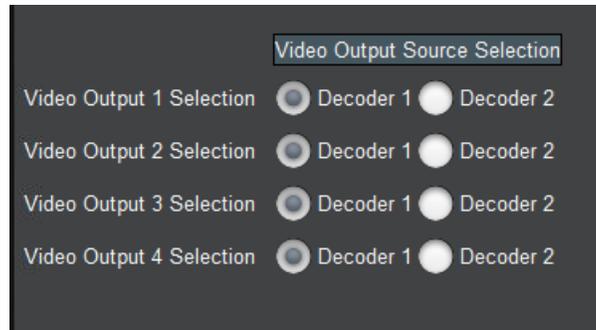
The Video Ports Tab is used to select the decoder video outputs.

### ***Video Ports Configuration Tab***

The 9992-DEC has the option to select which decoder:

- **Video Output 1-4 Selection:** Select which decoder is the source for each video output.

The Video Port configuration tab is shown below:



Note that if the 9992-DEC is in Single-Decode mode, this control will be grayed out and all the outputs will be attached to Decoder 1.

### ***Video Ports Statistics Tab***

The Video Ports Statistics tab has three lower-level tabs, namely **External Outputs**, **Reference Inputs** and **Mainboard Inputs**.

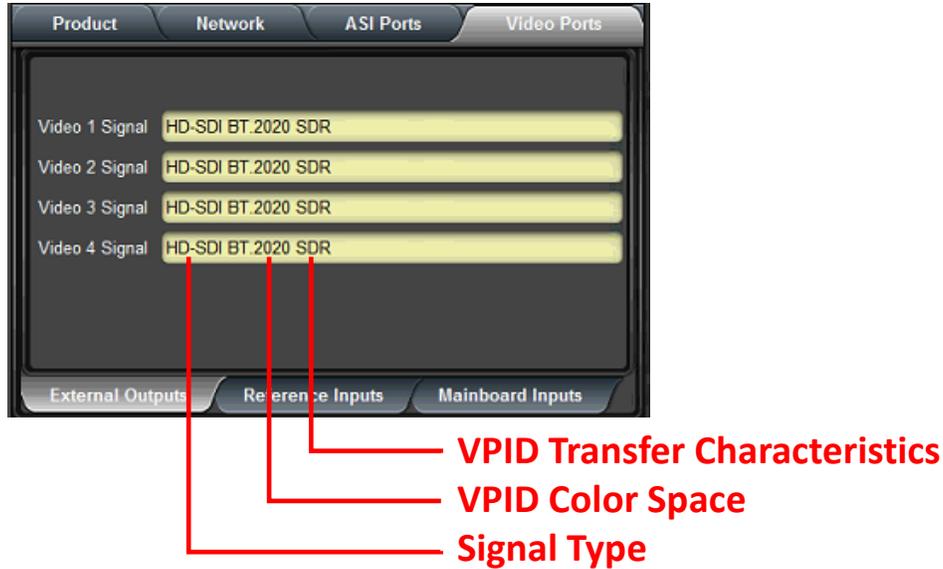
#### **Video Ports Statistics External Outputs Tab**

The External Outputs tab shows the signal of the actual decoder video outputs, as shown below.

For each video output, the following information is indicated:

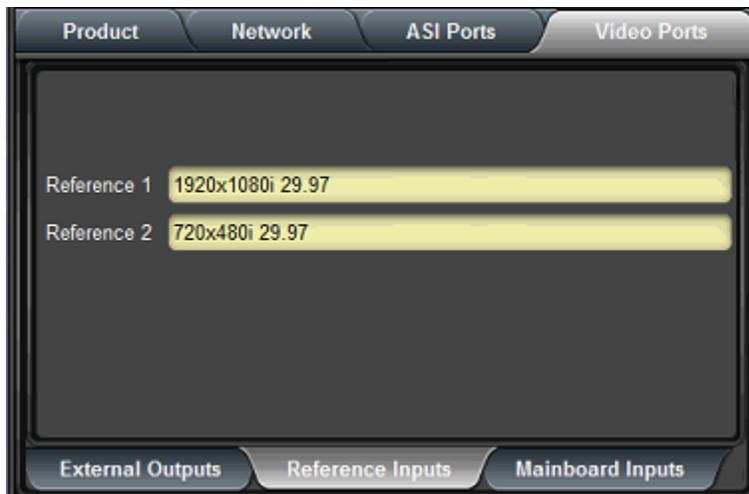
- **Video Signal:** This shows the type of signal being output, and the VPID information in the signal. The display is divided into three areas:
  - **Signal Type:** this will indicate SD-SDI, HD-SDI, 3G-SDI, 6G-SDI or 12-SDI.
  - **VPID Color Space:** this will indicate BT.709 or BT.2020.
  - **VPID Transfer Characteristics:** this will indicate SDR, HLG, or HDR.
  - Additionally, the word **Full** will be displayed if the Video Full-Range Flag is indicated.

The VPID information may be derived automatically from the incoming bitstream or may be manually set.



### Video Ports Statistics Reference Inputs Tab

The Reference Inputs tab shows the status of openGear frame reference inputs, used for the genlock function.



For each reference input, the resolution and frame rate are displayed. If there is no signal on a given reference input, the word **Unlocked** will be displayed.

### Video Ports Statistics Mainboard Inputs Tab

The Mainboard Inputs Tab is primarily for Cobalt Engineering use. It is displayed below.

---

The screenshot shows a control panel with four tabs: Product, Network, ASI Ports, and Video Ports. The 'ASI Ports' tab is active. Below the tabs, there are eight rows of status indicators, each with a colored circle and a text field:

Item	Status	Value
Input Lock 1	Green	OK
Input Lock 2	Green	OK
RX 1 Status	Green	1920x1080i 29.97
RX 2 Status	Red	No lock
RX 3 Status	Green	1920x1080i 29.97
RX 4 Status	Red	No lock
Port 1 Aligner	Green	Disabled
Port 2 Aligner	Green	Disabled

At the bottom of the panel, there are three additional tabs: External Outputs, Reference Inputs, and Mainboard Inputs.

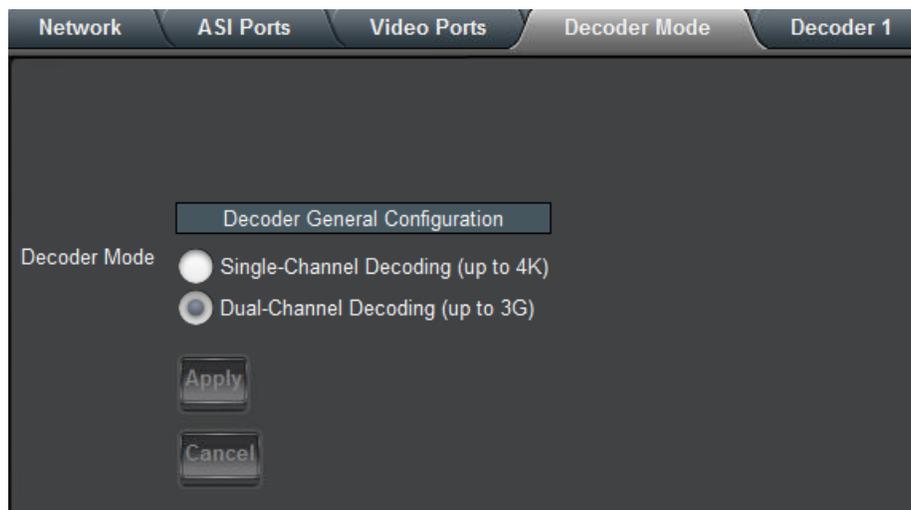
---

## Decoder Mode Tab

The Decoder Mode Tab is used to manage the parameters that are common to all decoder instances.

### ***Decoder Mode Configuration Tab***

The configurable parameters are:

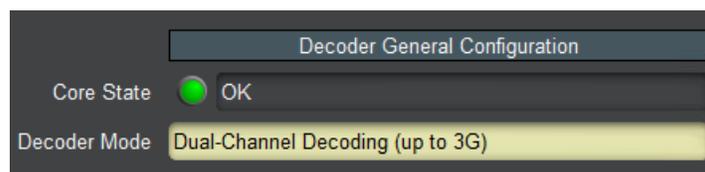


- **Decoder Mode:** The 9992-DEC can be configured either as a dual-channel HD decoder or a single-channel 4K decoder. Note that 4K operation requires the **+4K** option (factory installed in the 9992-DEC-4K-HEVC model). Also note that 4K operation is not supported for MPEG-2.

Once you make your selections click, **Apply**. **Note that making changes to this tab will cause all decoder instances to restart.** Clicking on **Cancel** reverts any changes.

### ***Decoder Mode Statistics Tab***

The Decoder Mode Statistics tab shows the current settings for the parameters in the Decoder Mode Configuration Tab.



This tab has one additional indicator, **Core State**. This indicator should always show **OK**. If it does not, please reboot the decoder and contact Cobalt Digital.

---

## Decoder 1-2 Tabs

The Decoder Tabs are used to configure/monitor the individual decoder channels. The number of tabs available depends on the configuration, as follows:

- In Single Channel mode, only Decoder 1 tab is available and provides up to 4 K decoding.
- In Dual-Channel mode, both Decoder 1 and Decoder 2 tabs are available and each tab provides up to 3 G decoding. The parameters in these Decoder tabs are identical.

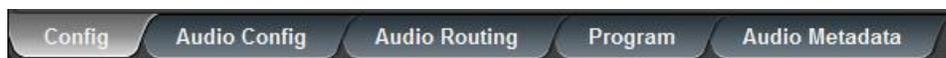
In general, the decoder user interface will change as a function of the parameter selections. Controls may appear or disappear as applicable.

All decoder tabs have **Apply/Cancel** buttons at the bottom. Clicking on **Apply** implements the changes, clicking on **Cancel** reverts them.

### ***Decoder Configuration Tab***

The Decoder Configuration Tab is divided into the five following tabs:

- **Config:** This tab has the common configuration parameters that apply to all decoding standards.
- **Audio Config:** This tab has the audio configuration options. They are generally a function of the decoding standard.
- **Audio Routing:** This tab has the routing configuration options.
- **Program:** This tab provides program information and the associated elements in the transport stream for that program.
- **Audio Metadata:** This tab has the audio service and the associated PID, including information pertaining to AC-4 and Dolby-E.



### **Decoder Config Tab**

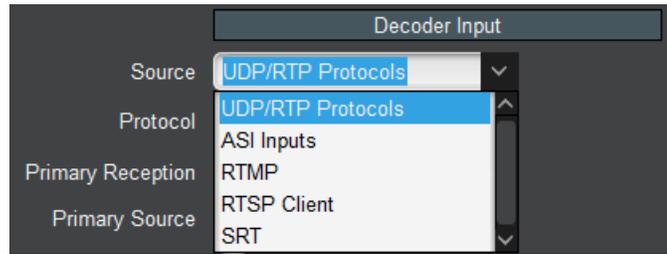
The decoder configuration tab is divided into the following functional areas:

- **Name:** All 9992-DEC decoder channels can be assigned a user-defined name. Use any descriptive name suitable for your application, or accept the default.
- **Decoder Input:** This allows you to select the **source** of the input.
- **Video Configuration:** This allows you to select parameters related to video decoding.
- **Ancillary Data Injection:** This allows you to select parameters to inject ancillary data.
- **Audio Parameters:** This allows you to select the number of audio channels.

#### **Config Tab – 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:

- **Source:** This control allows you select the source of the input for a decoder. This control has the following options; UDP/RTP Protocols, ASI Inputs, RTMP, RTSP Client and SRT.



The following stream sources are supported:

- **UDP/RTP Protocols:** the decoder will accept content on Ethernet over UDP/RTP, with optional support for SMPTE-2022 FEC or RIST. The decoder also supports the notion of a backup flow – if the primary flow disappears, the decoder will switch to the backup.
- **ASI Inputs:** the decoder will accept content on its ASI Input ports.
- **RTMP:** the decoder can operate as an RTMP client, retrieving a Flash stream from an RTMP Server, such as the Adobe Media Server or similar, or an RTMP server, accepting a stream from an RTMP client.
- **RTSP Client:** the decoder will connect to an RTSP server, such as an IP Camera, and play the content.
- **SRT:** the decoder will provide reliable transport over the Internet. By virtue of being a decoder device, the 9992-DEC is always a receiver. However, as far as the SRT connection is concerned, it can be a server (“listener”), waiting to be contacted by the sender, or a client (“caller”), which explicitly starts the connection with the sender. In either case, once the connection is established, the 9992-DEC will only receive. The FEC settings and encryption key length will be determined by the sender.
- **Decoder 1 Feed:** this option is only offered for **Decoder 2** in dual-decode mode. It copies whatever is being fed to Decoder 1 into Decoder 2. The main usage is when there is a unicast stream with multiple programs; configure Decoder 1 to receive it, and select this in Decoder 2 to decode a different program.

In all modes, the following buttons are available:



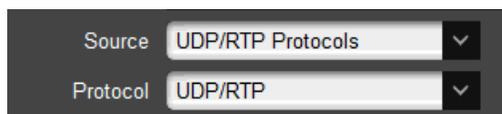
These buttons can perform a fast decoder restart if it stops for any reason and does not recover automatically.

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

---

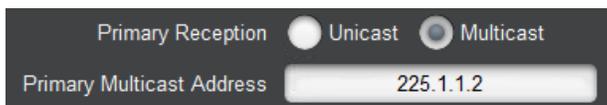
## Config Tab for UDP/RTP Protocols

When UDP/RTP or UDP/RTP+FEC Protocol is selected, the following controls become available:



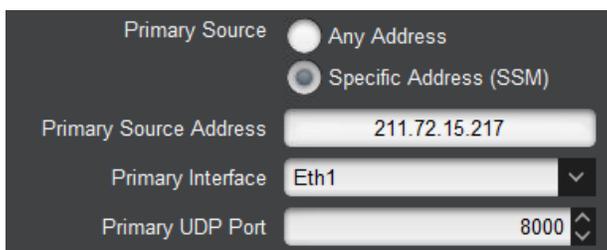
The screenshot shows two dropdown menus. The first is labeled 'Source' and has 'UDP/RTP Protocols' selected. The second is labeled 'Protocol' and has 'UDP/RTP' selected.

- **Protocol:** This control allows selection of the UDP/RTP Protocols. Options are:
  - **UDP/RTP:** UDP or RTP (auto-detected), no packet loss recovery.
  - **UDP/RTP+FEC:** UDP or RTP plus SMPTE ST 2022-1 FEC (optional license). FEC is automatically detected if present.
  - **UDP/RTP+RIST:** UDP or RTP plus VSF TR-06-1 RIST for packet recovery.
- **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:



The screenshot shows two radio buttons for 'Primary Reception': 'Unicast' (unselected) and 'Multicast' (selected). Below them is a text field labeled 'Primary Multicast Address' containing the value '225.1.1.2'.

- **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 9992-DEC will accept packets from any source IP address. If it is set to **Specific Address**, the 9992-DEC will only accept packets from a specific address, and a new field appears to configure this address:



The screenshot shows two radio buttons for 'Primary Source': 'Any Address' (unselected) and 'Specific Address (SSM)' (selected). Below them are three fields: 'Primary Source Address' with '211.72.15.217', 'Primary Interface' with 'Eth1', and 'Primary UDP Port' with '8000'.

- **Primary Source Address:** enter the specific source IP address from which the 9992-DEC will accept packets. If **Primary Reception** is set to **Multicast** and the 9992-DEC is configured for IGMPv3 operation, it will generate source-specific IGMP Join messages.
- **Primary Interface:** the selections are:
  - **Any:** accept packets on any interface. This selection is not available for multicast.
  - **Eth1:** only accept packets on the Ethernet 1 interface.
  - **Eth2:** only accept packets on the Ethernet 2 interface.
  - **RIST1:** only accept packets on the RIST1 tunnel. If the RIST1 tunnel is not configured, no packets will be received.

- **RIST2:** only accept packets on the RIST2 tunnel. If the RIST2 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:

The screenshot shows a configuration panel with the following settings:

- Redundant Reception:**
- Backup Reception:**  Unicast  Multicast
- Backup Source:**  Any Address  Specific Address
- Backup Interface:** Eth2
- Backup UDP Port:** 9000
- Flip Time (s):** 3
- Buttons:** Flip Redundancy, Restart Playback, Reset Network Statistics
- Pkt Loss Log Level (%):** 10.0

- **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).
- **Pkt Loss Log Level (%):** This can log excessive packet loss events. If the instantaneous uncorrected packet loss exceeds the threshold, a log entry will be created.

### Config Tab for UDP/RTP+RIST Protocols

When UDP/RTP+RIST Protocol is selected, the following controls become available:

- **Multi-Link:** this controls whether or not link aggregation is enabled. The options are:
  - **Single-Link:** if this is selected, the 9992-DEC will receive a single network stream for the content. Primary/Backup operation is still supported, and is configured exactly as described in the Config Tab for UDP/RTP section.
  - **Multi-Link:** if this is selected, the 9992-DEC 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 9992-DEC 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 9992-DEC 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 9992-DEC 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:

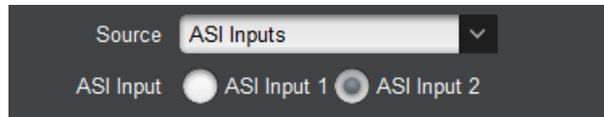
- **NACK Window (ms):** enter the window, in milliseconds, for the NACK packets. The value entered here should be at least equal to the round-trip delay between the encoder and the decoder multiplied by the value of the **Packet Retries** setting. Note that the value of the NACK window adds to the end-to-end (glass-to-glass) latency.
- **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.
- **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.
- **Packet Retries:** enter how many times the 9992-DEC should retry a dropped packet.

- **Reorder Buffer (ms):** enter the number of milliseconds the 9992-DEC 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.
- **Restart Playback button:** When clicked, this button
- **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.

