VIAVI

EASyCAP Encoder/Decoder 24.08

Emergency Management System

User's Guide

Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and VIAVI reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright/Trademarks

© Copyright 2024 VIAVI Solutions Inc. All rights reserved. No part of this guide may be reproduced or transmitted, electronically or otherwise, without written permission of the publisher. VIAVI Solutions and the VIAVI logo are trademarks of VIAVI Solutions Inc. ("Viavi"). All other trademarks and registered trademarks are the property of their respective owners.

Copyright release

Reproduction and distribution of this guide is authorized for US Government purposes only.

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to VIAVI standard terms and conditions, available at **www.viavisolutions.com/en/terms-and-conditions**.

Table of Contents

Chapter 4 53

Configuration 53

Chapter 1
General Information

Introduction

The VIAVI EASyCAP® (Model EASyCAP-1) EAS (Emergency Alert System) Encoder/Decoder is a 2U rack mounted control center capable of performing manual or automated EAS messaging for Cable, Broadcast, IPTV, and Wire line systems and is in accordance with CFR 47 part 11 FCC regulations.

The EASyCAP® Encoder/Decoder receives EAS messages from up to six audio sources (internal or external), decodes the FSK (Frequency-shift Keying) EAS message, and operates the target system equipment to replay the message for viewers/listeners. In addition, messages can be originated by the user via local or remote control of the EASyCAP®. The EAS Audio sources for the EASyCAP® include internal AM/FM/NOAA radios and external audio inputs that can be connected to any known EAS audio source.

EAS Audio is decoded by the internal AFSK circuitry, then sorted and interpreted to determine the type of emergency or test, locations for which the emergency applies, and other information supplied in the EAS Header. If a voice message is contained in the EAS message, it is recorded for possible playback to subscribers. EAS messages then pass through a series of tests to determine if the message matches predefined, user configurable parameters. If these tests pass, EAS activation (message playback) to the system occurs. To play an EAS message to viewers/listeners, the EASyCAP® activates TTLs, Contact Closures, RS-485 data commands, RS-232 data commands, and several IP based protocols, it also supplies pertinent video and re-encodes/plays the EAS FSK and recorded audio. The TTLs, Contact Closures, and serial data commands, and IP protocols activate routing equipment and end-user devices to provide the emergency audio and video to all viewers/listeners.

In addition to the EAS messaging capabilities, the EASyCAP® records all received and transmitted messages in the internal log for later retrieval.

FCC Certification

The EASyCAP Encoder/Decoder is certified to comply with 47 CFR, Part 11 (FCC regulations) for EAS encoders and decoders, and is registered with the FCC under identification number: P4V-EASYCAP-1.

Pursuant to FCC 15.21 of the FCC rules, changes not expressly approved by VIAVI might cause harmful interference and void the FCC authorization to operate this product.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

California Proposition 65

California Proposition 65, officially known as the Safe Drinking Water and Toxic Enforcement Act of 1986, was enacted in November 1986 with the aim of protecting individuals in the state of California and the state's drinking water and environment from excessive exposure to chemicals known to the state to cause cancer, birth defects or other reproductive harm.

For the VIAVI position statement on the use of Proposition 65 chemicals in VIAVI products, see the Hazardous Substance Control section of VIAVI's Standards and Policies web page.

Unpacking and Inspection

When the EASyCAP Encoder/Decoder arrives, immediately inspect the shipping container and contents for visible damage. Keep all packing materials until the equipment's intended performance characteristics have been verified. If any of the equipment is damaged or fails to operate properly due to transportation damage, immediately file a claim with the transportation company or, if insured separately, with the insurance company.

Each EASyCAP Encoder/Decoder will arrive in its own shipping container. The container will, at a minimum, include the following: EASyCAP Encoder/Decoder and AC Power Cord.

Claims for Damage in Shipment

Claims for shipping damage should be directed to the shipping and/or freight delivery service. Claims should be made within 7 days to insure prompt handling of the claim.

Ordering Information

For additional information about our products and services, contact your local VIAVI representative or visit **https://www.viavisolutions.com/en-us/how-buy**.

Where to Get Technical Support

Phone US: +1-844-GO-VIAVI or +1-844-468-4284

Outside US: +1-855-275-5378

Email: **Trilithic.EASySupport@viavisolutions.com**

Website: **https://support.viavisolutions.com/welcome**

Before any VIAVI EAS Encoder/Decoder can be returned for repair, VIAVI will issue a return material authorization (RMA) number. **No returned equipment will be accepted which does not have an RMA number prominently displayed on the outside shipping carton and on the shipping label**. A complete and full description, in writing, regarding the service issues with the equipment must be supplied inside the shipping container with each piece of equipment for which an RMA number has been issued.

> **NOTE**
> *Hardware or software modifications and changes may occur at any time during production, shipping, and/or during the equipment's life span. These changes may occur or be implemented by VIAVI without prior written notice or warning.*

How this Manual is Organized

This manual is divided into the following chapters:

- Chapter 1, "General Information" provides contact information and describes how this operation manual is structured.

- Chapter 2, "IPTV Installation and Maintenance" includes instructions for installing and maintaining the EASyCAP® IPTV Encoder/Decoder hardware.

- Chapter 3, "Overview" gives an overview of the EASyCAP® Encoder/Decoder hardware and how it works.

- Chapter 4, "Configuration" describes the steps necessary to configure the EASyCAP® Encoder/Decoder.

- Chapter 5, "Appendix" describes the specifications and warranty of the EASyCAP® Encoder/Decoder.

Conventions Used in this Manual

This manual has several standard conventions for presenting information.

- Connections, menus, menu options, and user entered text and commands appear in **bold**.

- Section names, web, and e-mail addresses appear in *italics*.

NOTE

A __NOTE__ is information that will be of assistance to you related to the current step or procedure.

CAUTION

A __CAUTION__ alerts you to any condition that could cause a mechanical failure or potential loss of data.

WARNING

A __WARNING__ alerts you to any condition that could cause personal injury.

Security Recommendations

Where possible, EAS Participants should adhere to the security best practices recommendation for EAS participants contained in the Communications Security, Reliability and Interoperability Council (CSRIC) EAS Security Subcommittee report.

EASyCAP® Software/Firmware upgrades are available from EASySupport@viavisolutions.com. VIAVI recommends checking for upgrades at least every six (6) months. If you become aware of security vulnerabilities for the Debian Linux operating system you should check for VIAVI EASyCAP® upgrades.

EASyCAP® upgrades are performed using the Web GUI by accessing the Administration/ Upgrade screen, which provides a means to upload and install the upgrade file. If the upgrade file has a .zip file extension it will also contain a readme text document providing important information or special instructions for the upgrade.

While EASyCAP® Encoder/Decoders utilize an internal firewall, VIAVI strongly recommends the use of an external router and firewall for connections facing the internet. Alternatively an http proxy may be used. A three-tier architecture is recommended.

- If able to manage the EASyCAP® from an internal private network (LAN), the internet facing firewall should completely block incoming connections while allowing outbound connections on port 443.

- If management over the internet is required, use of Network Address Translation to port 443 for the Web GUI is highly recommended. The internet exposed port should be a non-standard port (not a well-known port) between 11000 and 65000, and should avoid ending in common port numbers such as 21, 22, 80, and 443.

  - Some web browsers or other security features will not allow https connections over a port other than 443. In such a configuration there is no choice but to use port 443 for incoming connections.

  - If possible, restrict incoming IP addresses to known address ranges for your organization.

- If there is no choice but to place the EASyCAP® directly on the Internet

  - The non-secure web server interface should be disabled. Turn on the option to use secure https access in the Configuration/Web Configuration settings.

  - Disable the "Allow SSH" checkbox in the network settings for the internet-facing interface.

  - If the web interface is not required for the internet-facing connection, disable the "Allow Web Server" checkbox in the network settings for the internet-facing interface.

- Where possible, the Internet facing Ethernet port should be avoided for management and system activation protocols.

Spanish Language Support

EASyCAP supports English and Spanish languages. Audio and video interfaces, message origination, and delivery recipients can be configured to use English and/or Spanish. The languages presented during message playback will be dependent on the availability of languages in the received message as well as user configuration.

1. Audio inputs used to receive EAS messages will always be considered English audio sources.

2. If a CAP message does not include a Spanish info block, the alert text will consist of the required FCC translation text in Spanish followed by the CAP text in English.

3. If Spanish audio is not present in the received message:

   • If text-to-speech (TTS) is enabled then Spanish TTS audio will be used.

   • If TTS is disabled then English audio will be used.

4. If English audio is not present in the received message:

   • If TTS is enabled then English TTS audio will be used.

   • If TTS is disabled then no voice message will be played.

5. Alert text must be limited to 1800 characters. If a video output or delivery recipient is configured to use English followed by Spanish text, and the text exceeds 1800 characters, Spanish text will not be included.

IPTV Installation and Maintenance

Installation Information

NOTE	*The EASyCAP® should be installed in restricted access areas, where only authorized personnel are allowed access.*

CAUTION	*To ensure proper cooling, leave at least 3 inches of space in front and in back of the EASyCAP® chassis."*

CAUTION	*The EASyCAP® Encoder/ Decoder should be installed in a rack that is properly grounded.*

CAUTION	*The EASyCAP® should be connected to external Surge Protection Devices (SPD) when connected to AC power.*

CAUTION	*For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.*

CAUTION	*This device contains components sensitive to electrostatic charges. Use ESD mitigative procedures, such as wearing a wrist-strap during installation and maintenance of this device*

⚠ WARNING

The intrabuilding port(s) of the equipment is suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding port(s) of the equipment must not be metallically connected to interfaces that connect to the Outside Plant (OSP) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

⚠ WARNING

The Telephone port is an intra-building port and considered a Type 2 port as described in GR-1089-CORE. As such, this port shall only be connected via a method that assures isolation from OSP cabling. Such methods of connection would be via a PBX, Optical Network Terminal, or similar isolation devices

Wiring Recommendations

- All audio connections, general purpose inputs, and general purpose outputs use shielded twisted pair with the shield grounded at both ends.