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

### Config Tab for ASI Inputs

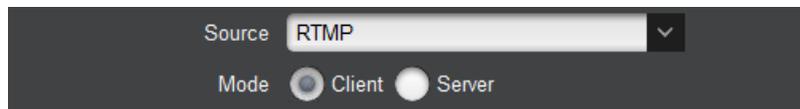
When ASI Input is selected, the following control becomes available:



- **ASI Input:** selects the ASI input

### Config Tab for RTMP

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



- **Mode:** selects either **Client** or **Server** mode for the RTMP source.

### *RTMP Client Configuration*

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 9992-DEC 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

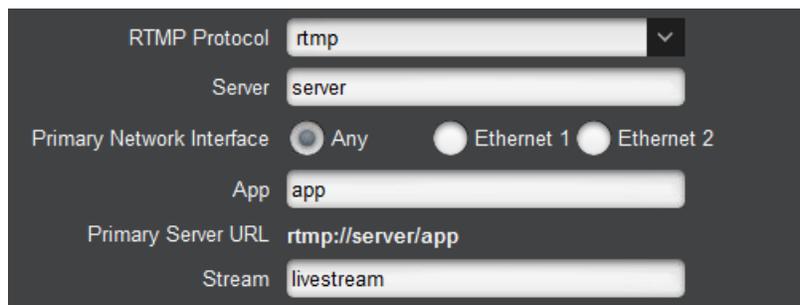
---

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:



The screenshot shows a configuration interface for an RTMP client. It features several input fields and a radio button group. The 'RTMP Protocol' is set to 'rtmp'. The 'Server' field contains 'server'. The 'Primary Network Interface' has three radio buttons: 'Any' (selected), 'Ethernet 1', and 'Ethernet 2'. The 'App' field contains 'app'. The 'Primary Server URL' field displays 'rtmp://server/app'. The 'Stream' field contains 'livestream'.

- **RTMP Protocol:** Select the protocol variant, as discussed above.
- **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 DNS Tab.
- **Primary Network 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 configured as a server, it will accept incoming connections on both Ethernet ports if the interface is set to **Any**.
- **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.
- **Primary Server URL:** This informational field is automatically updated as you configure the RTMP parameters. It displays the full RTMP URL for the primary server.
- **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.
- **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:

- **Port:** This field is only displayed if **RTMP Port Selection** is set to **Specific Port**. Configure a non-standard TCP port here.
- **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:

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

### *RTMP Server Configuration*

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://**.
- **App:** any arbitrary name can be used here. Configure the exact same name in the sender.
- **Stream:** this field is fixed at **livestream**. Configure this name in the sender.
- **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.

### Config Tab for 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 screenshot shows a configuration window titled "Decoder Input". It contains the following fields and controls:

- Source:** A dropdown menu set to "RTSP Client".
- RTSP URL:** A text input field containing "rtsp://server/file".
- TCP Transport:** A checked checkbox.
- Wait for Sync:** A checked checkbox.
- Authentication:** Radio buttons for "No" (selected) and "Yes".
- Username:** A text input field containing "cobalt".
- Password:** An empty text input field.

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 9992-DEC 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.
- **Authentication:** Some RTSP devices can be configured to require username/password authentication. Select **Yes** if this is the case.
- **Username:** enter the username expected by the RTSP device.
- **Password:** enter the password expected by the RTSP device.

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

RTSP support in the 9992-DEC 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 and H.265 compression are supported.
  - No support for encrypted passwords.

---

## Config Tab for SRT

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

Decoder Input

Source: SRT

Mode:  Caller  Listener  Rendezvous

UDP Port: 8000

Interface:  Any  Eth1  Eth2

Connection Timeout (ms): 5000

Connection Latency (ms): 100

Encryption:

Pkt Loss Log Level (%): 0.1

The configuration parameters are as follows:

- **Mode:** This selects between **Listener** (server), where the device will wait to be connected, **Caller** (client), where the device will explicitly connect to a sender, and **Rendezvous**, where the device will attempt to connect to another device in rendezvous mode. If **Caller** or **Rendezvous** are selected, new fields will appear, as indicated below:

Decoder Input

Source: SRT

Mode:  Caller  Listener  Rendezvous

Stream ID: Decoder 1

Server Address: 192.168.1.1

UDP Port: 8000

Interface:  Any  Eth1  Eth2

- **Stream ID:** this is an arbitrary string sent from the caller to the listener, for identification purposes. In rendezvous mode, the Stream ID of one of the endpoints is arbitrarily selected for the connection.
- **Server IP Address:** this is the IP address of the server (“listener”) to be contacted.
- **UDP Port:** This is the UDP port to be used for the communication. If the decoder is a **Listener**, it will listen on this port for incoming connections. If it is a **Caller**, it will connect to this port in the server. In **Rendezvous** mode, the specified UDP port is used both to listen for connections and to contact the partner.
- **Interface:** The 9992-DEC has two streaming interfaces. You can restrict communication on one of them, or leave it to the 9992-DEC to choose the most suitable. In particular, if

---

the decoder is a **Listener**, selecting **Any** will cause it to accept incoming connections on either one of the interfaces.

- **Connection Timeout:** This configures the amount of time the decoder will keep a connection open without any data. After the timeout, the connection is dropped and restarted.
- **Connection Latency:** This configures the incoming stream buffer. It should be a multiple of the round-trip time to the other endpoint.
- **Encryption:** Checking this box will enable encryption of the content. When the box is checked, a second field appears for the passphrase:



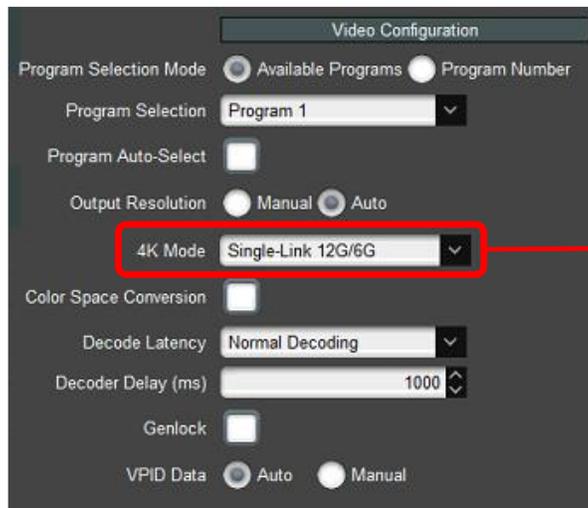
- **Encryption Passphrase:** Enter the encryption passphrase (minimum 10 characters). It must match the Passphrase at the sender or communication will not be possible.

Note that the encryption key length will be determined by the sender.

- **Packet Loss Log Level (%):** The 9992-DEC can log excessive packet loss events. If the instantaneous uncorrected packet loss exceeds the threshold, a log entry will be created.

## Config Tab – Decoder Video Configuration

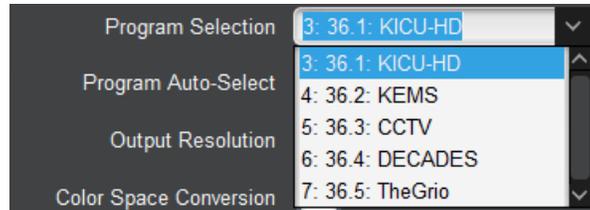
The configuration parameters are as follows:



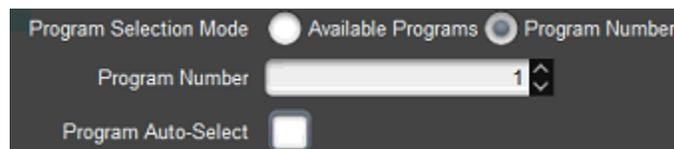
Only displayed in single-channel mode

- **Program Selection Mode:** a transport stream may contain multiple programs. This control defines how the decoder selects a program inside the transport stream to decode. The two options are:
  - **Available Programs:** in this mode, the **Program Selection** drop-down 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 front followed by the channel and the call letters. If not, the program is

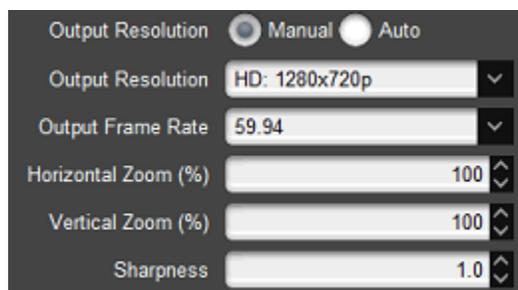
shown as **Program X**, where **X** is the actual program number. In the example below, program (3) has channel (36.1) and call letters (KICU-HD), so it shown as “**3: 36.1: KICU-HD**”, and the other programs that do not have that information will simply give it a generic number.



- **Program Number:** in this mode, the **Available Programs** dropdown disappears and is replaced by a **Program Number** selection field, where any program number between 1 and 65535 can be entered.

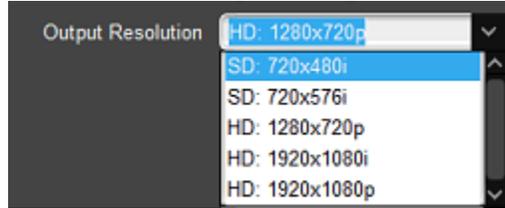


- **Program Auto-Select:** this checkbox controls the behavior of the decoder if the selected program does not exist in the transport stream. If it is checked, the decoder will play instead the first available program that has video. If it is not checked, and the selected program does not exist, the decoder will not play and will stay in alarm.
- **Output Resolution:** this controls the decoder output signal. Options are:
  - **Auto:** the decoder output signal resolution and frame rate will be set automatically to match the incoming bitstream.
  - **Manual:** the 9992-DEC includes a full-featured up/down/cross converter, capable of converting any input signal to any output resolution and frame rate up to 1920×1080p60<sup>3</sup>. If **Manual** is selected, the following additional options are presented:

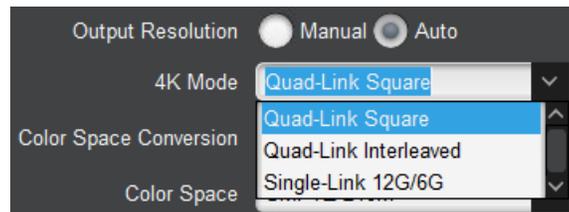


- **Output Resolution:** Select the spatial resolution, from one of the following options:

<sup>3</sup> 4K signals can be downscaled to 3G or lower resolutions. Upscaling to 4K is not supported in the 9992-DEC.



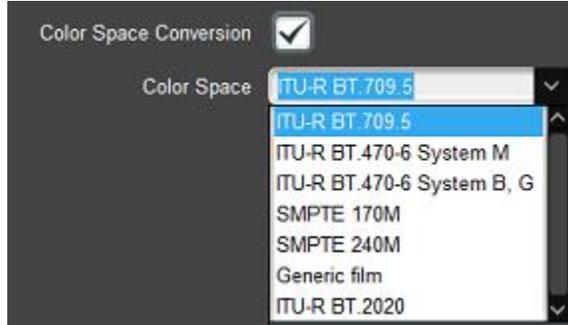
- **Output Frame Rate:** select the desired output frame rate, in frames per second<sup>4</sup>. This is a drop-down menu populated with the frame rates suitable for the selected output resolution.
- **Horizontal Zoom, Vertical Zoom:** these controls can be used to modify the image aspect ratio. The valid range is from 50% to 150%. Images whose size is reduced will be centered vertically and/or horizontally.
- **Sharpness:** this controls the sharpness of the conversion. The range is from 0.5 to 1.5. Higher values make the image sharper but can cause artifacts.
- **4K Mode:** This is only shown if the 9992-DEC is in single-channel decode mode, and is only effective if the input bitstream is actually 4K. Select the desired output type, between Single-Link 12G/6G, and quad-link HD/3G, in Square Division or Interleaved modes.



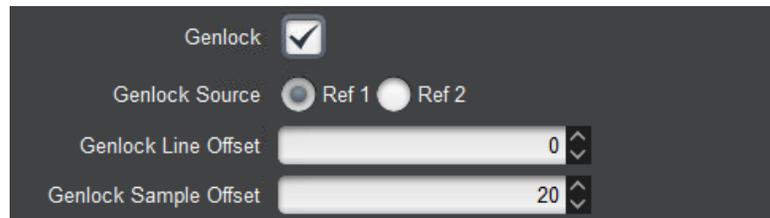
**Note:** In Single-Link 12G/6G, SDI outputs 1 and 2 will have the 12G/6G signal, while SDI outputs 3 and 4 will have a 3G/HD version of the same signal. Internally, the 9992-DEC generates a quad-link interleaved signal, and SDI outputs 3 and 4 represent lanes 3 and 4 of this signal. These lower-resolution signals are provided **as-is** for monitoring purposes only.

- **Color Space Conversion:** Check this box to cause the decoder to do color space conversion. If the box is not checked, no color space conversion is performed. If the box is checked, an additional control to select the color space is displayed:

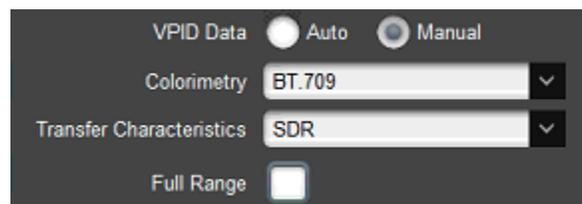
<sup>4</sup> This is in frames, not fields. For example, if the resolution is set to 1920x1080i, the frame rate options will be 25, 29.94, and 30.



- **Color Space:** Select the color space to use; ITU-R BT 709.5, ITU-R BT 470.6 System M, ITU-R BT 470.6 System B. G, SMPTE 170M, SMPTE 240M, Generic film, ITU-R BT 2020.
- **Decoder Delay (ms):** Set the decoding delay in milliseconds. The range is from zero to 3000 ms. If this value is set too low, audio decoding may be affected.
- **Genlock:** If this box is checked, the SDI output can be genlocked to a reference signal. The following controls become available:



- **Genlock Source:** Select the reference to use.
- **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.
- **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).
- **VPID Data:** the 9992-DEC will always include VPID in the output signal, and will set the correct resolution and frame rate for the signal. This control manages the VPID colorimetry, transfer characteristics, and video full range flag. The options are:
  - **Auto:** colorimetry, transfer characteristics, and video full range flag are set from bitstream metadata.
  - **Manual:** colorimetry, transfer characteristics, and video full range flag are set manually. The following controls become available:



- **Colorimetry:** options are BT.709, BT.2020, and Unspecified.
- **Transfer Characteristics:** options are SDR, HLG, PQ and Unspecified<sup>5</sup>.
- **Full Range:** if this box is checked, the Video Full Range flag is set in the VPID data.

## Config Tab – Ancillary Data Injection Configuration

The configuration parameters are as follows:

Ancillary Data Injection	
Closed Caption Type	SMPTE 334/708
CC VANC Line	9
Enable AFD	<input checked="" type="checkbox"/>
AFD VANC Line	10
Enable SMPTE-2038 ANC	<input checked="" type="checkbox"/>
Enable SCTE-35 Conversion	<input checked="" type="checkbox"/>
Automation Server	0
DPI PID Index	2
SCTE-104 VANC Line	13
Enable HDR Metadata	<input checked="" type="checkbox"/>
HDR VANC Line	11

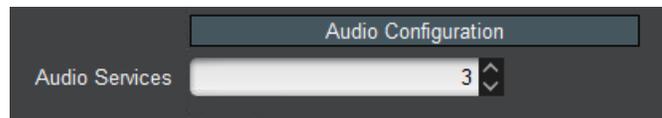
- **Closed-Caption Type:** The decoder supports Closed-Caption (CC) injection if the incoming bitstream has captions. The options are a function of output resolution:
  - **Off:** no Closed-Captioning injection.
  - **EIA-608 Line 21:** This option is only offered if the **Output Resolution** is manually set to SD. Closed-captions come out on 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.
- **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 AFD:** Check this box to enable Active Format Description (AFD) extraction and insertion. AFD is inserted in the video elementary stream as per ATSC A/72 and ETSI TS 101 154.
- **AFD VANC Line:** This control is only displayed if the **Enable AFD** box is checked. It determines in which VANC line AFD is inserted.

<sup>5</sup> In some devices, Unspecified is assumed to SLOG3.

- **Enable SMPTE-2038 ANC:** If generic ANC has been included in the stream using SMPTE ST 2038 formatting, the decoder can retrieve the encoded ANC and re-insert it into the outputted SDI stream if this box is checked (line location is the same as the line the encoder noted when integrating the ANC in the transport stream).
- **Enable SCTE-35 Conversion:** If this box is checked, the decoder converts transport stream SCTE-35 sections back to SCTE-104 VBI ANC and re-inserts this data. 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.
- **Enable HDR Metadata:** Check this box to enable SMPTE 2108 extraction and insertion as SEI messages in the video elementary stream.
- **HDR VANC Line:** If the **Enable HDR Metadata** box is checked, this control is displayed. It determines which VANC line to use for HDR metadata insertion.

### Config Tab – Audio Configuration

The configuration parameters are as follows:

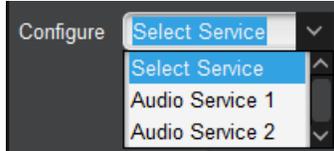


- **Audio Services:** This selects the number of Audio Services to be decoded, from zero to 8. The number of audio services configurable is subject to licensing. Note that an “Audio Service” is equivalent to an “Audio PID” and can be mono, stereo, or surround (for supported audio decoding standards). Also note that, in RTMP input source, this control is fixed to one (1) as RTMP has no support for more than one audio service.

Individual audio channel configuration is done in the Decoder Audio Config Tab.

### Decoder Audio Config Tab

The Audio Config Tab is used to configure individual audio decoding services. Only one service is configured at a time. The first step in configuring a service is to select it in the **Configure** drop-down menu. This menu will be populated with however many audio services have been selected in the Config Tab – Audio Configuration. An example is shown below.



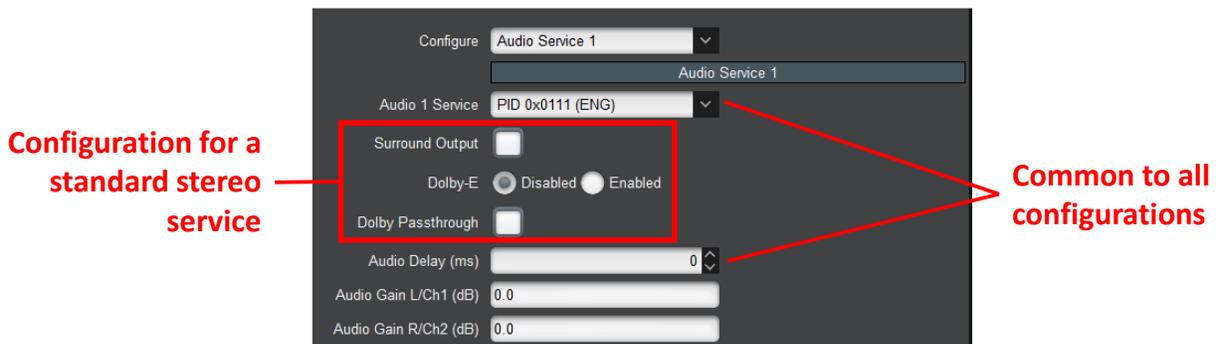
The appearance of the audio configuration controls depends on the selections made.

Note that the 9992-DEC has no a priori knowledge of what type of audio is coming in. Once it actually receives the audio, it will attempt to map the incoming signal into the desired configuration, as follows:

- If the decoder is configured for stereo output, and the incoming audio is surround, it will be automatically downmixed to stereo. For Dolby AC-4, the downmix algorithm can be selected.
- If the decoder is configured for surround output, and the incoming signal is stereo, it will be mapped to the Left/Right channels, and the remaining channels will have silence.
- If the decoder is configured for Dolby-E operation, and the incoming signal is not Dolby-E, it will be mapped to either the first two channels (if it is stereo) or six channels (if it is surround).
- If the decoder is not configured for Dolby-E operation, and it receives a Dolby-E signal, it will treat this signal as a SMPTE ST 302 LPCM signal. Note that frame alignment **is not** guaranteed in this case.

### Decoder Audio Config Tab – Standard Stereo Service

The configuration for a standard stereo service is displayed below.



The following parameters are common to all configurations:

- **Audio 1 Service:** Select the audio PID for this audio service. The drop-down list will be pre-populated with the detected audio PIDs in the program. By default, the first audio service will take the first audio PID, the second audio service will take the second audio PID, and so on. If your input source is set to RTMP this parameter will not appear.
- **Audio Delay (ms):** Use this to compensate for up to  $\pm 100$  milliseconds of audio delay in the signal. This setting will advance or delay the audio in relation to the video by the amount configured.

The following parameters define the desired output mode:

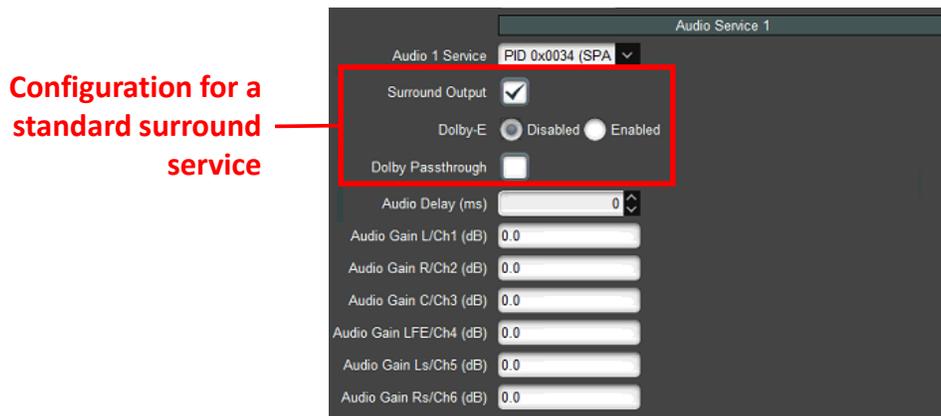
- **Surround Output:** Check this box to enable surround sound parameters. If Dolby-E is enabled this selection will not appear.
- **Dolby-E:** Select to **Disable** or **Enable** Dolby-E features. If enabled additional parameters are available to configure.
- **Dolby Passthrough:** Check this box to allow the Dolby passthrough. Since Dolby Passthrough is pre-encoded, the audio level controls are not available.

For all modes where there is actual audio decoding, the 9992-DEC allows for individual audio gain control for each of the decoded channels. The number of controls displayed is a function of the mode – i.e., two controls will be displayed for stereo, six for surround, and eight for Dolby-E. The operation is as follows:

- **Audio Gain L/Ch1 R/Ch2 (dB):** This control allows an independent gain adjustment for the left and right audio channels, from -18.0 dB to +18.0 dB, in steps of 0.5 dB. If this audio decoder channel is configured for Surround operation, additional gain controls become available.

### Decoder Audio Config Tab – Standard Surround Service

The configuration for a standard surround service is depicted below:

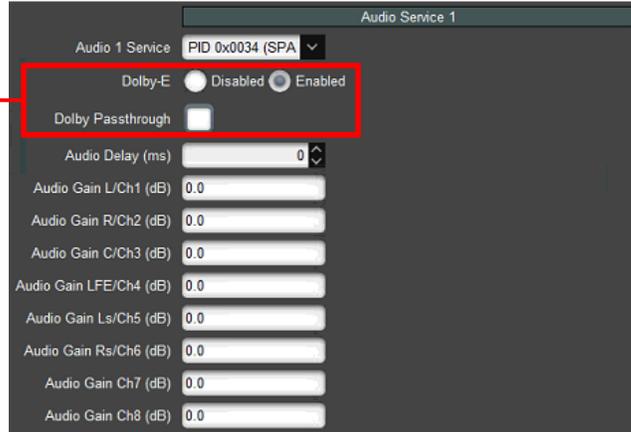


The parameters are the same as with stereo, but more gain controls are now available.

### Decoder Audio Config Tab – Dolby-E Mode

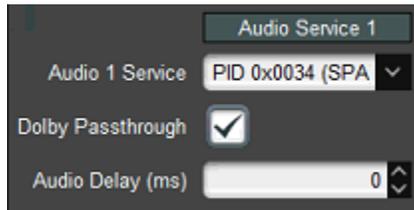
The configuration for Dolby-E is depicted below. It is similar to stereo and surround, but it offers eight gain controls, as a Dolby-E service may have up to 8 channels.

**Configuration for a  
Dolby-E service**



### Decoder Audio Config Tab – Dolby Passthrough

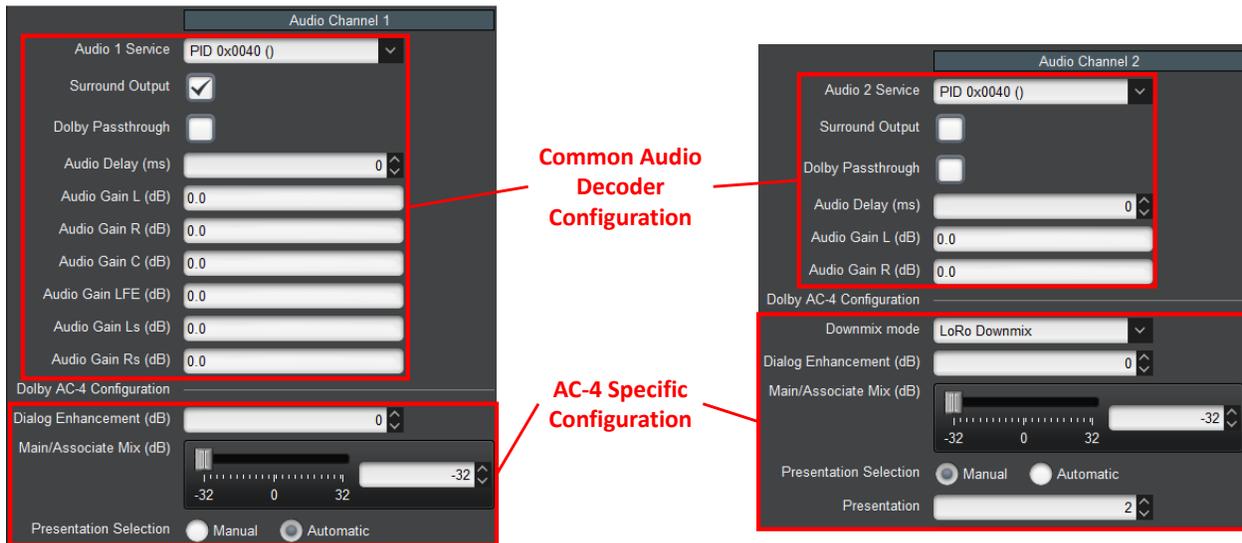
The configuration for Dolby pass-through is depicted below:



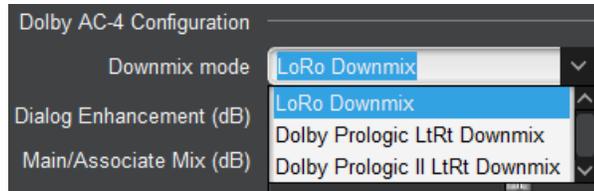
The 9992-DEC supports Dolby AC-3, EAC-3 and AC-4 pass-through. If the incoming bitstream is not one of these types, an alarm will be raised and no audio will be decoded.

### Dolby AC-4 Configuration

All audio configuration modes include Dolby AC-4 specific configuration. If the incoming bitstream is not Dolby AC-4, these settings are not used. The configuration parameters are:



- **Downmix mode:** this control is only displayed if the channel is configured for stereo output. It will be effective if the content is multi-channel, and it selects the downmix algorithm. Select the mode to downmix from the menu shown below. This parameter is only available if you do not use Surround or Dolby.
  - **LoRo Downmix:** Select for left and right only downmix.
  - **Dolby Prologic LtRt Downmix:** Select for Dolby Prologic downmix.
  - **Dolby Prologic II LtRt Downmix:** Select for Dolby Prologic II downmix.



- **Dialog Enhancement (dB):** This controls the dialog enhancement setting in the decoder. The range is from -12dB to +12dB in steps of 1dB.
- **Main/Associate Mix (dB):** Some AC-4 presentations may have a second substream of associate audio. If this slider is set to -32 dB, the 9992-DEC will only decode the Main substream. As the slider is moved, the Associate substream will be mixed in. At 0 dB, it will be mixed at the default level indicated in the bitstream. At 32 dB, only the associate substream will be played.
- **Presentation Selection:** An AC-4 stream may have multiple presentations. A given audio channel in the 9992-DEC will only decode one presentation. This control selects which presentation to decode. If it is set to **Manual**, a specific presentation can be selected using the following parameter.
- **Presentation:** Enter the number of the specific presentation.

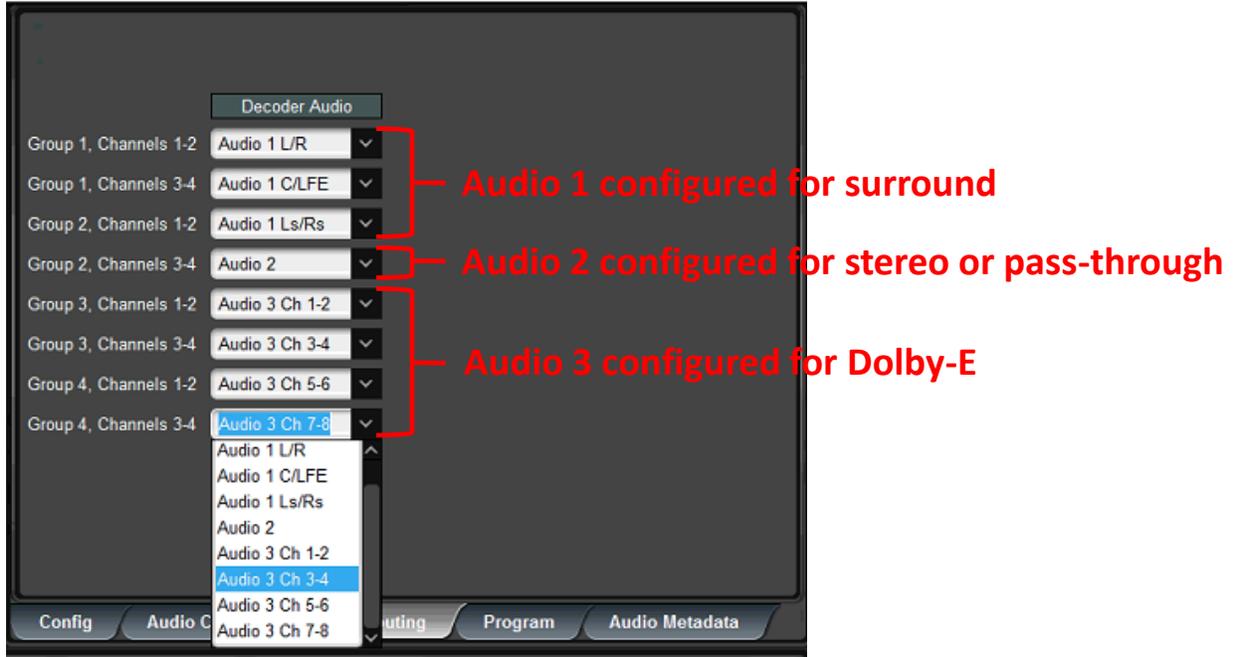
Note that if an AC-4 stream has multiple presentations, the 9992-DEC can decode them by enabling multiple audio channels, configuring them to accept the same PID, and selecting a different presentation on each channel. This is shown in the picture above: both decoder channels are processing PID 0x40, with Audio Channel 1 decoding the default presentation and Audio Channel 2 decoding Presentation 2. The same method can be employed to play the Main substream in one channel and the Associate substream in another channel.

## Decoder Audio Routing Tab

The Audio Routing Tab is used to map decoded audio pairs to SDI embedded pairs. Until this step is done, no audio comes out in the SDI signal. Note that the audio routing step can only be done after the **Apply** button is clicked – that is when the drop down menus in the audio routing tab are populated. There is no **Apply** button in this tab; all changes are implemented immediately.

Audio routing is done from the point of view of the SDI output: a decoded audio pair is assigned to each group/pair in the output. The same audio pair can be replicated to multiple group/pairs in the output. The number of available pairs for an audio service depends on its configuration – a stereo or pass-through service will have one pair, a surround service will have three pairs, and a Dolby-E service will have four pairs.

The figure below illustrates a scenario where Audio 1 has been configured for surround operation, Audio 2 has been configured for stereo operation, and Audio 3 has been configured for Dolby-E operation. The drop-down menus are automatically populated with the relevant options.

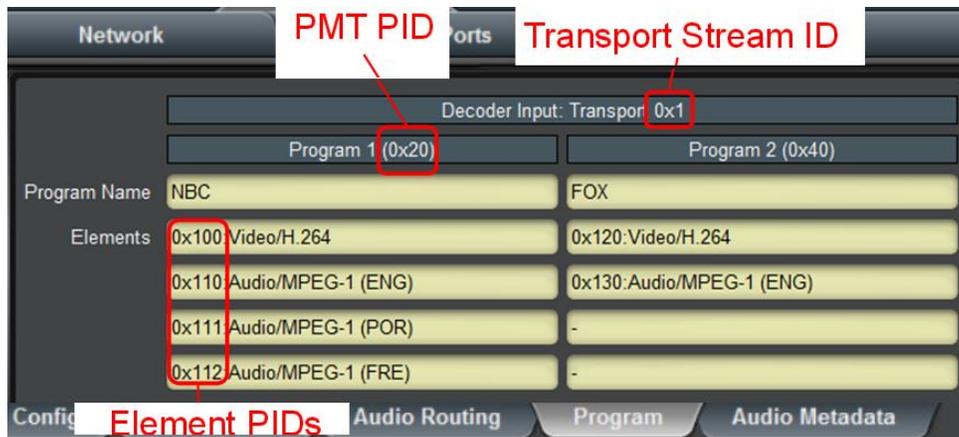


## Decoder Program Tab

The Program Tab is strictly informational, and its appearance is a function of the type of data being decoded.

### Decoder Program Tab – Transport Streams

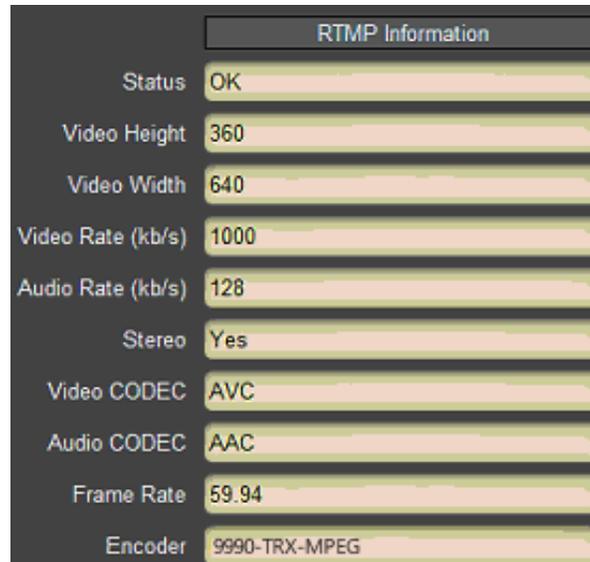
The Program Tab for Transport Streams is as follows:



- **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.