> ⚠️ **WARNING** *GR-1089-CORE compliance requires all intra-building audio, general purpose input, and general purpose output ports to use shielded intra-building twisted pair wiring with the shield grounded at both ends.*

> ⚠️ **WARNING** *The TTL output port is only intended for manufacturing use. GR-1089-CORE compliance requires that this port be unconnected.*

- All Ethernet connections use shielded Category 6 or 7 Ethernet cables that are grounded on both ends.

> ⚠️ **WARNING** *GR-1089-CORE compliance requires all intra-building Ethernet ports to use shielded intra-building cables that are grounded at both ends.*

- All video connections use shielded coaxial cables grounded on both ends.

> ⚠️ **WARNING** *GR-1089-CORE compliance requires all intra-building video ports to use shielded intra-building coaxial cabling that is grounded at both ends.*

- Radio antenna connections use shielded coaxial cables grounded on both ends.

> ⚠️ **WARNING**
> *GR-1089-CORE compliance requires all radio antenna ports to use shielded coaxial cabling that is grounded at both ends.*

> ⚠️ **WARNING**
> *GR-1089-CORE compliance requires external lightning protection to be used for the radio antenna ports to prevent transients of greater magnitude or duration than 600 Volts and 50 microseconds respectively.*

> ⚠️ **WARNING**
> *GR-63-CORE earthquake risk zones require coaxial cable to be made with compression F connectors (do not use crimped connectors).*

- Use shielded RS-232 cable grounded on both ends.

> ⚠️ **WARNING**
> *RS-232 ports are only intended for testing and troubleshooting. GR-1089-CORE compliance requires that these ports be unconnected during normal operation.*

> ⚠️ **WARNING**
> *USB ports are only intended for manufacturing use. GR-1089-CORE compliance requires that these ports be unconnected.*

Series 30 Hardware Installation

> 📌 **NOTE**
> *The EASyCAP® is suitable for deployment in Network Telecommunication Facilities or Locations where the NEC applies.*

Installation Recommendations for Earthquake Risk Zones

Note that the following installation recommendations are required for compliance with GR-63-CORE Earthquake Risk Zones.

Two Post Installation

1. Secure the front of the EASyCAP to the rack using four screws as shown.
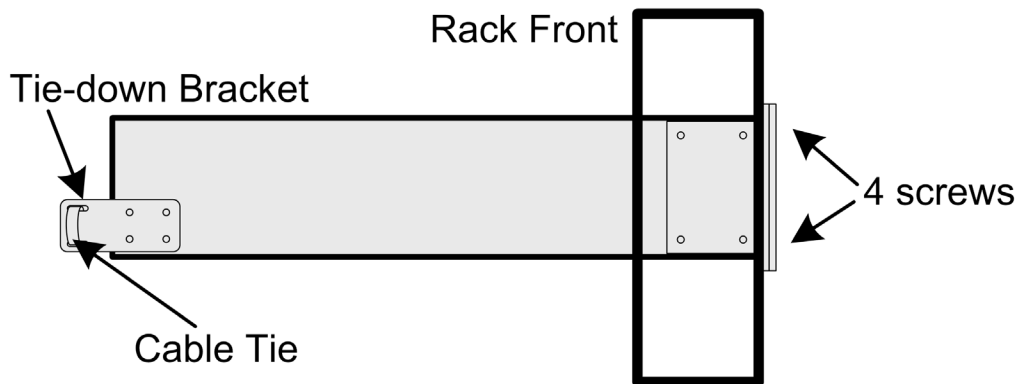
All wiring must be secured to prevent interruptions during an earthquake. The following recommendations provide one method to secure the wiring, but other methods may be preferable depending on the racks and equipment available at the site.

1. Secure the AC cord by wrapping a cable tie around the AC cord and through the tie-down bracket at the rear of the chassis as shown. Tighten the cable tie until the AC cord connector is pulled slightly towards the bracket (by about 1/8 inch). Do not overtighten to prevent damaging the power entry.


Secure AC cord to rear bracket

2. Secure all wires to the tie-down brackets or to the closest point on the rack that will allow for the cables to be secured with cable ties. Tighten the cable ties enough to prevent movement of the cables.

Four Post Installation

Shelf angle brackets must be installed in the rack to support the EASyCAP chassis. Use Gaw Technology 404PC110905D2 or similar shelf angle brackets that are secured to both the front and rear of the rack and allow no more than ½" deflection at 50 pounds static pull.

1. Install the shelf angle brackets, mounting them to both sides of the rack and securing them to the front and rear of the rack as shown.

2. Place the EASyCAP chassis directly on top of the angle brackets so that it sits flat on the angle brackets for the entire depth of the chassis.

3. Secure the front of the EASyCAP to the rack using four screws as shown.

4. Secure the back of the EASyCAP to the shelf angle brackets using 14.5" cable ties with 50 pounds tensile strength (Panduit PLT4S-C30 or equivalent). Wrap the cable ties through the rear EASyCAP brackets and around the shelf angle brackets as shown, ensuring that the cable ties are tight enough to prevent the rear of the EASyCAP chassis from vertical movement.
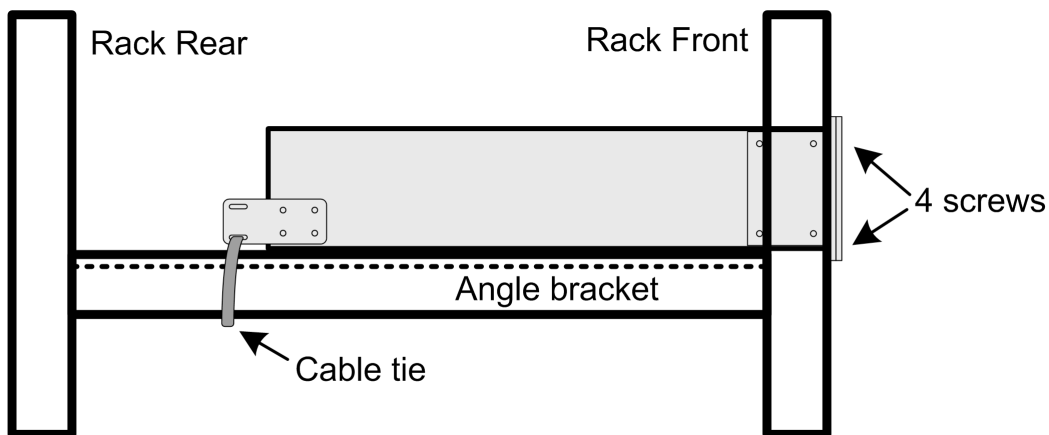
Rack Rear   Rack Front   4 screws   Angle bracket   Cable tie

All wiring must be secured to prevent interruptions during an earthquake. The following recommendations provide one method to secure the wiring, but other methods may be preferable depending on the racks and equipment available at the site.
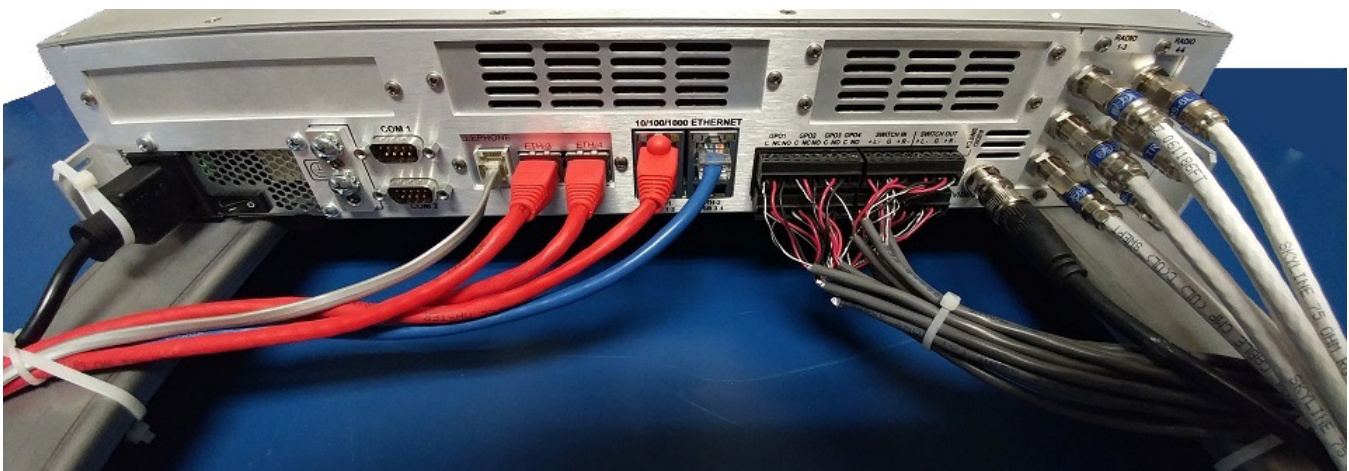

1. Secure the AC cord by wrapping a cable tie around the AC cord and through the rear bracket of the chassis as shown. Tighten the cable tie until the connector on the AC cord is slightly pulled towards the bracket (by about 1/8 inch). Do not overtighten or it could cause damage to the AC power entry.

Secure AC cord to rear bracket

Secure cables to shelf angle bracket
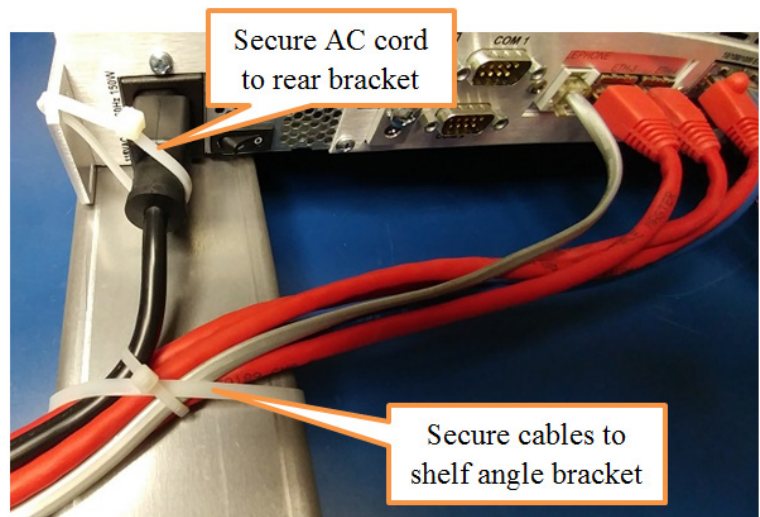
2. Secure the AC cord, Ethernet, and Telephone cables to the shelf angle bracket as shown. Wrap a cable tie around the shelf angle bracket and the cables. Wrap a second cable tie around the cables and the first cable tie. Tighten the cable ties enough to prevent movement of the cables.

3. Bundle all of the audio, general purpose input, general purpose output, and TTL output wires together and wrap a cable tie around them about 2 inches from the connectors.

4. Bundle all of the video and antenna coaxial cables and then wrap a cable tie around them about 4-5 inches from the connectors.

Bundle audio and GPIO wires together

Bundle coaxial cables together
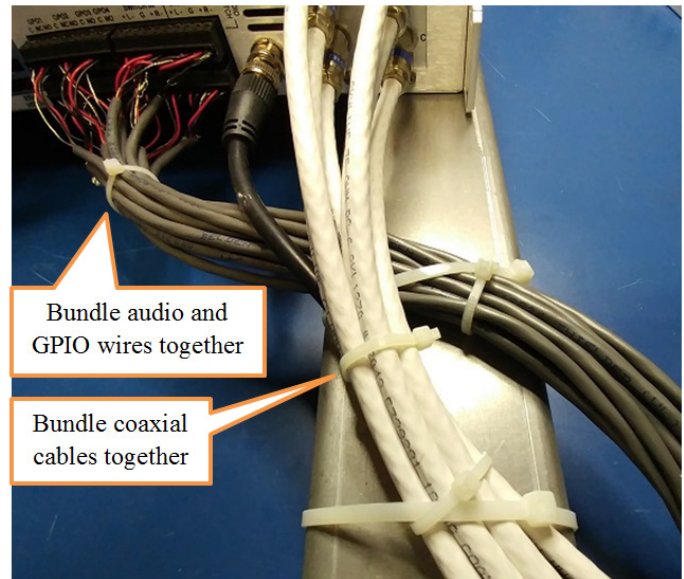
5. Secure the bundle of audio and general purpose input/output cables to the shelf angle bracket as shown. Wrap a cable tie around the shelf angle bracket and the cables. Wrap a second cable tie around the cables and the first cable tie. Tighten the cable ties enough to prevent movement of the cables.

Secure coaxial cables to the shelf angle bracket

Secure audio and GPIO wires to the shelf angle bracket
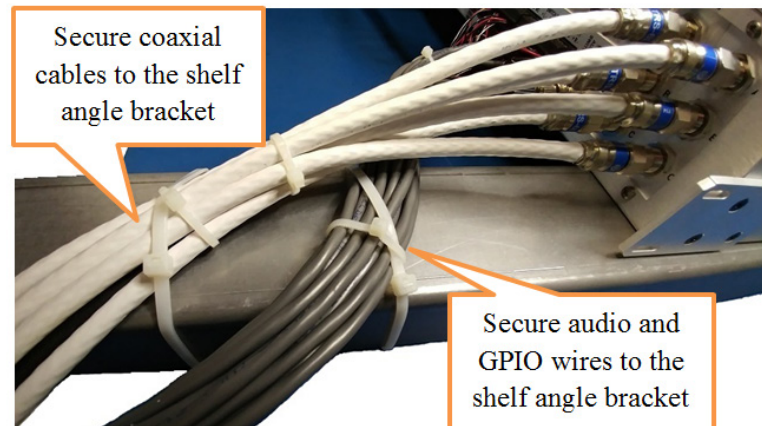
6. Secure the bundle of antenna and video coaxial cables to the shelf angle bracket as shown. Wrap a cable tie around the shelf angle bracket and the cables. Wrap a second cable tie around the cables and the first cable tie. Tighten the cable ties enough to prevent movement of the cables.

Chassis Grounding

The EASyCAP® chassis must be grounded to a Common Bonding Network for NEBS compliant grounding in a Telecommunications Central Office, Data Center, VHO, NOC, or VOC. The ground connection must use a 10-14 AWG copper cable and the supplied grounding hardware, or equivalents. The ground wire must be installed in accordance with local electrical safety standards.

Install the grounding wire before connecting the EASyCAP® to AC power. See the ground lug manufacturer's recommendations for wire gauge and installation instructions.

1. Strip approximately ½ inch of the insulation away from the ground wire. The ground wire must be 10–14 AWG copper cable.

2. Coat the stripped ground wire with an antioxidant compound before making crimp connections.

3. Insert the stripped end of the ground wire into the open end of the supplied ground lug (ILSCO CSWD-10-10-58, or equivalent Listed ground lug).

4. Crimp the ground wire in the barrel of the ground lug (see the ground lug manufacturer's recommendations for crimping tools).

5. Secure the ground lug to the chassis using the supplied screws and washers. The lock washers must be located between the screw head and the ground lug.

10-14 AWG Grounding/Bonding Wire

Ground Lug

Two #10 lock washers
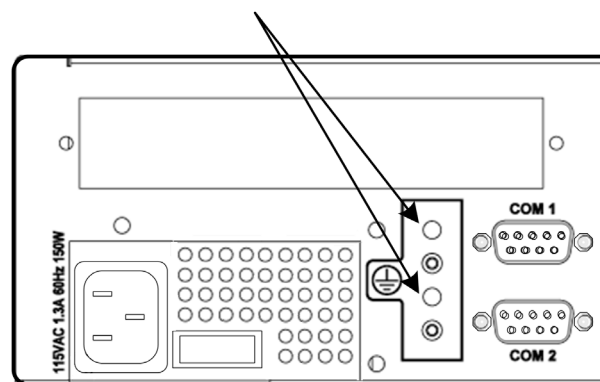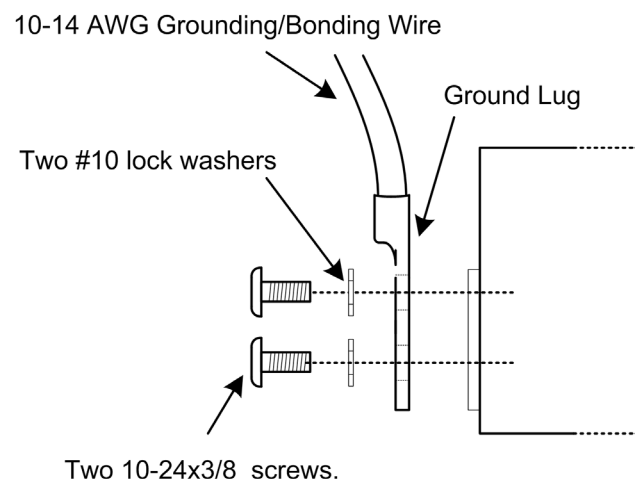
Two 10-24x3/8 screws.

Supplied screws: (2) two 10-24 x 3/8" tri-lobular thread-rolling screws (Fastenal 0143623 or equivalent)

Supplied washers: (2) two #10 lock washers (Fastenal 1133735 or equivalent)

6. Prepare the other end of the ground wire and connect it to the rack ground or to the common bonding system.

Maintenance

Replacing the Fan Filter

The fan filter can be purchased from VIAVI or directly from the filter manufacturer (Universal Air Filter Company, part number TR-170206-1). The filter manufacturer recommends that the fan filter be replace every six months; however, for sites that maintain an ambient temperature below 25 degrees Celsius and whose environment does not have a high level of contaminants, it is recommended to replace the filter once a year.

1. Remove the two thumb screws securing the fan grill to the front panel.

2. Remove the fan grill.

3. Remove the fan filter.
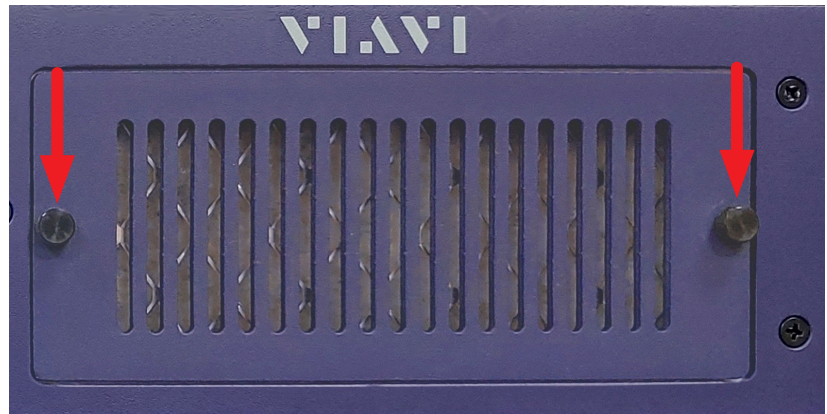
4. Insert the new fan filter, ensuring that the arrow on the side of the filter is pointing into the EASyCAP chassis (as shown here).

5. Install the fan grill back onto the front panel using the two thumb screws removed in step one.

Replacing the Fans

The fans can be purchased from VIAVI or directly from the manufacturer (Dynatron, part number DF126025BL-3G). The EASyCAP must be taken out of service to replace the fans.

NOTE: The estimated time required to replace a fan is less than 30 minutes.