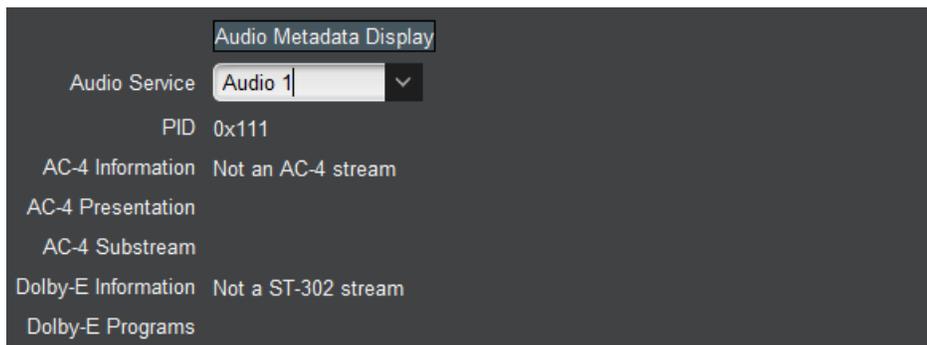
### Decoder Program Tab – RTMP Mode

For RTMP Streams, the Program Info Tab shows the RTMP Information, if it has been provided by the connected party. This information is retrieved from the RTMP metadata; not all devices provide it.



### Decoder Audio Metadata Tab

This tab can be used to inspect the Dolby AC-4 or Dolby-E metadata of any audio channel. If the channel is not running Dolby AC-4 or Dolby-E the following is displayed:



- **Audio Service:** Select the audio service from the drop-down list.
- **PID:** Indicates the audio PID for this stream.
- **AC-4 Information:** This is general information for the whole stream.
- **AC-4 Presentation:** This information is specific to the presentation.
- **AC-4 Substream:** This information is specific to the substreams in the presentation. The 9992-DEC will only show up to two substreams.
- **Dolby-E Information:** This provides general information on the Dolby-E stream, including the channel mode and which channels are active.
- **Dolby-E Programs:** This provides detailed information on the Dolby-E programs in the stream, if present.

. Here is an example of decoded AC-4 metadata:

```

AC-4 Information  Bitstream Version: 2
                  Bit rate mode: Average Bit Rate
                  Frame Rate: 25 fps
                  Sample Rate: 48 kHz
                  Presentations: 2

AC-4 Presentation Number of substreams: 2
                  Configuration: Main + Associate
                  Type: Associate with Main
                  Level: 2
                  Group: Undefined

AC-4 Substream  Substream 1:
                  Mode: 5.1
                  Type: Main
                  Substream 2:
                  Mode: Mono
                  Type: Associate

```

Here is an example of decoded Dolby-E metadata:

```

Dolby-E Information  ST-302 size: 20 bits
                    ST-337 size: 20 bits
                    Active Channels: 8
                    Program Mode: 8x1
                    Active Channels: 12 34 56 78

Dolby-E Programs    Pgm 1: Test Program E
                    Pgm 2: Test Program E
                    Pgm 3: Test Program E
                    Pgm 4: Test Program E
                    Pgm 5: Test Program E
                    Pgm 6: Test Program E
                    Pgm 7: Test Program E
                    Pgm 8: Test Program E

```

---

## 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 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. 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 Keys 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 Cobalt Digital 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.

## The Apply/Cancel Buttons

The **Apply/Cancel** buttons are available at the bottom of the **Config** and **Audio Config** tabs. These are not separate buttons – they are multiple instances of the same buttons, repeated on each screen for convenience. If no changes have been made to the settings, the **Apply/Cancel** buttons are grayed out; once any changes are made, they become available. Changes do not take effect until the **Apply** button is pressed. If you make changes but decide not to apply them, click on the **Cancel** button and the user interface reverts to where it was before. Once you click on the **Apply** button, the changes are implemented.



In general, most changes will cause the decoder channel to stop and start again, causing a brief (2-second) interruption to the stream. Changes to the following parameters are implemented on-the-fly, without stopping the decoder:

- Any VBI/Ancillary data changes in Config Tab – Ancillary Data Injection Configuration.
- VPID changes in Config Tab – Decoder Video Configuration.
- Audio Gain changes in Decoder Audio Config Tab.

---

## Decoder Statistics Tab

The Decoder Statistics Tab is divided into five lower tabs, as indicated below:

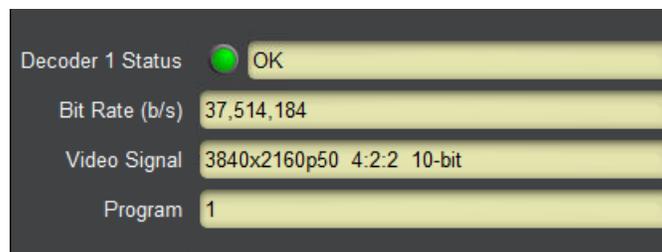


The **Config** tab in the Decoder Statistics is a direct equivalent of its configuration counterpart. It presents the current value of each of the configuration parameters. When the **Apply/Cancel** buttons are grayed out, the contents of this tab exactly matches its configuration counterpart. When the **Apply/Cancel** buttons are active, configuration parameters have not been changed. The current (running) decoder configuration can still be inspected in the statistics tabs, prior to clicking on the **Apply** button.

### Status Tab

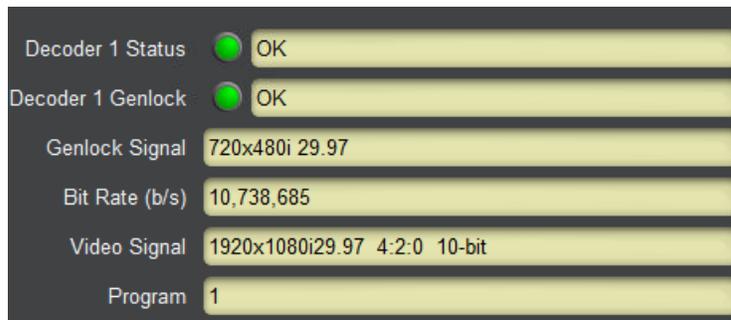
The **Status** Tab provides a summary of the status of the decoder. The variables displayed in this tab vary according to the encoder configuration.

The following basic parameters are always displayed:



- **Decoder 1 Status:** This gives the overall decoder status. Its values are:
  - **OK:** The decoder is running normally.
  - **Illegal Stream:** The decoder has valid input, but the stream has illegal syntax. This will happen when the video elementary stream is missing the Access Unit Delimiters (AUDs), which is illegal for transport stream content.
  - **Not Running:** The decoder is not running because it has not recognizable input. This may be because it has no input, or because it is looking for a program that is not present in the transport stream, and the **Program Auto Select** box in the Config Tab – Decoder Video Configuration is not checked.
- **Bit 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.
- **Video Signal:** If there is any recognizable video signal at the decoder video input, this field will indicate what type of signal the decoder is detecting. If no recognizable video signal is detected, this field will indicate **No signal**. Note that, for MPEG-2 streams, the color mode (4:2:2 versus 4:2:0) is not displayed.
- **Program:** This section contains the current program number being decoded.

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:

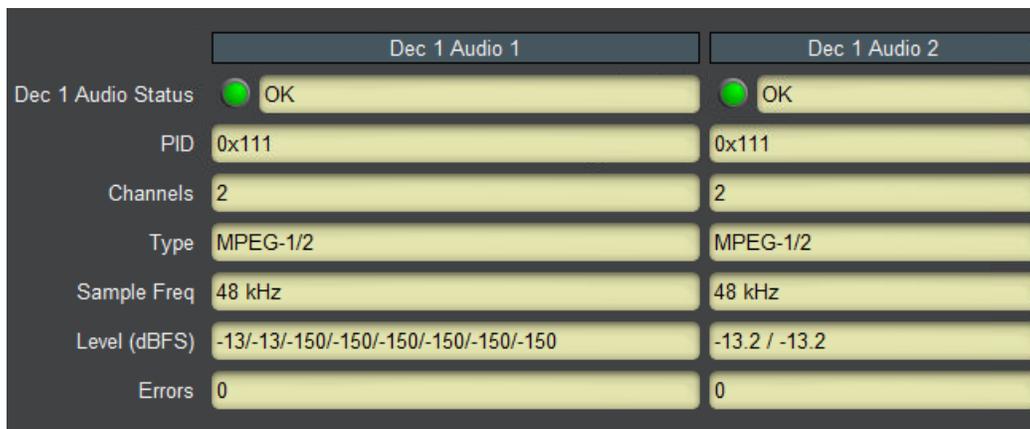


- **Genlock Status:** this field can show the following values:
  - **OK:** The genlock function is operating normally, and the output is genlocked to the reference.
  - **Incompatible Reference:** The Decoder has detected a valid genlock signal, but the decoder output is incompatible with this genlock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

## Audio Status Tab

The **Audio Status** Tab provides a summary of the status of the decoder audio service. If you have not configured an Audio Service this tab will not appear. The variables displayed in this tab vary according to the decoder configuration.

The following parameters are displayed:



- **Dec 1 Audio Status:** This gives the overall audio status. Its values are:
  - **OK:** The decoder is running normally.
  - **Not Present:** The audio service is not present in the transport stream.
- **PID:** shows the audio PID for this audio service.

- **Channels:** Indicates the number of channels for this service. This indicator will have the value of 1 for mono services, 2 for stereo services, and 6 for surround services. Note that an incoming surround service configured for stereo output will have the value 6 here.
- **Type:** Provides the compression standard for the audio service.
- **Sample Freq:** Provides the sampling frequency for the audio service. Note that SDI signals require a 48 kHz audio sampling rate. The 9993-DEC will automatically convert the sample rate of incoming signals to 48 kHz for output.
- **Level (dBFS):** Provides the instantaneous audio level. For stereo services, two values are provided, corresponding to left/right levels. For surround services, six values are provided, corresponding to L/R/C/LFE/Ls/Rs.
- **Errors:** Provides a running count of the number of errors. This this count can be reset by clicking the **Reset Network Statistics** button in the Config Tab – Decoder Input Configuration.

## Network Tab

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

### Network Tab for UDP/RTP Stream

The following statistics are displayed for UDP/RTP:

Received Rate (b/s)	37,516,646
Protocol	UDP
Stream Source IP Address	10.10.9.80
Current Source	Primary
Received Packets	6218278101
Lost 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.
- **Stream Source IP Address:** This is the source IP address used.
- **Current Source:** This states the current source, primary or backup.
- **Received Packets:** This shows how many packets have been received.
- **Lost Packets:** This shows how many packets have been lost. Note that the 9992-DEC can only detect lost packets if the protocol is RTP.

### Network Tab for UDP/RTP+FEC Stream

The following additional statistics are displayed:

- **SMPTE 2022 FEC:** Indicates the detected FEC mode, as follows:
  - **None:** SMPTE 2022 FEC transmission is not being detected by the 9992-DEC.

- **Column Only:** The 9992-DEC is detecting SMPTE 2022 FEC in Column Only mode.
- **Row and Column:** The 9992-DEC 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 9992-DEC.
- **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 9992-DEC 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.

Received Rate (b/s)	14,193,716
Protocol	RTP
Stream Source IP Address	10.10.9.82
Current Source	Primary
SMPTE 2022 FEC	Column only
Columns	5
Rows	10
Received Packets	119975
Lost Packets	0
Recovered Packets	0
Unrecovered Packets	0
Invalid FEC Packets	0

---

## Network Tab for UDP/RTP+RIST Stream

The following additional statistics are displayed for UDP/RTP+RIST:

Received Rate (b/s)	4,635,173
Protocol	RTP
Stream Source IP Address	10.10.9.82
Current Source	Primary
Received Packets	172534830
Retransmissions Received	2496
Lost Packets	432
Recovered Packets	0
Unrecovered Packets	0
NACKs Sent	8
Late Packets	0
Duplicate Packets	80141739
RTCP Received	1927600
RTCP Source IP Address	10.10.9.82
RTCP Source Port	8001
RTT	0 ms
Buffer (Pkts)	1098

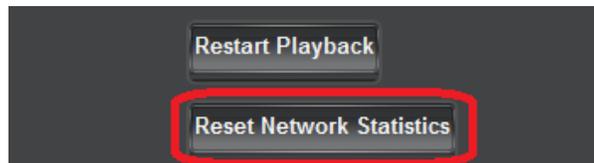
- **Retransmissions Received:** This shows how many retransmissions have been received.
- **Recovered Packets:** This indicates the total number of packets recovered with RIST since the last time the statistics were reset.
- **Unrecovered Packets:** This indicates the total number of lost packets that could not be recovered with RIST because a retransmission for them was never received.
- **NACKs Sent:** This 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:** This 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:** This 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:** This 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:** This 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 9992-DEC 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 Config Tab – Decoder Input Configuration, also reproduced below:



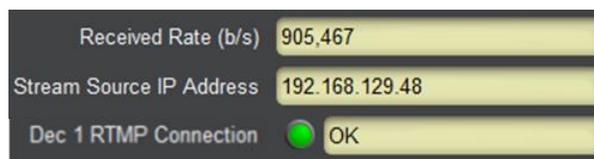
### Network Tab for ASI Input

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 RTMP Client and Server

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



- **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.
- **Dec 1 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)	1,866,609
Stream Source IP Address	192.168.129.127
Dec 2 RTSP Connection	● OK
Video Frame Rate	30
Video UDP Port	33708
Video CODEC	H264
Audio UDP Port	0
Audio CODEC	

- **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.
- **Dec 1 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 Frame Rate:** This field contains the video frame rate, as measured by the decoder.
- **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 9992-DEC only supports H.264 or H.265 in RTSP mode, but this field will always be updated.
- **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. 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 9992-DEC 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 SRT

The Network Tab Statistics for the SRT is depicted below:

Received Rate (b/s)	4,719,736
Stream Source IP Address	10.10.9.4
Stream ID	ciro_stream
Connection State	Connected
Encryption State	<span style="color: green;">●</span> Secured OK
Encryption Key	128-bit
Received Packets	19075890
Retransmissions Received	0
Lost Packets	1
Unrecovered Packets	0
Late Packets	0
SRT Undecrypted	0
SRT FEC Recovered	2777313
SRT FEC Unrecovered	4
RTT	0.5 ms

The available statistics are:

- **Received Rate (b/s):** indicates the current incoming payload bit rate (does not include overhead).
- **Stream Source IP Address:** indicates the IP address of the remote endpoint.
- **Stream ID:** indicates the current Stream ID. If the decoder is in **Caller** mode, this will be the Stream ID configured in the GUI. If it is in **Listener** mode, it will be the Stream ID received from the remote end. If it is in **Rendezvous** mode, it will be the final selected Stream ID for the connection.
- **Connection State:** indicates the current connection state.
- **Encryption State:** indicates the current encryption state. This is an alarm and will be red in error conditions. The text indicates the exact condition.
- **Encryption Key:** indicates the current key size. The key size is set at the sender.
- **Received Packets:** count of packets received so far in this connection.
- **Retransmissions Received:** count of retransmissions received so far in this connection.
- **Lost Packets:** count of lost packets.
- **Unrecovered Packets:** count of lost packets that the protocol has not been able to recover.
- **Late Packets:** count of good packets that arrived too late (based on the **Connection Latency**) setting.
- **SRT Undecrypted:** count of packets for which the decryption failed.

- **SRT FEC Recovered:** count of packets recovered using FEC.
- **SRT FEC Unrecovered:** count of packets that were not recovered using FEC.
- **RTT:** measured Round Trip Time to the sender, in milliseconds.

## Multi-Link Tab

The Multi-Link Tab is only displayed if the decoder is configured for UDP/IP+RIST Protocols (see Config Tab for UDP/RTP+RIST Protocols) and in Multi-Link mode. This tab provides per-link statistics similar to those presented in the Network Tab for UDP/RTP+RIST Stream.

	Link 1	Link 2
Bitrate	6,647,786	6,530,052
Pkt RX	34858525	34162135
Pkt Used	34837733	20792
Retrans RX	0	0
RTCP RX	584546	579012
RTT	0 ms	
Source	10.10.9.10	10.10.9.12

- **Bitrate:** indicates the instantaneous received bit rate in the link.
- **Pkt RX:** indicates the number of packets received in the link.
- **Pkt Used:** indicates the number of packets used from this link in the final playback.
- **Retrans RX:** indicates the number of retransmissions received in this link.
- **RTCP RX:** indicates the number of RTCP messages received in this link.
- **RTT:** indicates the Round-Trip Time for this link, if it can be measured.
- **Source:** indicates the source IP address for the packets received in this link.

## Ancillary Data Tab

The **Ancillary** Tab provides the status of the ancillary data injection in the decoder. The variables displayed in this tab vary according to the decoder configuration; it will only include the ancillary data injection functions currently enabled (see Config Tab – Ancillary Data Injection Configuration). Note that if no ancillary data processing is enabled, this tab will not be present.

The following parameters are displayed:

Closed Captions	Not Present	} Closed Captions
AFD	Not Present	
HDR Metadata	Not Present	} Active Format Descriptor
SMPTE-2038	Not Present	
SMPTE-2038 Inserted	0	} HDR Metadata
SCTE-104 Inserted	0	
SCTE-35 Errors	0	} SMPTE 2038
		} SCTE 104 to SCTE 35

- Closed Captions:** This reports Closed Caption insertion. This field will report either **Present** or **Not Present**. If Closed Captions are reported as **Not Present**, the possible reasons are:
  - If the caption source is EIA-608 Line 21, it means that the decoder cannot find a valid closed caption waveform on that line.
  - If the caption source is SMPTE-334 VANC, it means that the decoder is either not receiving closed caption messages, or it is receiving EIA-708 messages without a caption field.

Note that it is possible for the decoder to be receiving closed caption data that is empty (without actual captions). These will be reported as **Present**.
- AFD:** This reports AFD insertion. This field will report either **Not Present** (if no AFD is being received) or **Code XXXX**, if AFD is being received; XXXX is the current AFD code being inserted. If AFD Source is set to Manual AFD Selection, this field will report the selected manual code.
- HDR Metadata:** This field will report either **Present** or **Not Present**, depending on whether or not HDR metadata is being detected in the video signal.
- SMPTE-2038:** This 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:** This indicates the count of SMPTE-2038 ANC packets inserted.
- SCTE-104 Inserted:** This indicates the count of SMPTE-104 ANC packets inserted.
- SCTE-35 Errors:** This indicates the number of invalid SCTE-35 messages.