1. Power down the EASyCAP, remove it from the rack and place it on a bench.

2. Remove the screws from the top cover and then remove the cover from the chassis.

3. Remove the two thumb screws securing the fan grill to the front panel.

4. Remove the fan grill and the fan filter.

5. Fan-1 is located on the left side and Fan-2 is located on the right side as shown.

6. Remove the 4 screws securing the fan to the fan bracket.
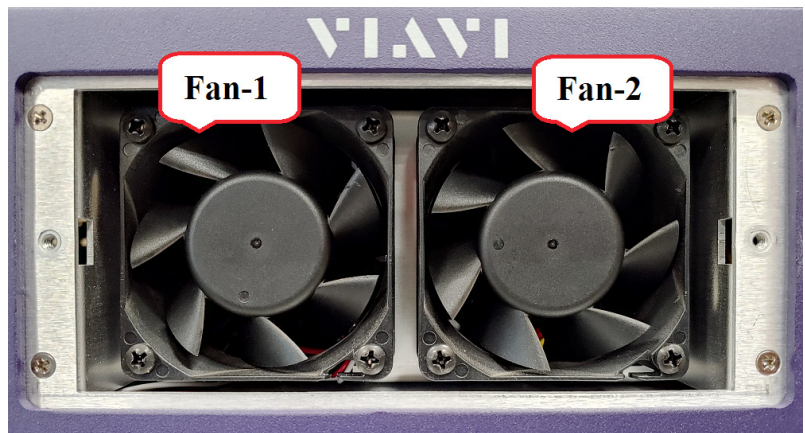
7. Cut the cable tie securing the fan connector and then disconnect the fan connector from the PC board on the front panel. The top connector (P5) is Fan-1 and the bottom connector (P6) is Fan-2.
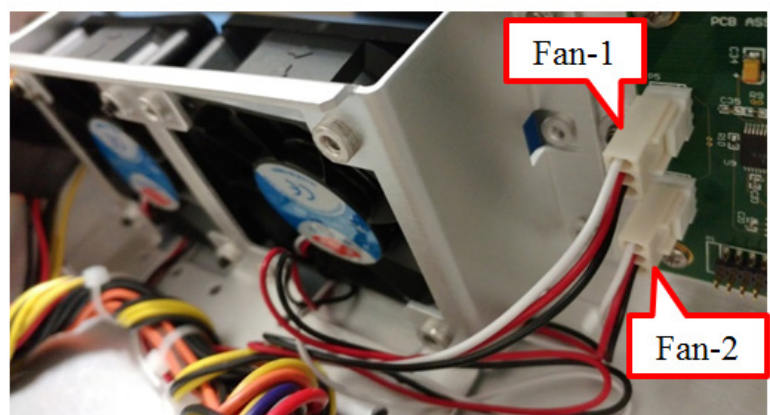
8. Cut and remove the cable tie that secures the fan cable and then remove the fan.

9. Install the new fan using the 4 screws that were removed in step 6. Make sure the airflow arrows located on the side of the fan point into the EASyCAP chassis.
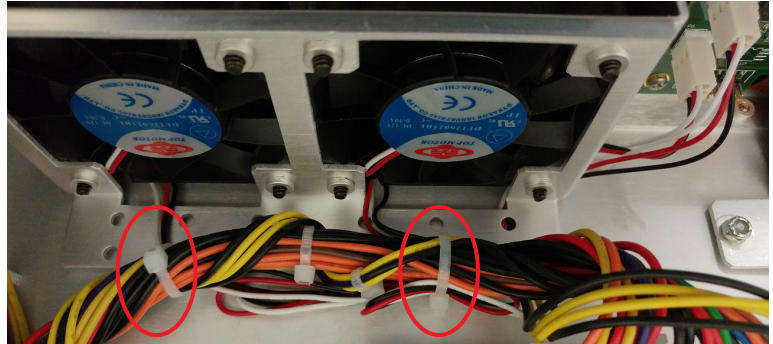
10. Connect the fan cable back to the connector on the front panel's PC board and wrap a cable tie around the connector to secure it to the header on the board.

11. Replace the cable tie removed in step 8 with a new cable tie to secure the fan cable, ensuring that it does not block airflow.
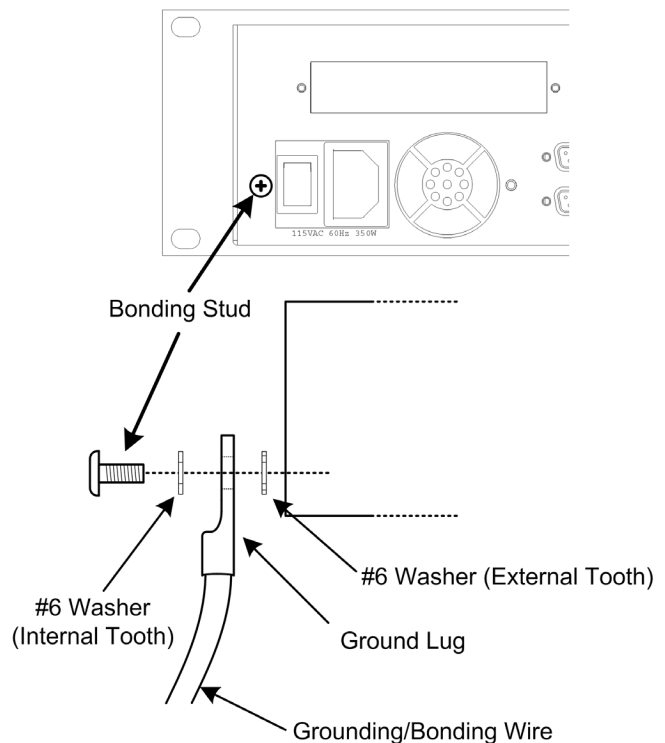
Series 20 Chassis Grounding

The EASyCAP® chassis must be grounded to a Common Bonding Network for NEBS compliant grounding in a Telecommunications Central Office, Data Center, VHO, NOC, or VOC. The ground connection must use a copper cable and the grounding hardware supplied, or their equivalents. A 10 AWG copper cable is recommended. Bare conductors must be treated with antioxidant before crimp connections are made. A star washer must be used as shown to prevent rotation of the ground stud. The ground wire must be installed in accordance with local electrical safety standards.

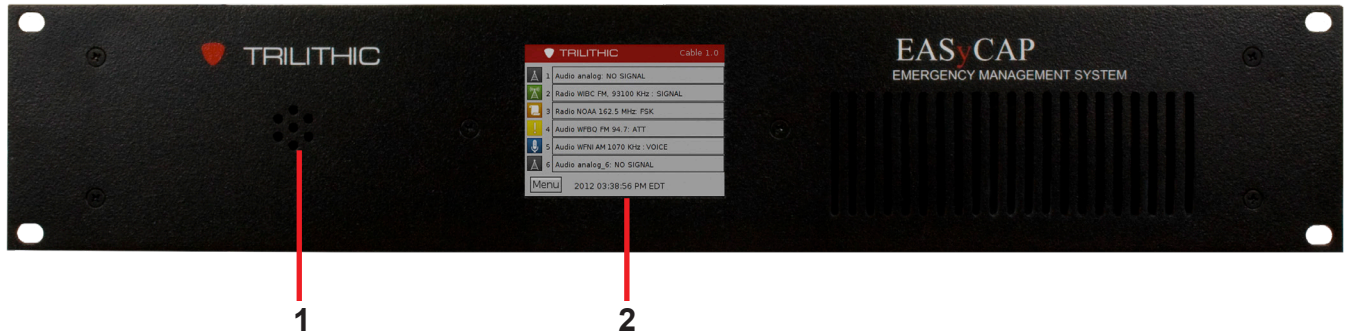Install the grounding wire before connecting the EASyCAP® to AC power.

1. Strip approximately ½ inch of the insulation away from one end of the ground wire.

2. Coat the stripped ground wire with an antioxidant compound before making crimp connections.

3. Insert the stripped end of the ground wire into the open end of the supplied ground lug.

4. Crimp the ground wire in the barrel of the ground lug.

5. Remove the grounding stud screw from the chassis as shown in the diagram.

6. Secure the ground lug and washers to the chassis using the grounding stud screw as shown in the diagram. The external tooth washer must be located between the ground lug and the chassis, and the internal tooth washer must be located between the screw head and the ground lug.

7. Prepare the other end of the ground wire and connect it to the rack ground or to the common bonding system.

Bonding Stud

#6 Washer (Internal Tooth)

#6 Washer (External Tooth)

Ground Lug

Grounding/Bonding Wire

115VAC 60Hz 350W

Hardware Overview (Series 20)
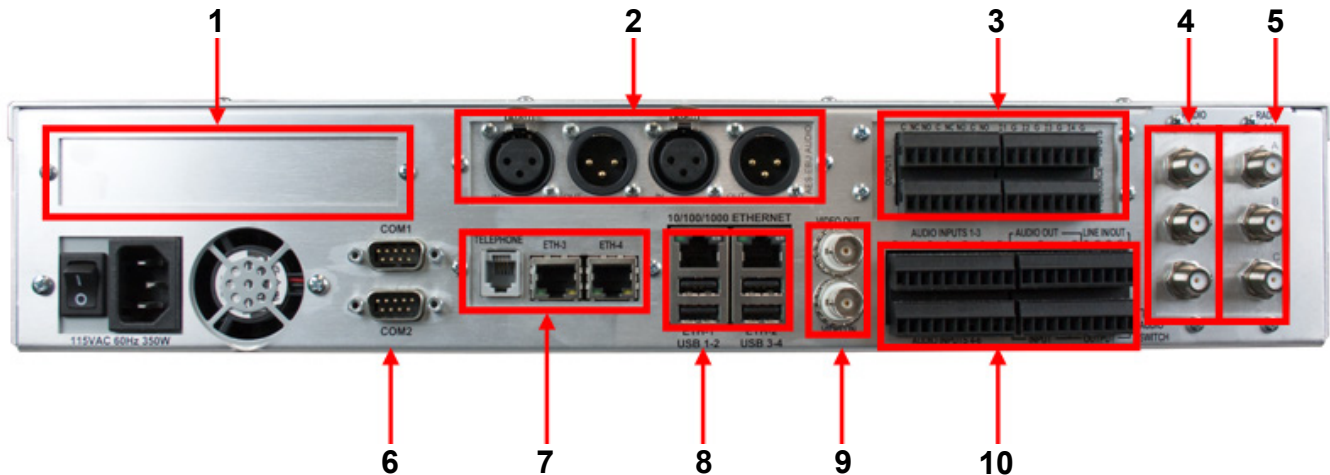
Front Panel View

1. **Speaker** – Used for monitoring audio inputs and to provide aural feedback during EAS activations.