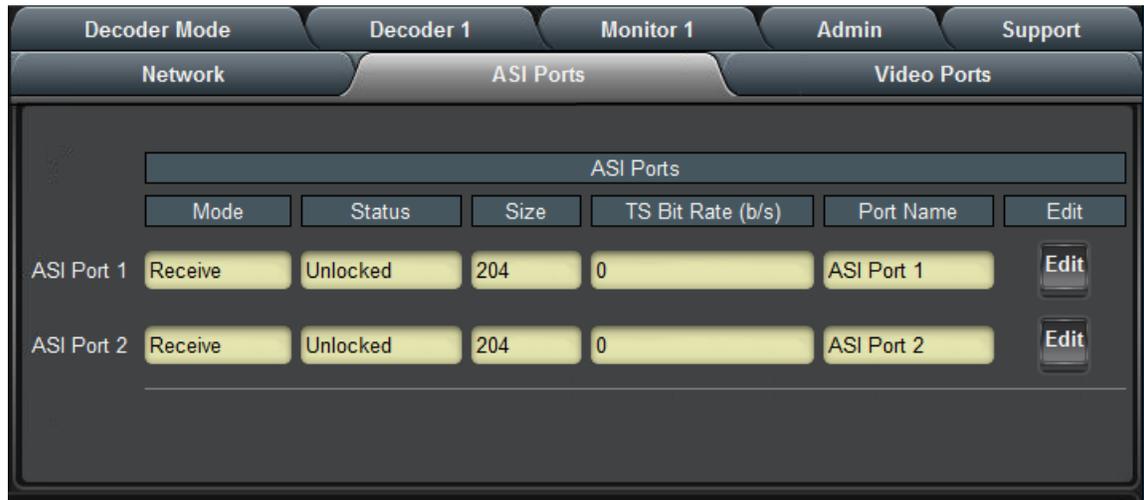
---

## ASI Ports Tab

The 9992-DEC card has two ASI ports that can be independently configured. Use this tab to configure and manage the ASI ports.

### ASI Ports-Configuration Tab

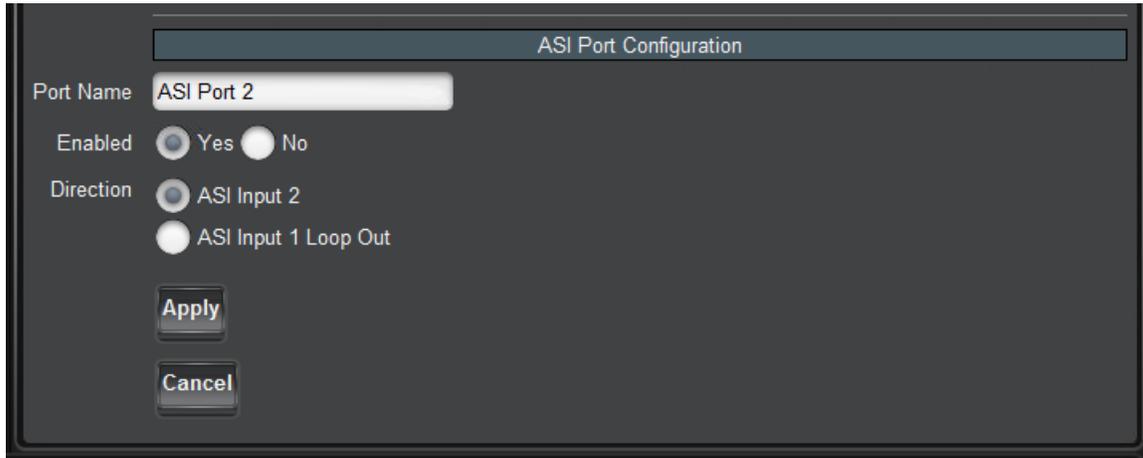
The default appearance of the Configuration tab is:



The **ASI Ports** table contains the current configuration of the ports, as follows:

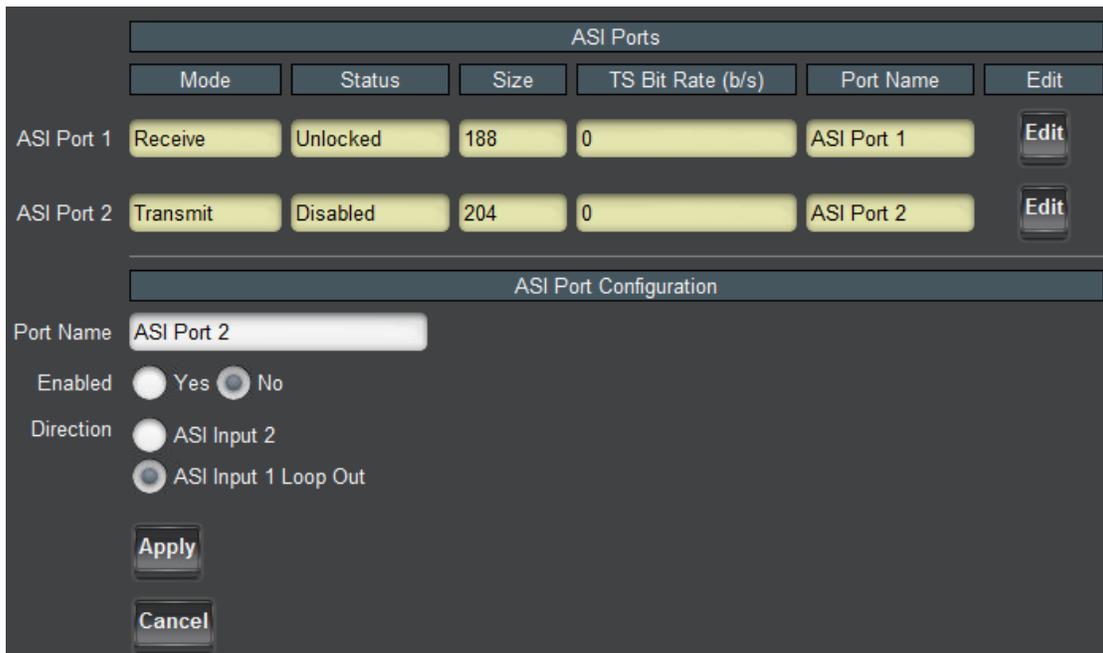
- **Mode:** This indicates the mode of the ports. ASI Port 1 is receive only. ASI Port 2 can be receive or transmit, depending on configuration.
- **Status:** Indicates the port status. It can contain the following values:
  - **OK:** Port is operating normally.
  - **Unlocked:** Port is unlocked. This means that the port is in Automatic Bit Rate mode and it has no input.
  - **Overflow:** Transmit overflow. This means that the ASI Output is in Manual mode, and the configured bit rate is insufficient to carry the bitstreams connected to it. This situation will raise an alarm as packets are being dropped.
- **Size:** Indicates the configured transport packet size, in bytes.
- **TS Bit Rate (b/s):** This reports the actual transport stream bit rate, in bits/second.
- **Port Name:** This reports the user-configured Port Name.
- **Edit Button:** Clicking on this button allows configuration of the port. The ASI Port Configuration screen appears, with the settings for the selected port.

To configure an individual port, click on the **Edit** button for that port. The following configuration interface opens:



The ASI Port Configuration Parameters are:

- **Port Name:** All 9992-DEC ports 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:** Select **Yes** or **No**.
- **Direction:** Select **ASI Input 2** or **ASI Input 1 Loop Out**. If you select to loop out that port will transmit that stream, as shown in the mode of ASI Port 2. This control is only available for ASI Port 2.

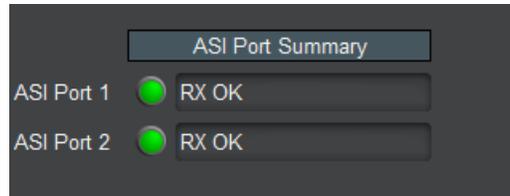


Once the port is configured, click on the **Apply** button, and the configuration takes effect.

---

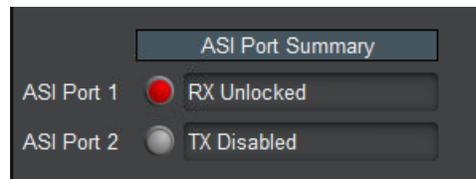
## ASI Ports - Statistics Tab

The Statistics Tab for the ASI Ports provides a quick visual summary status for the ports. A sample, corresponding to the table example of the previous section, is depicted below.



Each of the ASI Port indicators can have the following values:

- **RX OK:** The port is operating normally in receive mode (ASI Input).
- **TX OK:** The port is operating normally in transmit mode (ASI Loop Out).



- **RX Overflow:** The connected received bit rate is excessive.
- **TX Overflow:** 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 reduce the connected bit rate, or increase the ASI input bit rate, or configure the port in Automatic mode. **If this alarm is active, data is being dropped.**
- **RX Unlocked:** The port not locked to any signal.
- **TX Unlocked:** The port is in automatic bit rate, and there is no data rate coming to it. Any downstream ASI receivers will lose lock. Dashboard™ Card State and the Status LED will be red if there is a connection to this port.
- **RX Disabled:** The port is disabled.
- **TX Disabled:** The port is disabled.

---

## Monitor Tab

The 9992-DEC 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.

The Monitoring function of the 9992-DEC 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

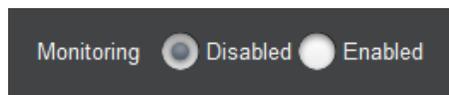
The Monitoring Configuration Tab is divided into two sub-tabs:



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

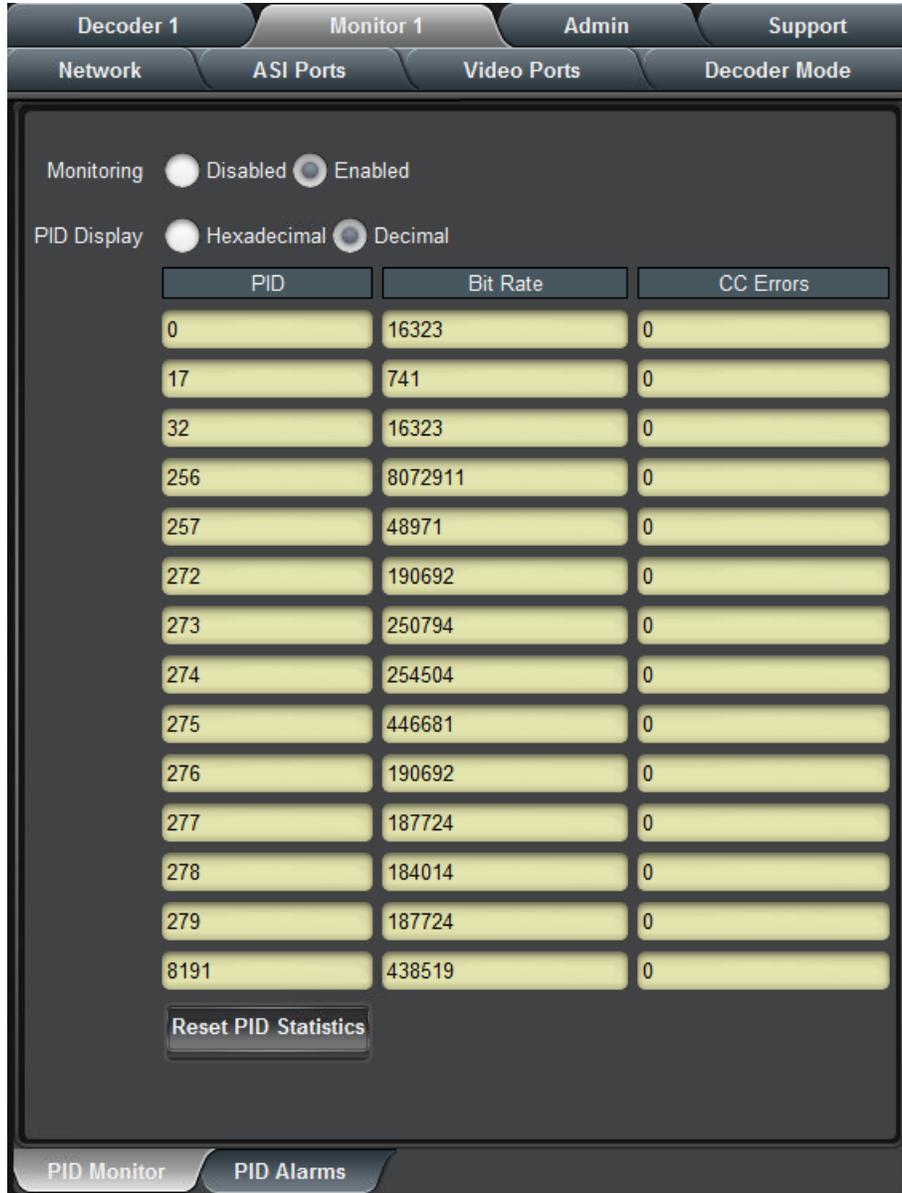
### PID Monitor Configuration Tab

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.



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.

---

## Monitor Configuration- PID Alarms 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
0	10	<input checked="" type="checkbox"/>	0	OK
17	10	<input checked="" type="checkbox"/>	1	OK
32	10	<input type="checkbox"/>	0	Off
256	10	<input type="checkbox"/>	0	Off
257	10	<input checked="" type="checkbox"/>	0	OK
272	10	<input type="checkbox"/>	0	Off
273	10	<input type="checkbox"/>	0	Off
274	10	<input checked="" type="checkbox"/>	0	OK

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.

## Monitor Statistics Tab

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



## Monitor Statistics - PID Monitor Tab – PID Alarms

The PID Statistics tab is shown below once you select **Enable** from the Monitoring button in the configuration section.

The left screenshot shows the 'Monitoring Enabled' status and a table of PID statistics:

PID	Bit Rate	CC Errors
0	16323	0
17	741	0
32	16323	0
256	8072911	0
257	48971	0
272	190692	0
273	250794	0
274	254504	0
275	446681	0
276	190692	0
277	187724	0
278	184014	0
279	187724	0
8191	438519	0

The right screenshot shows the 'PID Alarms' configuration table:

PID	Trigger (s)	Enable	Elapsed (s)	Alarm
0	10	Enabled	0	<input checked="" type="radio"/> OK
17	10	Enabled	1	<input checked="" type="radio"/> OK
32	10	Disabled	0	<input type="radio"/> Off
256	10	Disabled	0	<input type="radio"/> Off
257	10	Enabled	0	<input checked="" type="radio"/> OK
272	10	Disabled	0	<input type="radio"/> Off
273	10	Disabled	0	<input type="radio"/> Off
274	10	Enabled	0	<input checked="" type="radio"/> OK

---

## Admin Tab

The Admin tab contains several general administrative functions, each on its own tab shown below.



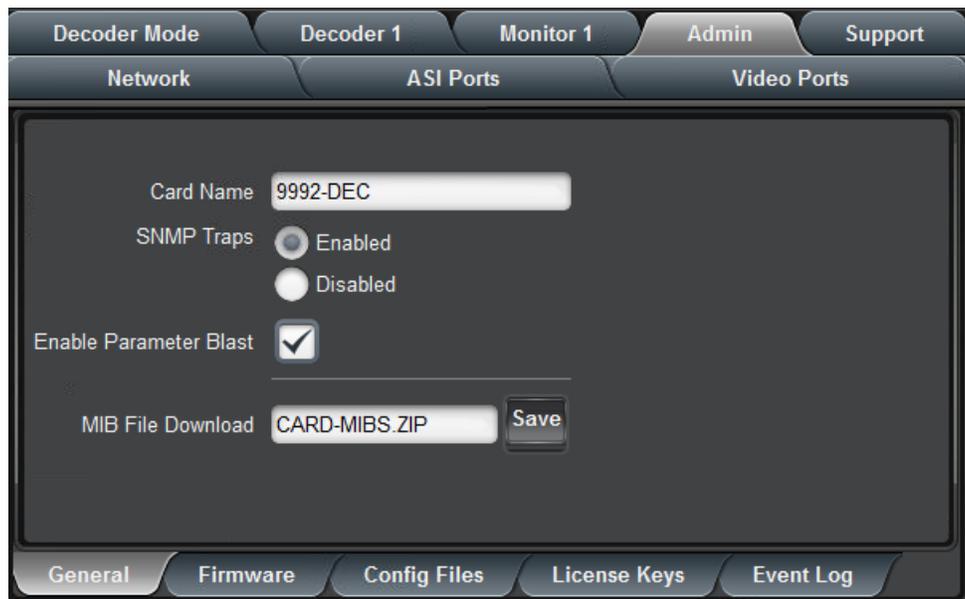
The Admin tabs are:

- **General:** Manages a number of general card parameters; provides an SNMP MIB download.
- **Firmware:** Manages firmware images.
- **Config Files:** The 9992-DEC has the ability to store multiple configurations. These are managed in this tab.
- **License Keys:** Contains the current licensing state of the 9992-DEC, and allows new license keys to be entered.
- **Event Log:** The 9992-DEC 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.