2. **Touchscreen LCD Display** – Provides visual feedback during programming, setup, monitoring, and activations and it is used for local control of the EASyCAP® and access to the on-board menu system.

> **NOTE**
>
> *The keypad and LCD display provide an on-board menu system, allowing for a limited amount of configuration, tests, and encoding functions. A secure web interface provides more comprehensive configuration and control of the encoder/ decoder.*

Rear Panel View

1. **PCIe Expansion Slot (Optional)** – This is a PCI Express expansion slot that will accommodate one (1) PCIe card. This is reserved for future use. Only use cards approved by VIAVI. Use of unapproved cards may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.

2. **Audio Expansion Slot (Optional)** – One (1) slot is provided for expansion audio boards. An AES-EBU digital audio board is currently available. Additional cards may be available. Contact EAS Customer Support for information.

AES-EBU Digital Audio Board – Provides independent synchronized AES-EBU audio switches for in-line replacement of programming audio during EAS operations. It includes two (2) AES-EBU digital audio switches on 110 Ohm XLR connections. The internal switches replace the normal AES-EBU program audio with alert audio. The alert audio automatically locks to the incoming bit rate and sample rate (up to 192 kHz). If no input is provided, the output sample rate will be 48KHz. Bypass relays are provided to ensure the program audio is not interrupted during a power loss.

AES-EBU Input 110 Ohm XLR female

Pin 1: Ground/drain
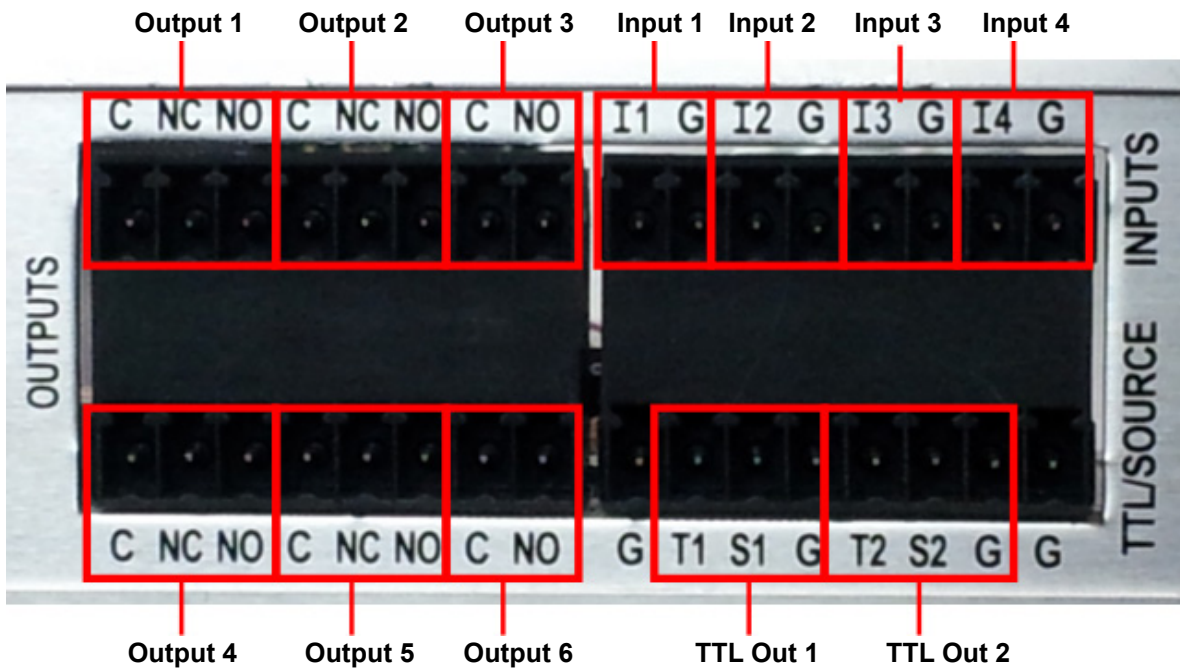
Pin 2: Balanced +

Pin 3: Balanced -

AES-EBU Output - 110 Ohm XLR male

Pin 1: Ground/drain

Pin 2: Balanced +

Pin 3: Balanced –

3. **General Purpose Inputs/Outputs** – The EASyCAP® Encoder/Decoder comes standard with six (6) general purpose outputs, four (4) general purpose inputs, and two (2) TTL outputs. Additional cards may be available, contact EAS Customer Support for information.

General Purpose Outputs – Six (6) contact closure outputs (switches) are provided for activating equipment to route the alert audio and video, sound alarms, and activate other devices during EAS transmission. When an output is active, the common and normally opened terminals are shorted together (closed).

(C) Common contact

(NC) Normally-closed contact

(NO) Normally-open contact

The following shows the default configuration for the outputs, TTL, and inputs. These are all configurable in the software.

Output 1, Transmitting Audio – Activates when alert audio playback is in progress. This is used to activate audio distribution and routing equipment during EAS activations in order to replace the normal program audio with the alert audio.

Output 2, Transmitting – Activates when alert playback is in progress (audio and video). This is used to activate audio and video distribution and routing equipment during EAS activations in order to replace the normal program audio and video with the alert information.

Output 3, Time Adjusted – Activates a configurable number of seconds before or after the alert audio and video playback begins and deactivates a configurable number of seconds before or after the alert playback ends. It is used to trigger equipment that requires time to acquire the EAS audio/video, create an MPEG stream, or send commands across a network.

Output 4, EAN/Live Event Active – Activates when an EAN or a Live Event is in progress.

Output 5, Reserved – This output is reserved for future use.

Output 6, Reserved – This output is reserved for future use.

TTL Outputs – Provide a five (5) volt DC signal (and ground) used to activate EAS audio and video routing equipment. A current source is also provided.

TTL 1, Transmitting – Activates at the same time as General Purpose Output 1.

TTL 2, Reserved – Activates at the same time as General Purpose Output 2.

EASyCAP Encoder/Decoder User's Guide
Document 0010340001, Rev. 24.08

General Purpose Inputs – Four (4) general purpose inputs provide a means for operators and external automation equipment to trigger and abort EAS activations.

The default settings are shown below.

Input 1, Abort – When closed (shorted), stops playback of the EAS message in progress. The EASyCAP® will attempt to stop all video and audio replacement equipment and then return to monitoring for incoming alert messages. This input is edge-triggered. Holding it closed will not continuously abort messages.

> **(G)** Contact ground
>
> **(I1)** Opto-isolated input

Input 2, Disabled

> **(G)** Contact ground
>
> **(I2)** Opto-isolated input

Input 3, Disabled

> **(G)** Contact ground
>
> **(I3)** Opto-isolated input

Input 4, Disabled

> **(G)** Contact ground
>
> **(I4)** Opto-isolated input

4. **Radios 1-3 (optional)** – A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Each audio input can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).

   (A) Channel 1 radio receiver antenna input (75 ohm F connector)

   (B) Channel 2 radio receiver antenna input (75 ohm F connector)

   (C) Channel 3 radio receiver antenna input (75 ohm F connector)
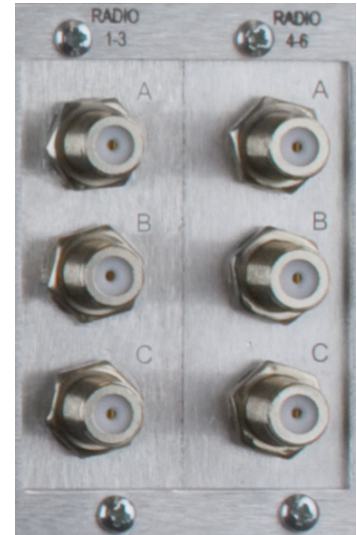
5. **Radios 4-6 (optional)** – A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed in this slot, providing up to 6 (six) internal radio receivers. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Each audio input can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).

   (A) Channel 4 radio receiver antenna input (75 ohm F connector)

   (B) Channel 5 radio receiver antenna input (75 ohm F connector)

   (C) Channel 6 radio receiver antenna input (75 ohm F connector)

6. **RS-232 Serial Ports** – Two (2) RS-232C compliant serial data connections are provided on DB-9 male connectors.

COM-1 (top DB-9 connector) – This port provides a command line console into the EASyCAP® for low-level configuration, control, and troubleshooting.

COM-2 (bottom DB-9 connector) – This port can be configured to provide EAS information to external equipment such as character generators, sign boards, and logging/monitoring systems.

9-pin RS-232C DTE Interface – Normally connects to PCs or equipment with a 9-pin NULL-MODEM cable.

Pin 2: Receive data*	**Pin 3:** Transmit data*
Pin 4: Data terminal ready	**Pin 5:** Signal ground*
Pin 6: Data set ready	**Pin 7:** Request to send
Pin 8: Clear to send	**Pin 9:** Ring indicator

* Required signal

7. **Communications Expansion Slot** – The EASyCAP® can accommodate one (1) optional communications expansion board. Contact EAS Customer Support for information.