### ***Admin General Configuration Tab***

The Admin General Tab is depicted below:



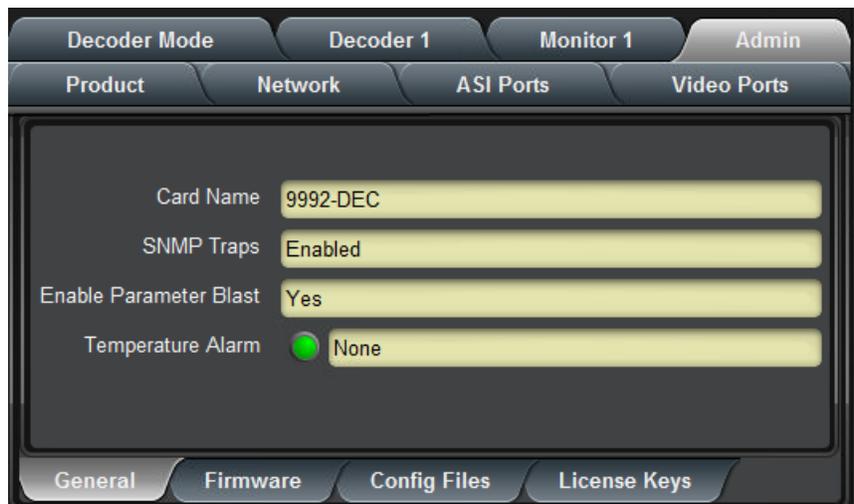
The Admin General Tab includes the following parameters:

- **Card Name:** This field defaults to “9992-DEC” but can be set to any descriptive name. The name provided here also appears in the Dashboard™ Tree View.

- **SNMP Traps:** This allows SNMP traps to be enabled or disabled<sup>6</sup>. You must click the **Reboot** button for the changes to take effect (image shown below).
- **Enable Parameter Blast:** This feature that speeds up DashBoard startup over high-latency links (i.e., when the computer running DashBoard has a WAN connection to the decoder or the frame housing the decoder). This feature requires DashBoard version 8.2 or later.
- **MIB File Download:** The 9992-DEC 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.

### Admin General Statistics Tab

The Admin General Statistics Tab is shown below. It shows the current configuration for the **Card Name**, **SNMP Traps** and **Enable Parameter Blast** controls.



This tab also includes one additional item, **Temperature Alarm**, which shows the current state of the 9992-DEC thermal protection system. The possible values are:

- **None:** There is no temperature alarm and the 9992-DEC is operating normally.
- **Chassis Door Open:** The 9992-DEC has detected that the chassis door is open. The ventilation fans are built into the chassis door; opening the door disengages the fans and cuts the airflow. While the 9992-DEC can operate for short periods of time without this airflow, such operation is not guaranteed over long periods of time (more than a few minutes). The 9992-DEC will remain in yellow alarm for as long as the chassis door is open. Depending on the chassis loading and ambient temperature, operating with the door open for more than a few minutes can cause the 9992-DEC to overheat and shut down.
- **FPGA Temperature Warning:** The 9992-DEC has detected that its internal temperature has exceeded 70°C. The exact value can be found in the Product Statistics

<sup>6</sup> SNMP is an optional feature in the openGear™ frame controller. The 9992-DEC SNMP functions are only available if SNMP is licensed in the frame controller.

---

Tab. While the 9992-DEC can operate indefinitely in this condition without any damage, it is recommended that the situation be corrected as the thermal operation margin is reduced.

- **FPGA Temperature Critical:** The 9992-DEC has detected that its internal temperature has exceeded 80°C. The exact value can be found in the Product Statistics Tab. While the 9992-ENC can operate indefinitely in this condition without any damage, the situation **MUST** be corrected immediately. If the internal temperature reaches 85°C, the 9992-DEC will **shut down** without any further notice to protect itself from damage. After a thermal shutdown, the 9992-DEC automatically starts again when the temperature is reduced to a safe operational value.

### **Admin Firmware Tab**

The 9992-DEC 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 fallback 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. Finally, the push buttons on the front of the card allow for a forced override to the factory image, as described in the Front Switches section.

### **Uploading a Firmware Upgrade**

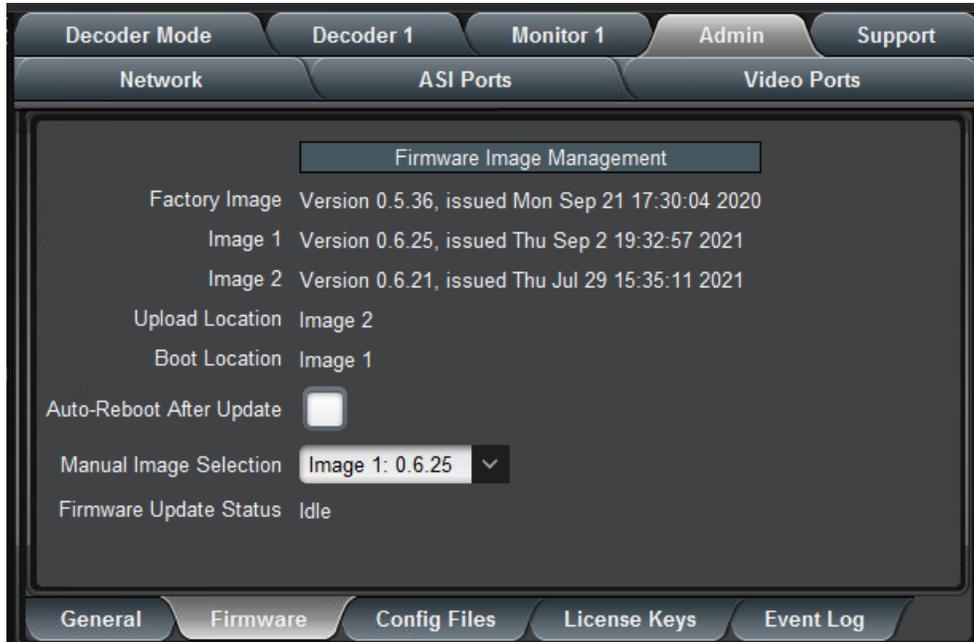
When applicable, Cobalt Digital Inc. provides for continual product enhancements through software updates. As such, functions described in this manual may pertain specifically to cards loaded with a particular software build. You can update your card by downloading the new Update software by going to the Support → Firmware link at [www.cobaltdigital.com](http://www.cobaltdigital.com). Download “Firmware Update Guide”, which provides simple instructions for downloading the latest firmware for your card onto your computer, and then downloading it to your card through DashBoard™. When you have the firmware upgrade file placed, in the desired location, on your computer click on the **Upload** button at the bottom of the user interface.



**Click here to start firmware update**

A classic dialog box allows you to browse your computer to select the upgrade file. You can simultaneously upgrade all of your 9992-DEC cards over multiple chassis as well. Uploading firmware to the 9992-DEC does not affect its operation in any way and does not introduce any glitches in the inputs/outputs.

**Note:** To allow for a controlled transition to operation when upgrading firmware, reboot the card to engage the new firmware. The card will go off-line while rebooting.



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 valid image is present, this field will indicate **No Image**.
- **Upload Location:** This field contains the location where the image upload will go. The 9992-DEC 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 9992-DEC will automatically reboot after a successful firmware upload through Dashboard. By default, the 9992-DEC will **not** reboot after an update. You can upload the firmware at any time, and reboot later during a maintenance window.
- **Manual Image Selection:** Select one of the previously uploaded images from the drop-down list and click the **Reboot** button to make the changes.
- **Firmware Update Status:** This describes the status of the Firmware running on the encoder.

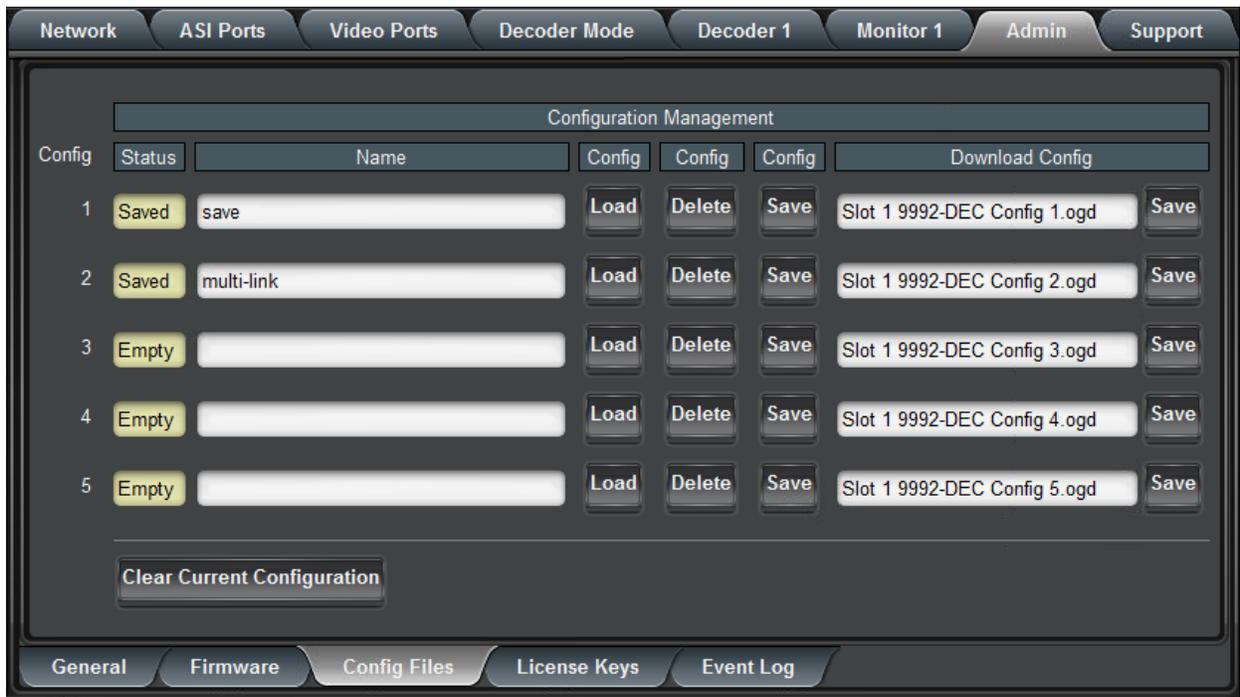
### ***Admin Config Files Tab***

As you make configuration changes to the 9992-DEC, they are automatically persisted in non-volatile storage. If you reboot or power-cycle the card, it will come back in the same configuration.

In addition to automatic configuration persistency, the 9992-DEC also offers the ability to save up to five 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.

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



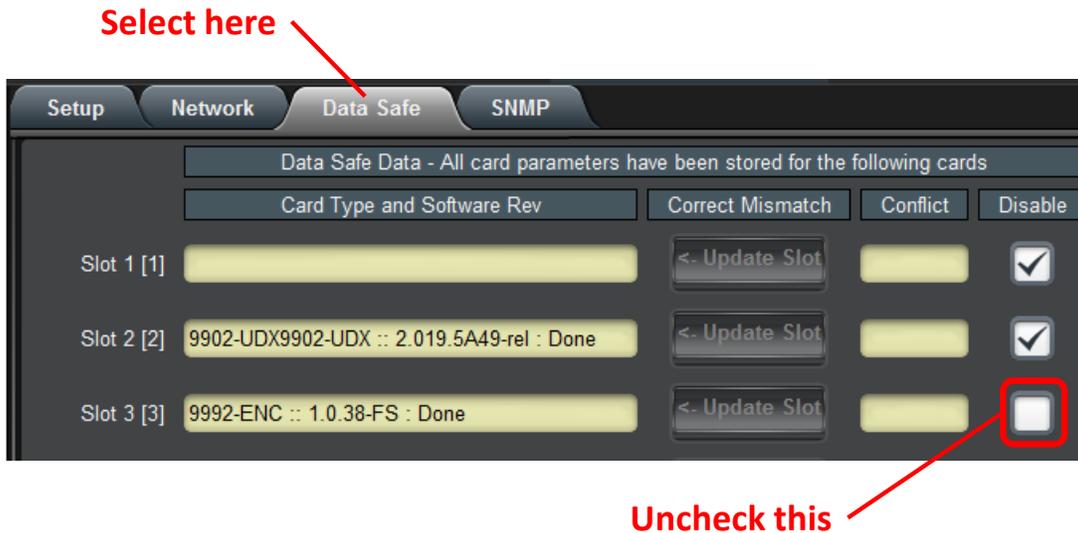
## User-Saved Configurations

The fields in the user-saved configuration are:

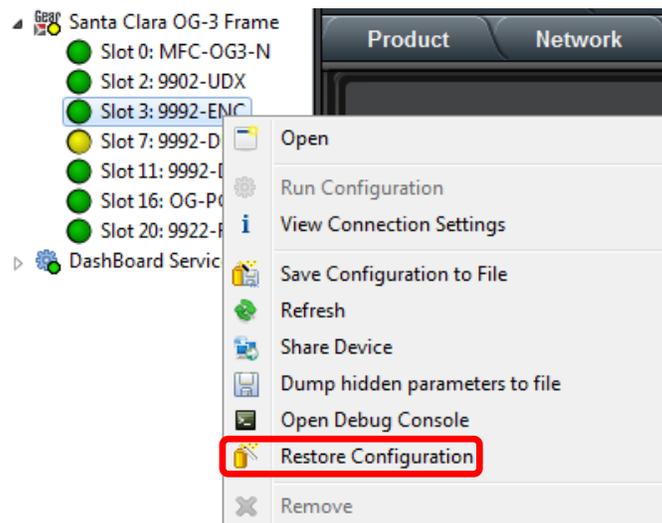
- **Status:** This indicates whether there is a saved configuration on that particular slot. It will contain the words **Saved** or **Empty**.
- **Name:** This is an optional name for the configuration. It is not required but highly advisable. The name can be edited at any time (even when there is no saved configuration).
- **Config Load Button:** Click on this button and the corresponding configuration is loaded on the 9992-DEC 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 9992-DEC 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 9992-DEC, use the following procedure:

1. On Dashboard™, open the user interface for the frame controller (slot 0).
2. Select the **Data Safe** tab in the configuration area.
3. Uncheck the **Disable** checkbox corresponding to the card you wish to restore the configuration. This step is depicted below.



4. 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 – **Restoring Configurations to Devices**.

---

## Clear Current Configuration Button

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

- All ASI Ports are set to manual configuration, 20 Mb/s, 188-byte packets.
- All Decoders are stopped and configured with a default set of parameters.
- All Video ports are deleted.
- All Connections are removed.

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 9992-DEC is virtually instantaneous. The Status Message Area will indicate the result of the operation.

## Admin License Keys Tab

The 9992-DEC 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 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. It is simply the sum of the permanent and temporary licenses.
- **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”.



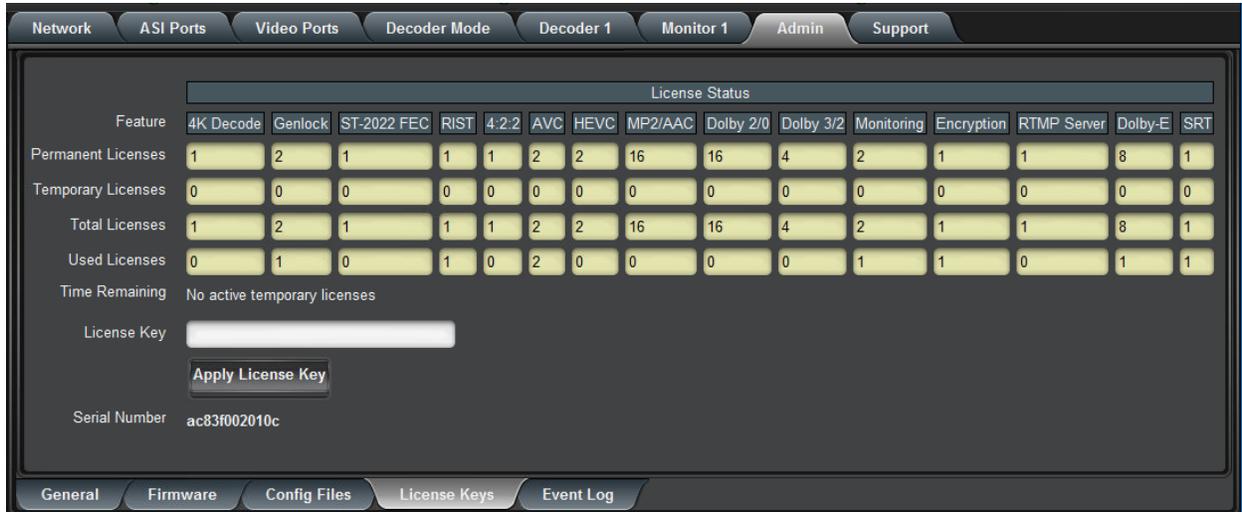
The table columns correspond to the licensable features, as follows:

- **4K Decode:** This enables 4K decoding for the board. If you have the 9992-DEC-4K-HEVC model, this license was pre-installed in the factory.
- **SMPTE 2022 FEC:** This enables FEC for the board. This is not a counted feature; if FEC is enabled, the corresponding number is 1; if it is disabled, the corresponding

---

number is 0. The Used Licenses field will be set to 1 if there is at least one FEC instance in use.

- **RIST:** This enables RIST for the board. This is not a counted feature; if RIST is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one RIST instance in use.
- **4:2:2:** This enables 4:2:2 decoder for the board. This is not a counted feature; if 4:2:2 is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one 4:2:2 instance in use.
- **AVC:** This is the maximum number of AVC/MPEG-2 decode instances licensed for the board. If you have the 9992-DEC-4K-HEVC model, one instances of this license was pre-installed in the factory.
- **HEVC:** This is the maximum number of HEVC decode instances licensed for the board. If you have the 9992-DEC-4K-HEVC model, two instances of this license were pre-installed in the factory.
- **MP2/AAC:** This is the maximum number of combined MPEG-1 Layer II and AAC decode sessions licensed for this board. Each AVC or HEVC license comes with 2 decode sessions. An AAC 5.1 surround decode session requires 3 licenses.
- **Dolby 2/0:** This is the maximum number of Dolby stereo decoding sessions licensed for this board. Each license can be used either for AC-3 stereo or EAC-3 stereo.
- **Dolby 3/2:** This is the maximum number of Dolby 5.1 surround sessions licensed for this board. Each license can be used either for AC-3 or EAC-3. Surround licenses can also be used for Dolby 2/0 stereo operation.
- **Monitoring:** This
- **Encryption:** This enables RIST Main Profile Encryption and Authentication for the board. This is not a counted feature; if encryption is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one encryption instance in use.
- **RTMP Server:** This is the maximum number of RTMP server instances licensed on this board.
- **Dolby-E:** This is the maximum number of Dolby-E decode services licensed on this board.
- **SRT:** This enables SRT for the board. This is not a counted feature; if SRT is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one SRT instance in use.