Expansion communications board with Dual LAN and MODEM

- Two (2) 10/100 Ethernet Ports
- One (1) Telephone Modem Port (56K data and voice) – Allows DTMF and data communication for remote generation of emergency messages.
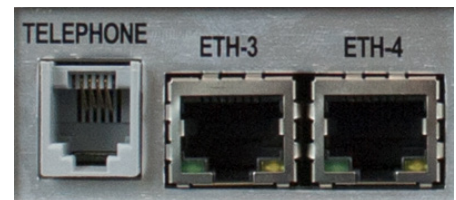
8. **Ethernet and USB Ports**

   Ethernet – Two (2) 10/100/1000 Ethernet ports provide an interface for remote management of the EASyCAP®, monitoring CAP feeds, and providing EAS information to downstream audio, video, and distribution equipment.

   USB Ports – Four (4) USB ports are provided. Only use devices approved by VIAVI. Use of unapproved devices may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.

9. **CG VIDEO –** The EASyCAP® includes an internal analog video character generator to display the alert text. An internal analog video switch is provided to automatically switch the internal character generator into the program video during message playback. It includes a video bypass relay to ensure that the program video is not interrupted during a power loss.

   VIDEO IN – NTSC video input connection to the internal video switch for the normal program video.

   VIDEO OUT – NTSC video output connection from the internal switch. The video output normally contains the program video fed into the input. During alert message playback, the output is automatically switched to the internal character generator.

10. Audio Inputs and Outputs
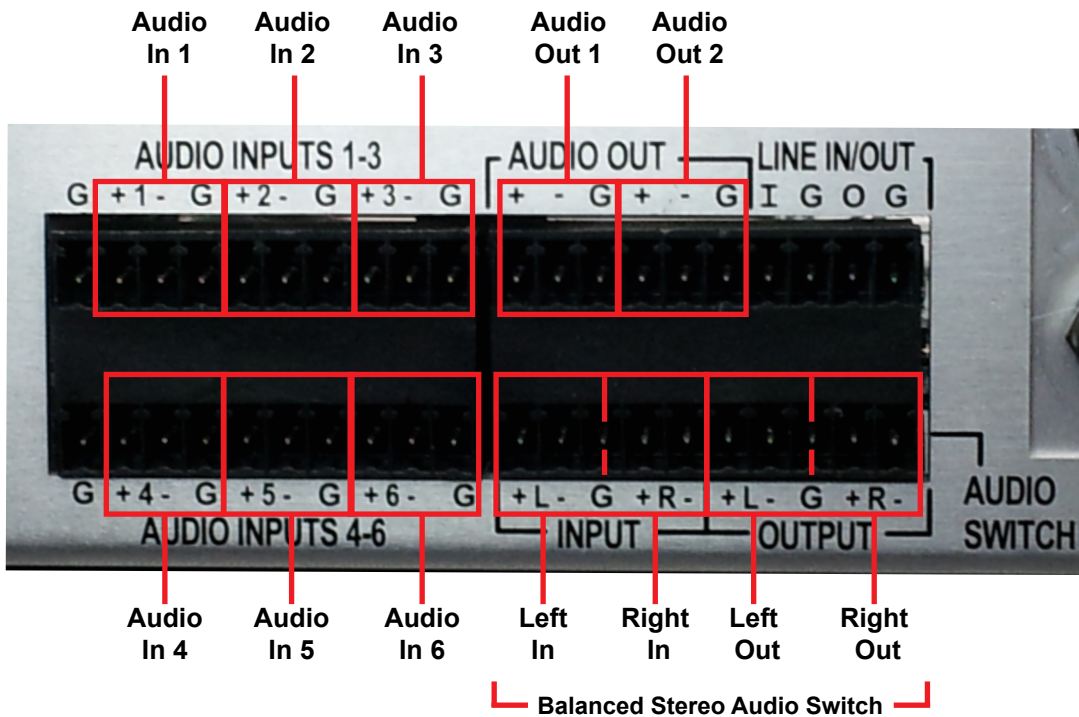
Audio inputs – Six (6) balanced 600 ohm audio inputs are provided to monitor external audio sources for EAS. They can be connected to audio sources such as external radio receivers, TV tuners, and satellite receivers. Configuration is provided to select between external audio sources and internal radio receivers for each input.

(+) Positive analog audio input for the respective channel

(-) Negative analog audio input for the respective channel

(G) Ground

Audio outputs – Two (2) balanced 600 ohm audio outputs are provided for the alert audio. They can be connected to EAS distribution and routing equipment. The outputs contain audio generated by the EASyCAP® during EAS activations.

(+) Positive analog audio output

(-) Negative analog audio output

(G) Ground

Audio Switch – A 600 ohm balanced stereo audio switch is provided to replace normal program audio with alert audio during EAS activations. The switch includes a bypass relay to ensure that program audio is not interrupted during a power loss.

Input – Connect normal program audio to the audio switch input.

Output – Connect the audio switch output into the normal program audio path. The output from the audio switch normally contains the program audio fed into the input. During EAS activations, the output contains the alert audio.

Audio Switch Terminals (from left to right)

Inputs

(+) Positive analog audio input for the left channel

(-) Negative analog audio input for the left channel

(G) Ground

(+) Positive analog audio input for the right channel

(-) Negative analog audio input for the right channel

Outputs

(+) Positive analog audio output for the left channel

(-) Negative analog audio output for the left channel

(G) Ground

(+) Positive analog audio output for the right channel

(-) Negative analog audio output for the right channel

Hardware Overview (Series 30)

Front Panel View

1. **Speaker** – Used for monitoring audio inputs and to provide aural feedback during EAS activations.

2. **Touchscreen LCD Display** – Provides visual feedback during programming, setup, monitoring, and activations and it is used for local control of the EASyCAP® and access to the on-board menu system.

> **NOTE**
>
> *The keypad and LCD display provide an on-board menu system, allowing for a limited amount of configuration, tests, and encoding functions. A secure web interface provides more comprehensive configuration and control of the encoder/decoder.*

Rear Panel View

1. **PCIe Expansion Slot (Optional)** – This is a PCI Express expansion slot that will accommodate one (1) PCIe card. This is reserved for future use. Only use cards approved by VIAVI. Use of unapproved cards may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.

   SDI Video Output Board - The optional SDI Video Output board is shown. It can be configured to output standard definition (SD) or high definition (HD) SDI video. Eight (8) channels of embedded audio is supported for HD, and 2 channels is supported for SD. The video normally contains a static display of a configurable image or color. During alert message playback, the alert text is overlaid onto a configurable image or color. Different images can be configured for different types of alerts. Note that the SDI Video Board is only available for the Series 30 Hardware.

2. **Audio Expansion Slot (Optional)** – One (1) slot is provided for expansion audio boards. An AES-EBU digital audio board is currently available. Additional cards may be available. Contact EAS Customer Support for information.

AES-EBU Digital Audio Board – Provides independent synchronized AES-EBU audio switches for in-line replacement of programming audio during EAS operations. It includes two (2) AES-EBU digital audio switches on 110 Ohm XLR connections. The internal switches replace the normal AES-EBU program audio with alert audio. The alert audio automatically locks to the incoming bit rate and sample rate (up to 192 kHz). If no input is provided, the output sample rate will be 48KHz. Bypass relays are provided to ensure the program audio is not interrupted during a power loss.

Input: 110 Ohm XLR female	**Output: 110 Ohm XLR male**
Pin 1: Ground/drain	**Pin 1:** Ground/drain
Pin 2: Balanced +	**Pin 2:** Balanced +
Pin 3: Balanced -	**Pin 3:** Balanced –

3. **Radios 1-3 (optional, included with IPTV models)** – A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Each audio input can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).

    (A) Channel 1 radio receiver antenna input (75 ohm F connector)

    (B) Channel 2 radio receiver antenna input (75 ohm F connector)

    (C) Channel 3 radio receiver antenna input (75 ohm F connector)
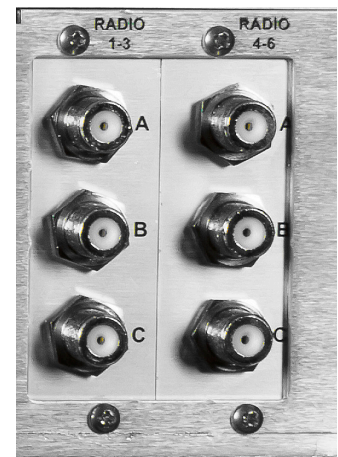
4. **Radios 4-6 (optional, included with IPTV models)** – A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed in this slot, providing up to six (6) internal radio receivers. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Audio input 4 can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).

    (A) Channel 4 radio receiver antenna input (75 ohm F connector)

    (B) Channel 5 radio receiver antenna input (75 ohm F connector)

    (C) Channel 6 radio receiver antenna input (75 ohm F connector)

5. **RS-232 Serial Ports** – Two (2) RS-232C compliant serial data connections are provided on DB-9 male connectors.

    COM-1 (top DB-9 connector) – This port provides a command line console into the EASyCAP® for low-level configuration, control, and troubleshooting.

    COM-2 (bottom DB-9 connector) – This port can be configured to provide EAS information to external equipment such as character generators, sign boards, and logging/monitoring systems.

    9-pin RS-232C DTE Interface – Normally connects to PCs or equipment with a 9-pin NULL-MODEM cable.

Pin 2: Receive data*	**Pin 3:** Transmit data*
Pin 4: Data terminal ready	**Pin 5:** Signal ground*
Pin 6: Data set ready	**Pin 7:** Request to send
Pin 8: Clear to send	**Pin 9:** Ring indicator

    * Required signal

6. **Communications Expansion Slot (optional, included with IPTV models)** – The EASyCAP® can accommodate one (1) optional communications expansion board. Contact EAS Customer Support for information.

    Expansion communications board with Dual LAN and MODEM

    *   Two (2) 10/100 Ethernet Ports
    *   One (1) Telephone Modem Port (56K data and voice) – allows DTMF and data communication for remote generation of emergency messages.
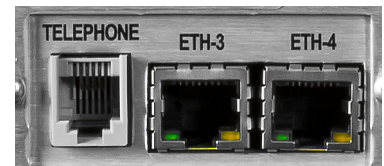
7. **Ethernet and USB Ports**

    Ethernet – Two (2) 10/100/1000 Ethernet ports provide an interface for remote management of the EASyCAP®, monitoring CAP feeds, and providing EAS information to downstream audio, video, and distribution equipment.

    USB Ports – Four (4) USB ports are provided. Only use devices approved by VIAVI. Use of unapproved devices may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.
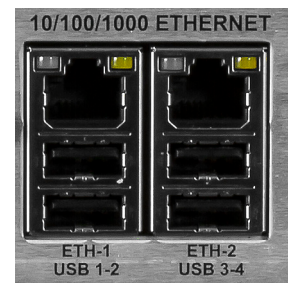
8. **General Purpose and Audio Inputs/Outputs** – The EASyCAP® Series 30 Encoder/ Decoder comes standard with four (4) general purpose outputs, two (2) general purpose inputs, one (1) TTL output, two (2) audio outputs, one (1) stereo audio switch, and four (4) audio inputs.
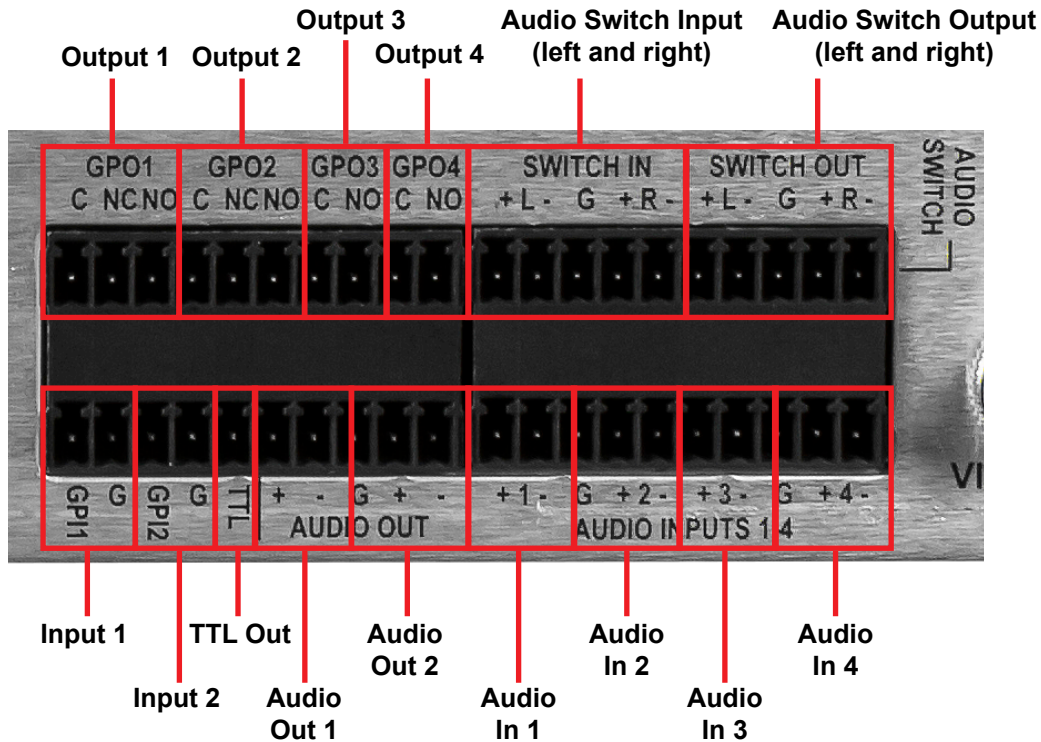
General Purpose Outputs – Four (4) contact closure outputs (switches) are provided for activating equipment to route the alert audio and video, sound alarms, and activate other devices during EAS transmission. When an output is active, the common and normally opened terminals are shorted together (closed).

(C) Common contact

(NC) Normally-closed contact

(NO) Normally-open contact

> **NOTE**
>
> *The following shows the default configuration for the outputs, TTL, and inputs. These are all configurable in the software.*

Output 1, Transmitting Audio – Activates when alert audio playback is in progress. This is used to activate audio distribution and routing equipment during EAS activations in order to replace the normal program audio with the alert audio.

Output 2, Transmitting – Activates when alert playback is in progress (audio and video). This is used to activate audio and video distribution and routing equipment during EAS activations in order to replace the normal program audio and video with the alert information.

Output 3, Time Adjusted – Activates a configurable number of seconds before or after the alert audio and video playback begins and deactivates a configurable number of seconds before or after the alert playback ends. It is used to trigger equipment that requires time to acquire the EAS audio/video, create an MPEG stream, or send commands across a network.

Output 4, EAN/Live Event Active – Activates when an EAN or a Live Event is in progress.

TTL Output – This output provides a five (5) volt DC signal (and ground connection) used to activate EAS audio and video routing equipment.

Activates at the same time as General Purpose Output 1.

General Purpose Inputs – Two (2) general purpose inputs provide a means for operators and external automation equipment to trigger and abort EAS activations. The following functions can be assigned to the inputs.

(GPI1)   Input 1 pin

(G)   Contact ground

(GPI2)   Input 2 pin

(G)   Contact ground

The following input functions are assigned by default, but all inputs are configurable in the software.

Input 1: Abort – When closed (shorted), stops playback of the EAS message in progress. The EASyCAP® will attempt to stop all video and audio replacement equipment and then return to monitoring for incoming alert messages. This input is edge-triggered. Holding it closed will not continuously abort messages.

Input 2: Disabled

Audio inputs – Four (4) balanced 600 ohm audio inputs are provided to monitor external audio sources for EAS. They can be connected to audio sources such as external radio receivers, TV tuners, and satellite receivers. Configuration is provided to select between external audio sources and internal radio receivers for each input.

(+) Positive analog audio input for the respective channel

(-) Negative analog audio input for the respective channel

(G) Ground

Audio outputs – Two (2) balanced 600 ohm audio outputs are provided for the alert audio. They can be connected to EAS distribution and routing equipment. The outputs contain audio generated by the EASyCAP® during EAS activations.

(+) Positive analog audio output

(-) Negative analog audio output

(G) Ground

Audio Switch – A 600 ohm balanced stereo audio switch is provided to replace normal program audio with alert audio during EAS activations. The switch includes a bypass relay to ensure that program audio is not interrupted during a power loss.

Input – Connect normal program audio to the audio switch input.

Output – Connect the audio switch output into the normal program audio path. The output from the audio switch normally contains the program audio fed into the input. During EAS activations, the output contains the alert audio.

Audio Switch Terminals (from left to right)

Inputs

(+) Positive analog audio input for the left channel

(-) Negative analog audio input for the left channel

(G) Ground

(+) Positive analog audio input for the right channel

(-) Negative analog audio input for the right channel

Outputs

(+)   Positive analog audio output for the left channel

(-)   Negative analog audio output for the left channel

(G)   Ground

(+)   Positive analog audio output for the right channel

(-)   Negative analog audio output for the right channel

9. **CG VIDEO** – The EASyCAP® includes an internal analog video character generator to display the alert text.

> **VIDEO OUT** – The NTSC video output normally contains a static display of a configurable image or color. During alert message playback, the alert text is overlaid onto a configurable image or color. Different images can be configured for different types of alerts.

Front Panel Menu Overview

Touch Screen LCD

The EASyCAP® Encoder/Decoder includes a touch-screen LCD on the front panel to provide EAS status indicators and a simple graphical user interface for a limited amount of configuration and control.

Main Screen (Home Page)
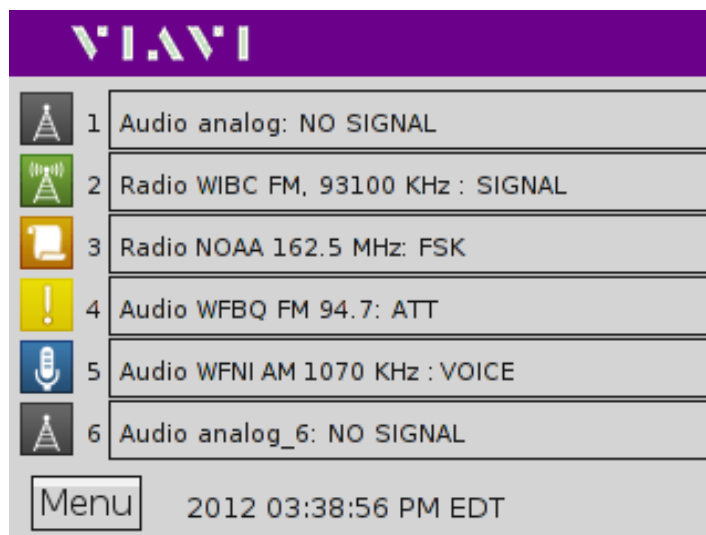
The Main screen is displayed when the system is idle and monitoring for EAS messages. The EASyCAP® application type and software version are displayed in the top right corner of the screen. The bottom line shows the current date and time of the EASyCAP®.

The **Menu** button is located in the bottom left corner of the screen to allow access to the front panel menu.

Current Status

The current status of each EAS audio input is displayed on the main screen. The following information is displayed for each audio input:

- Channel

- Type of audio source – "Audio" if the input is configured to receive audio from an external audio source or "Radio" if the input is configured as an internal radio.

- Configured name of the audio source

- The current status

- If the input is an internal radio - the radio station frequency is displayed.