To request a license key from Cobalt, 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 us, 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:** 9992-DEC license keys are specific to a card. You entered a valid license key, but it is intended for a different card, whose serial number is displayed in the message. You must use this key on the correct card.
- **This key has already been applied:** License keys can only be applied once. This is a valid key for this card, but you have already applied it, and its features are already available.

## Admin Event Log Tab

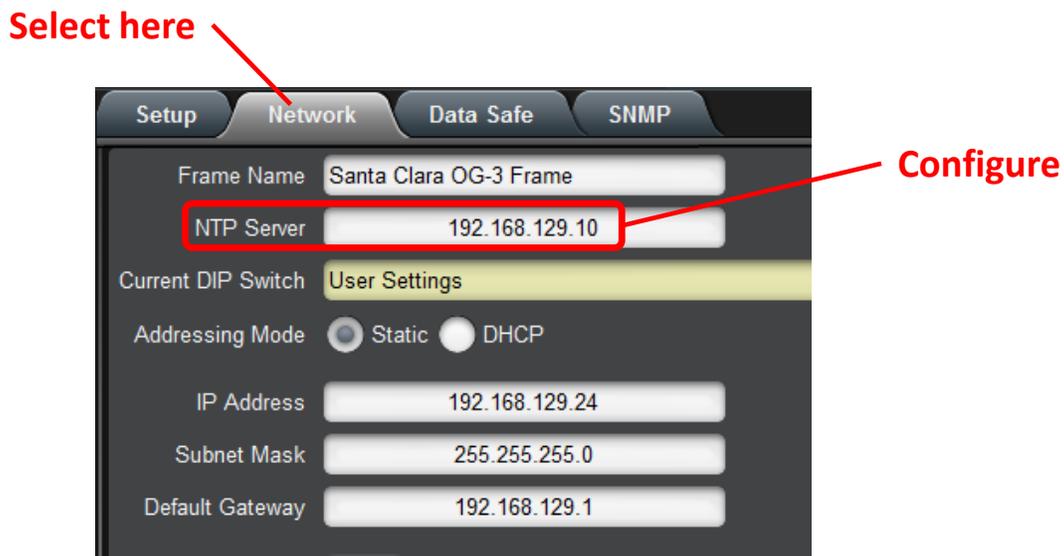
The 9992-DEC includes an Event Log in non-volatile storage. This event log can be used for faultfinding and to check for error conditions. The following information is included in each 9992-DEC event in the log:

- **Date:** The calendar date in which the event occurred.
- **Time:** The time at which the event occurred.
- **Severity:** The severity of the event. The 9992-DEC defines three severity levels:
  - **Error:** Any events that affect the operation of the device. For example, an ASI Input losing lock or an IP Input no longer receives packets. An error will impact service until addressed.

- **Warning:** Any events that may produce visible glitches, but they do not have a continuous service impact. Examples of warnings are automatic redundancy switches and ARP renewal failures.
- **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.

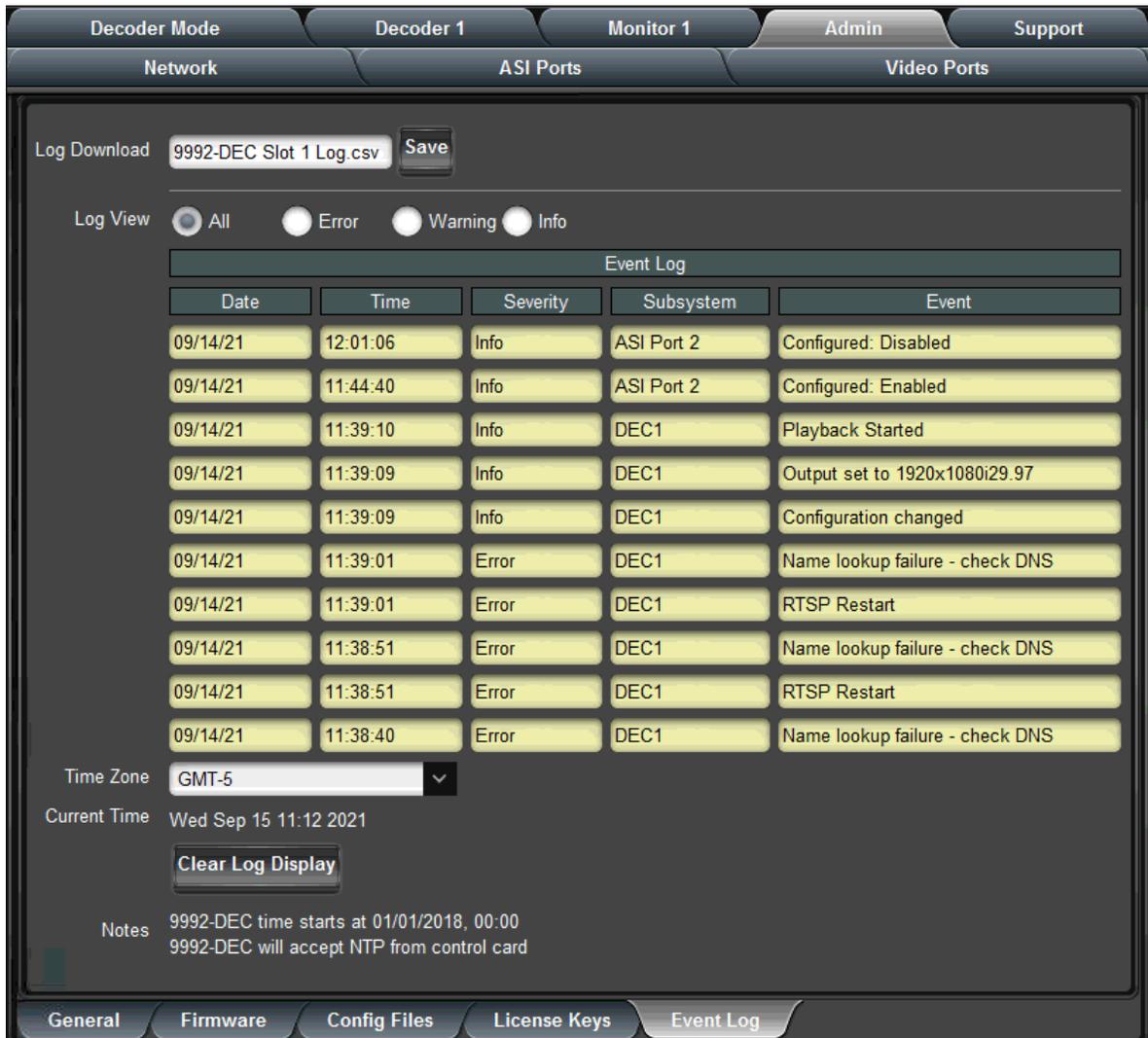
The 9992-DEC does not have a battery-backed real-time clock. It depends on the frame controller to obtain the current date and time, and the frame controller depends on an external Network Time Protocol (NTP) server to obtain current date and time. By default, the 9992-DEC will initialize its internal time-of-day clock to January 1, 2018, GMT. If the frame controller is NTP-synchronized, the 9992-DEC will then accept time from it and set its time-of-day clock accordingly.

In order to configure the 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 frame controller 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 9992-DEC 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 9992-DEC 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 9992-DEC 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.

---

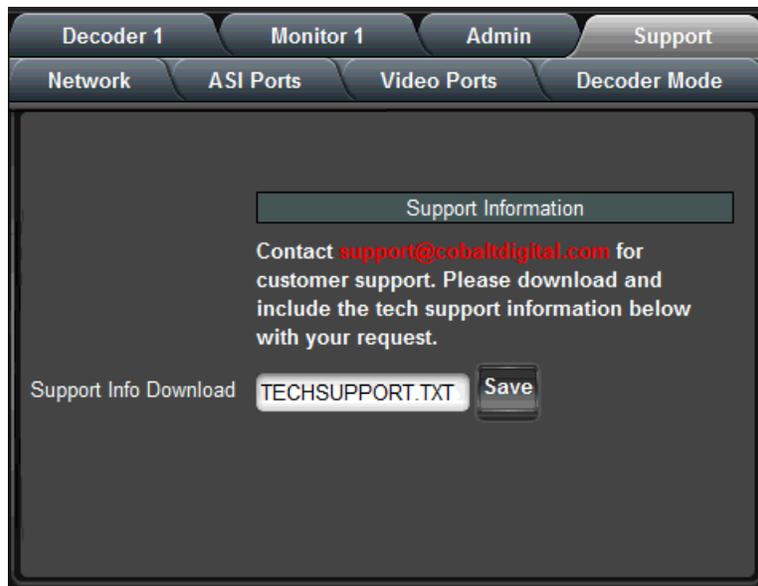
## Support Tab

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](mailto: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 decoder. This includes the make and model of any connected devices being used, as well as the connection network (IP or ASI) between the decoder 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.

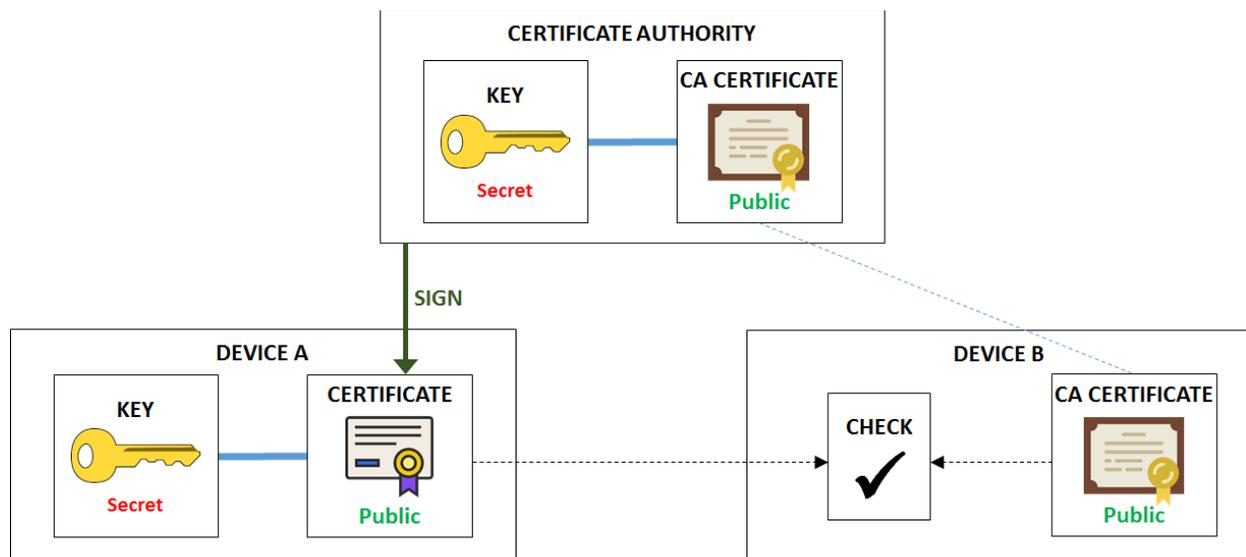


Figure 1: Certificate Checking

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](http://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.

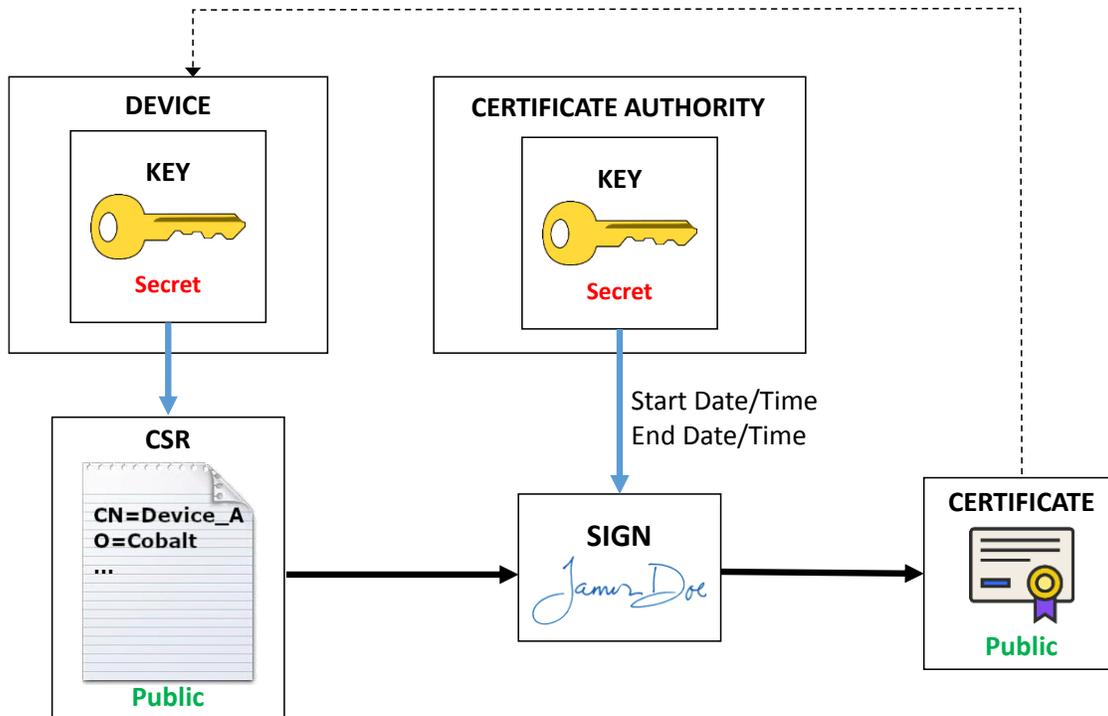


Figure 2: Certificate Signing Process

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 9992-DEC decoder can support two simultaneous decoding sessions, it can support up to 2 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.

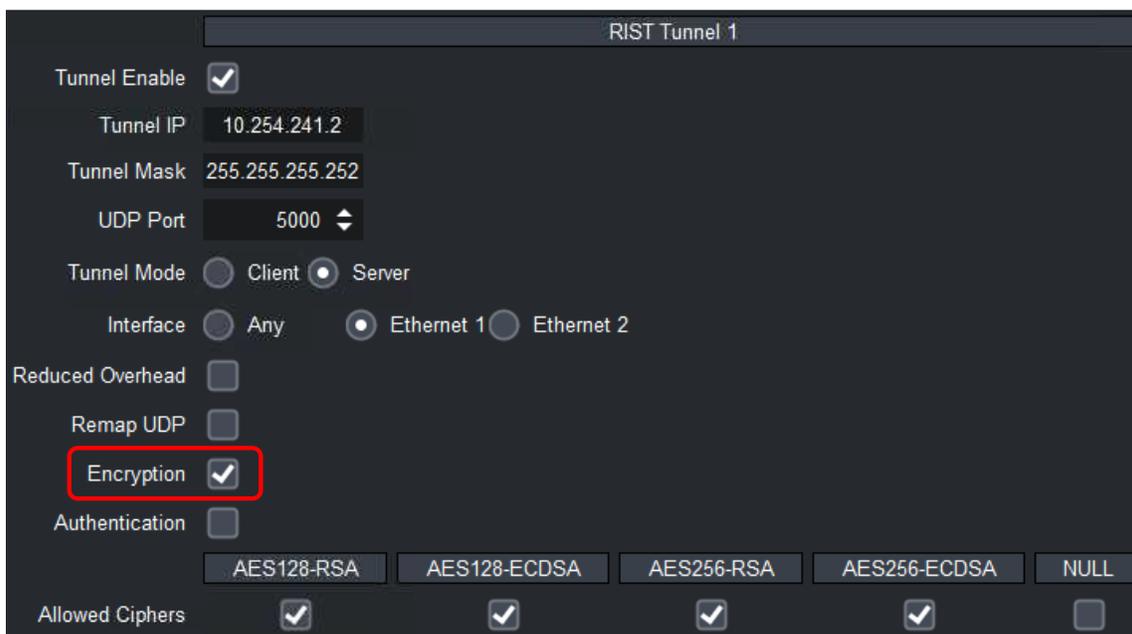


Figure 3: Configuring Encryption

---

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.

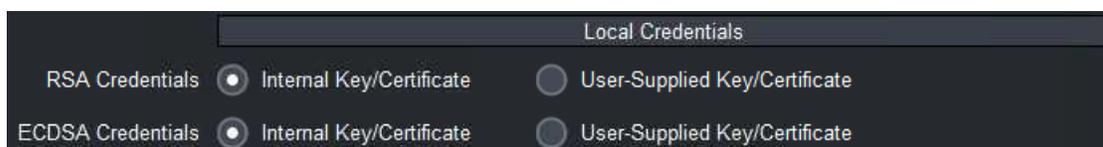


Figure 5: Configuring the Local Credentials

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:	<input checked="" type="radio"/> RSA <input type="radio"/> ECDSA
Country:	<input type="text" value="US"/>
State:	<input type="text" value="IL"/>
Locality:	<input type="text" value="Champaign"/>
Organization:	<input type="text" value="Cobalt Digital"/>
Organizational Unit:	<input type="text" value="Compression Division"/>
Common Name:	<input type="text" value="Device"/>
<input type="button" value="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.

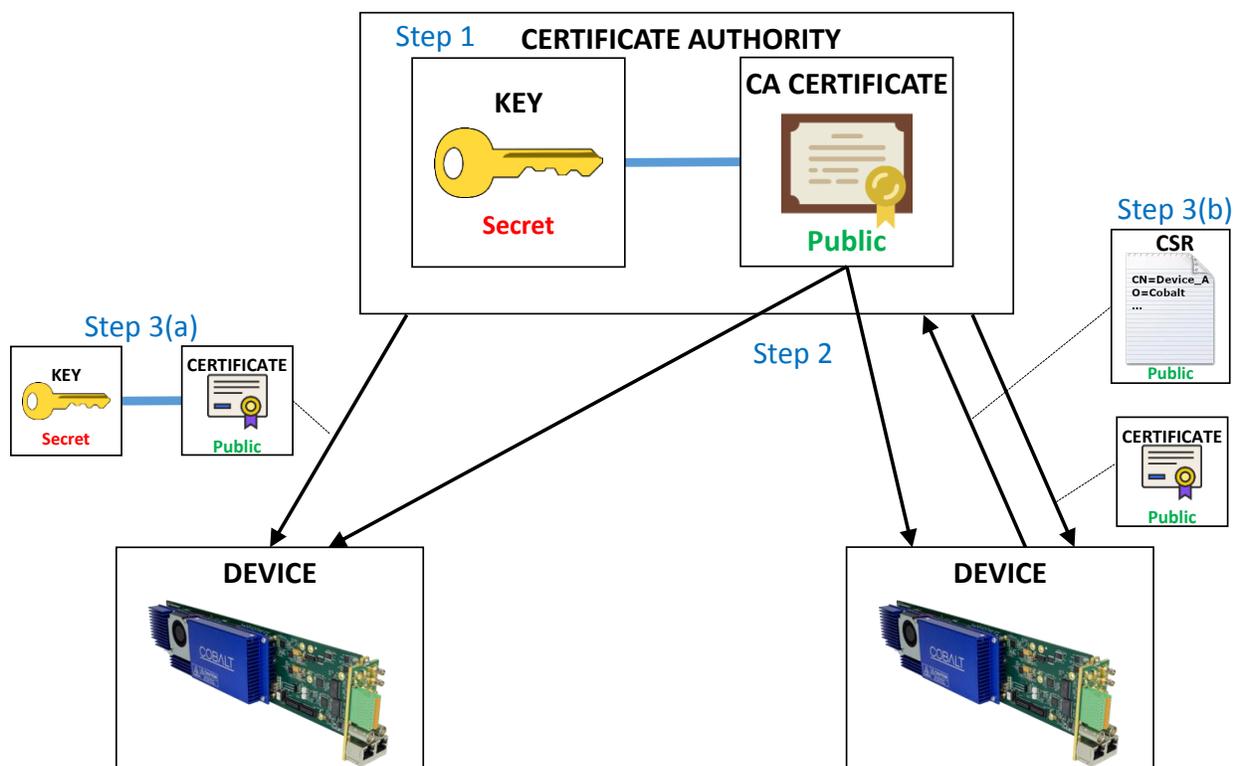


Figure 8: Using an external Certificate Authority

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.

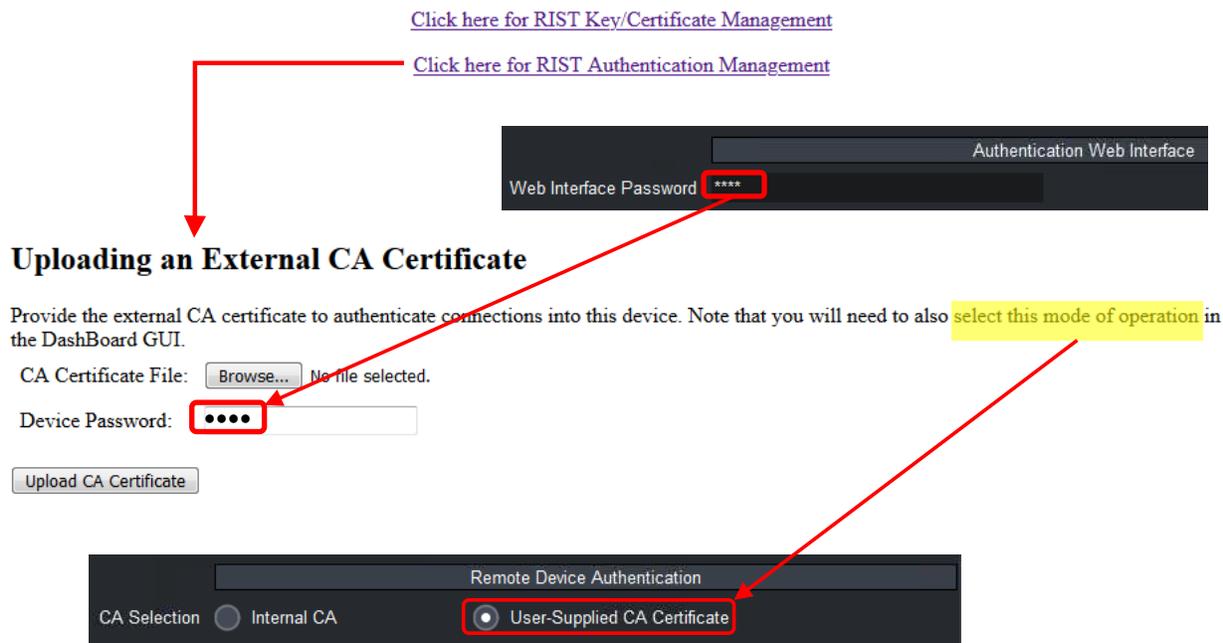


Figure 9: Uploading an External CA Certificate

## 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.

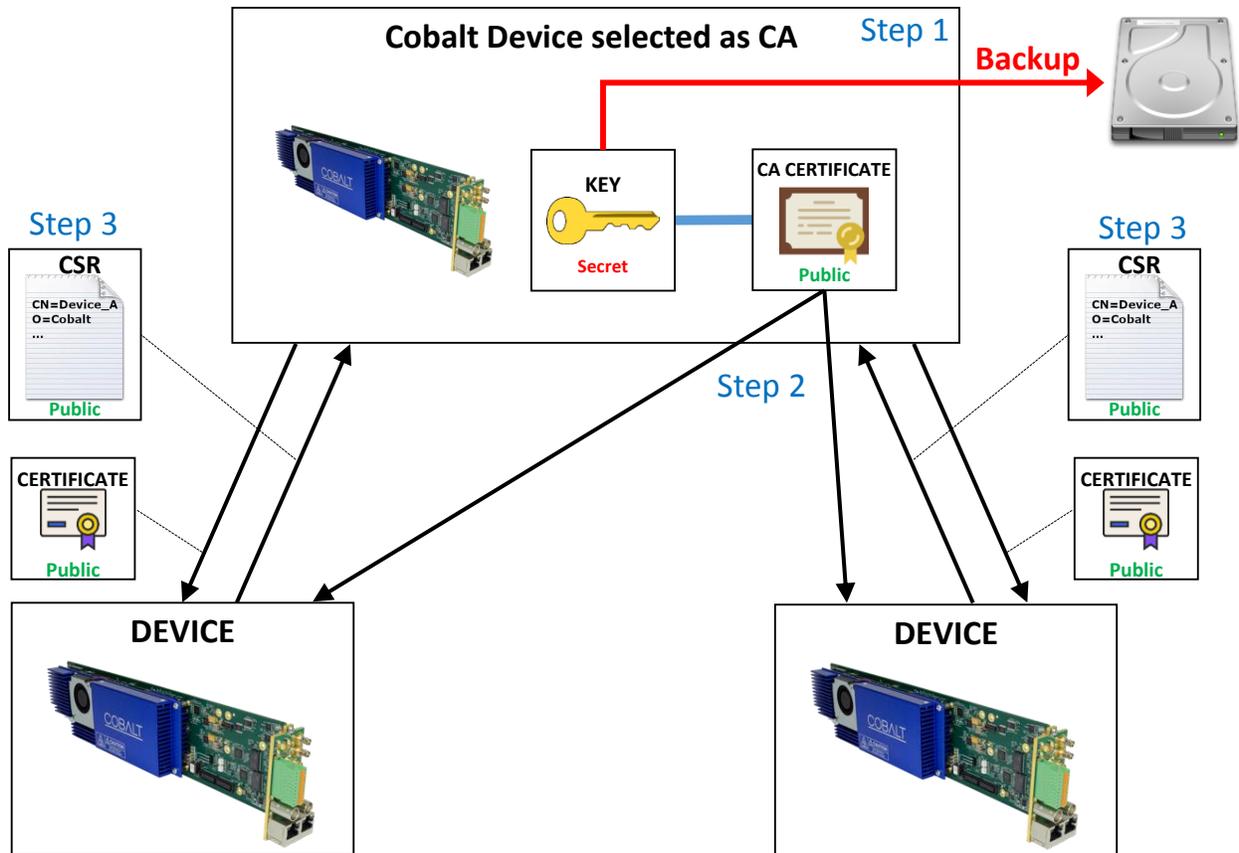


Figure 10: Using a Cobalt Device as the CA

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.

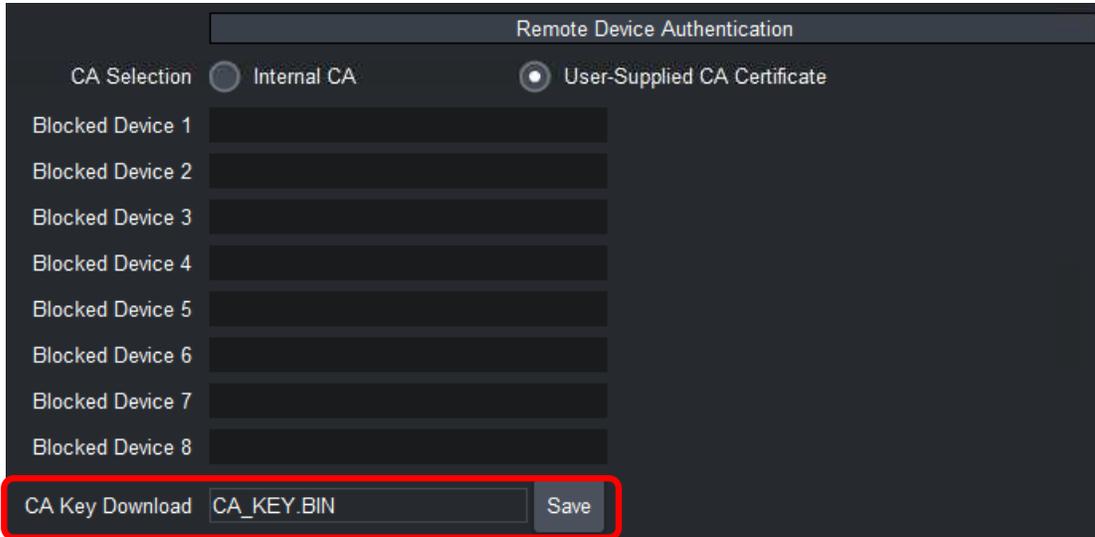


Figure 11: Downloading the device's internal CA key

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.

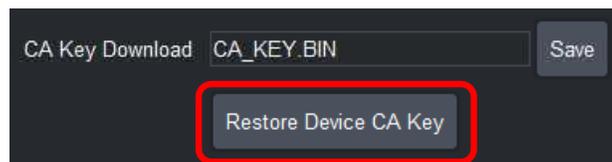
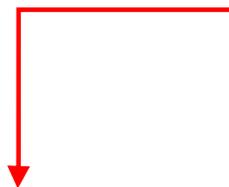


Figure 12: Restoring the original CA key

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”.

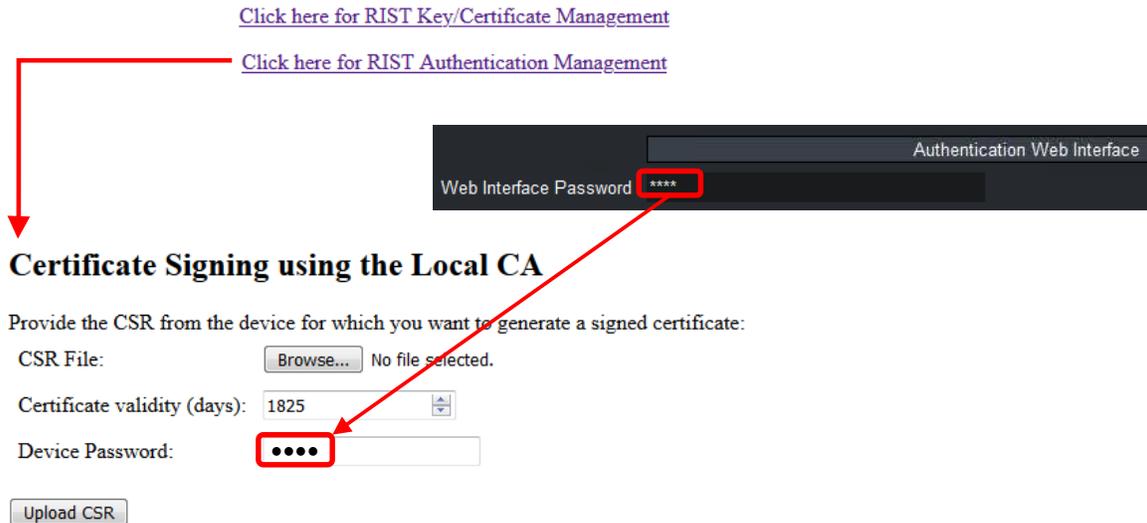


Figure 14: Signing a Certificate

### 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.

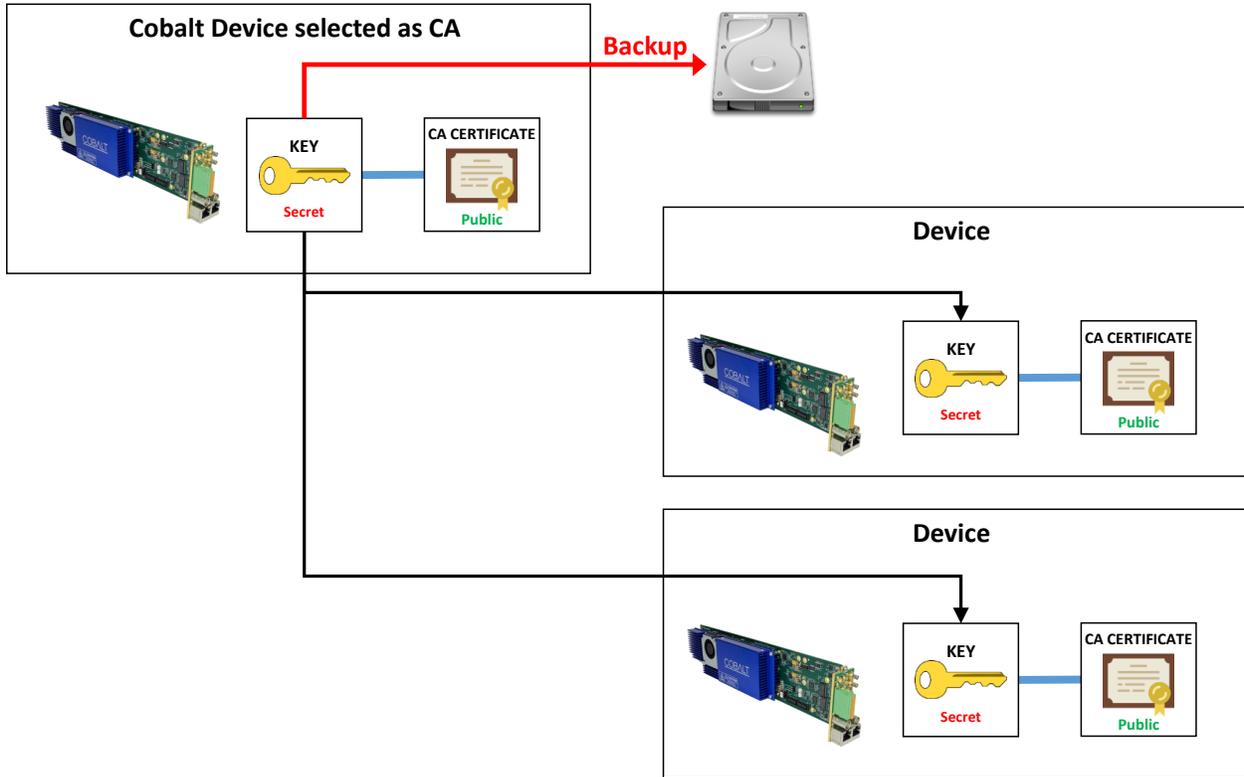


Figure 15: Copying the CA Key to all devices

## 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.

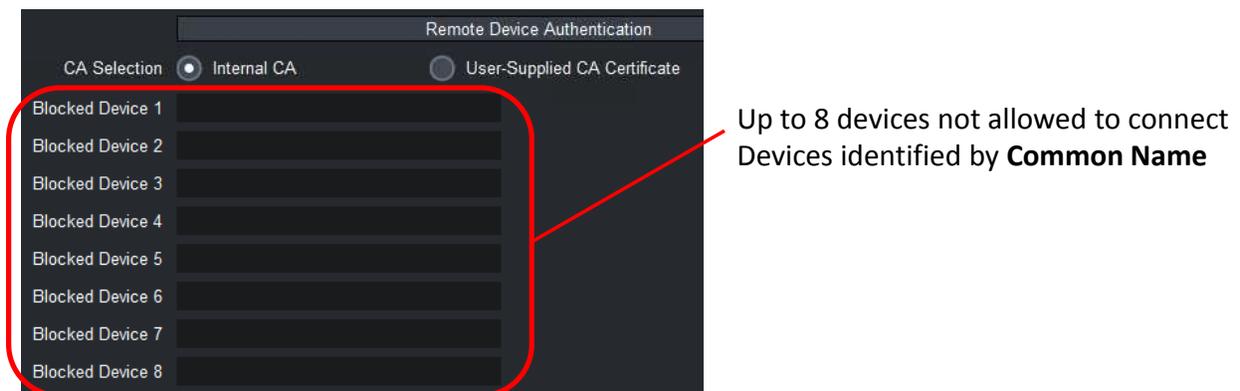


Figure 16: Blocked Device List

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, **9992-ENC\_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.

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		

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”.