Status: NO SIGNAL

A status of "NO SIGNAL" indicates that audio is not detected at this input.


```
 A   1 | Audio  WFNI AM 1070 KHz : NO SIGNAL
```
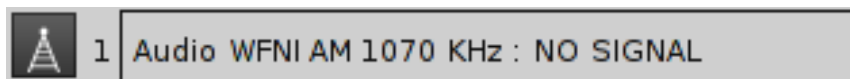
Status: SIGNAL

A status of "SIGNAL" indicates that audio is detected at this input.


```
 A   2 | Radio WIBC FM, 93100 KHz : SIGNAL
```
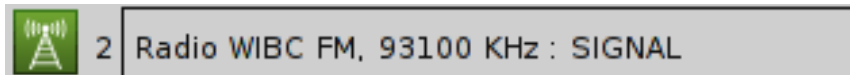
Status: FSK

A status of "FSK" indicates that EAS FSK is being received on this input.


```
     3 | Radio NOAA 162.5 MHz: FSK
```
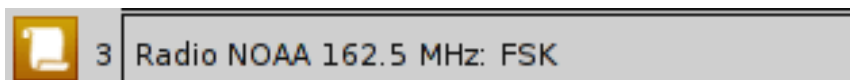
Status: ATT

A status of "ATT" indicates that an Attention Tone is being received on this input.


```
  !  4 | Audio WFBQ FM 94.7: ATT
```
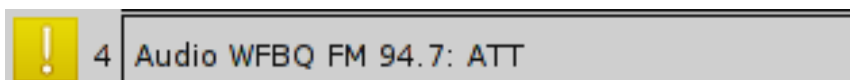
Status: VOICE

A status of "VOICE" indicates that an EAS Voice Message is being recorded.


```
     5 | Audio WFNI AM 1070 KHz : VOICE
```
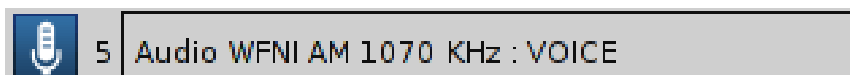
Alert Playback Screen

The **EAS Alert Playback** screen is displayed during EAS message playback. The alert text of the current alert playback can be viewed.

Select the **Cancel** button to stop the current message playback. It will end the local playback and, where possible, send cancel messages to configured external equipment.

When running a Broadcast Application in manual mode a Confirm button will be displayed on this screen to allow the operator to confirm that the alert should be transmitted.
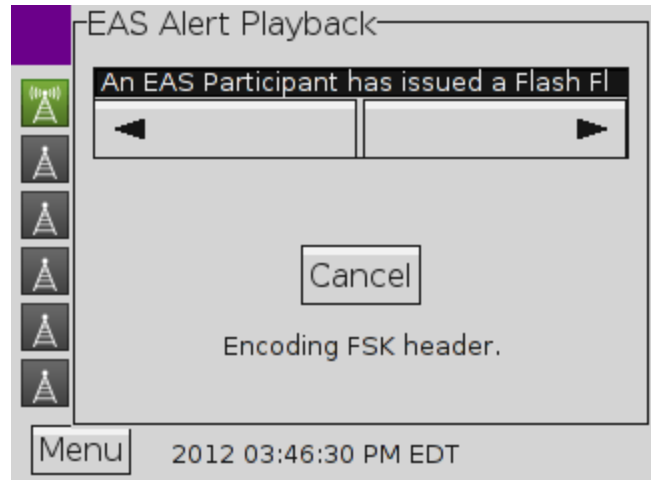
Login Menu

The **Login** screen is displayed after the **Menu** button is selected. A valid User PIN must be entered before entering the menu. Note that the user account must have configuration privileges.

Enter your User PIN (4-8 digit code) and select the **OK** button. The factory default PIN is 2345.

To go back to the **Main** screen and cancel the Login, select the **Cancel** button.
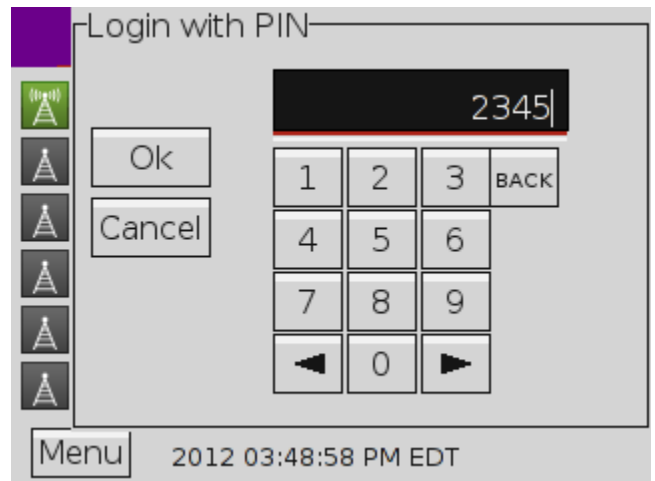
Setup Menu

The **Setup** screen is displayed after logging into the menu. It provides access to any available menus for configuration and control.

Network button – Displays the **Network Setup** menu. This menu allows you to view and change network settings.

System button – Displays the **System Control** menu. This menu allows you to restart the EASyCAP®, and to encode a RWT.

Front Panel button – Displays the **Front Panel Configuration** menu. This menu allows you to configure the themes (colors and styles) for the LCD and on-board menu.

Close button – Exits the **Setup** menu and returns to the **Main** screen.
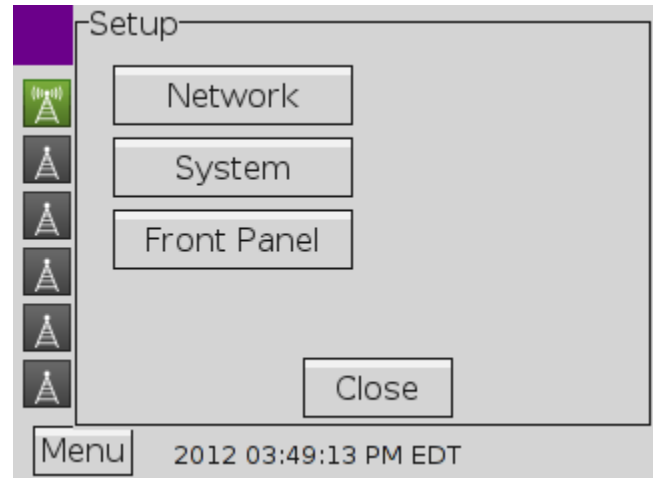
Network Setup Menu

The **Network Setup** menu displays the available network interfaces and the MAC address of each. A button is provided to view and change the settings for each network interface.

Ethernet <N> button – Opens the configuration menu for the selected network interface.

Save button – Saves any changes made to the network interfaces settings and closes the **Network Setup** menu.

Cancel button – Cancels any changes made to the network interfaces settings and closes the **Network Setup** menu.
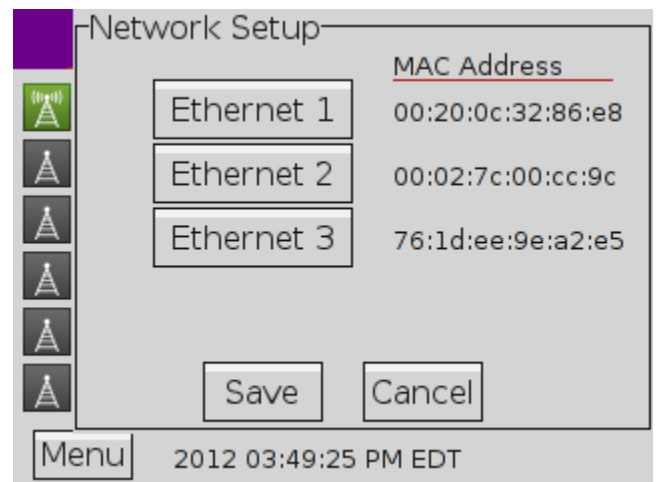
Ethernet Interface Setup Menu

The **Ethernet Interface Setup** menu shows the current settings for the interface and provides controls to change the interfaces settings.

DHCP/Static/Disabled – Select if the Ethernet interface is configured automatically using DHCP or manually using Static configuration. The interface can also be disabled.

When DHCP is selected, all network settings are obtained automatically from the DHCP server. No additional settings are needed.

IP Address button – Displays a menu with a keyboard to enter the Static IP Address.

Subnet button – Displays a menu with a keyboard to enter the interfaces subnet mask.

Gateway – Displays a menu with a keyboard to enter the IP address for the Default Gateway.

> **NOTE**
>
> ***When network settings are saved from the front panel menu, SSH and the Web Interface will be enabled for all interfaces.***
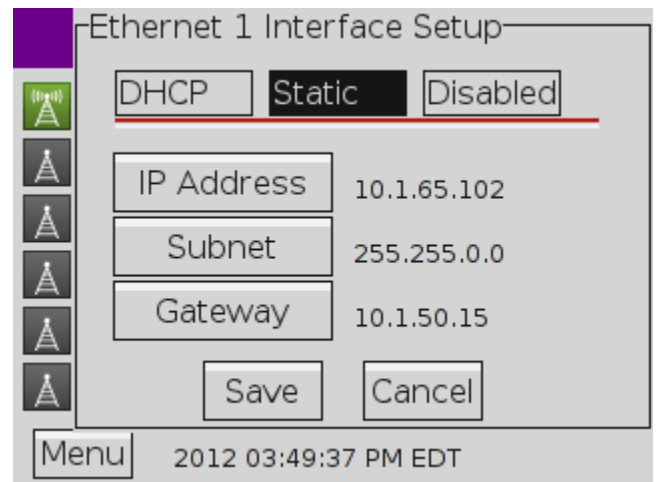
IP Address Entry Menu

The **Ethernet IP Address** menu provides an edit box and keyboard to allow IP addresses to be entered. Enter the IP address using the keypad. This menu is also used to enter a subnet mask and gateway address.

Select the **Save** button to save the IP address.

Press the **Cancel** button to discard changes to the IP address and close the **Ethernet IP Address** menu.
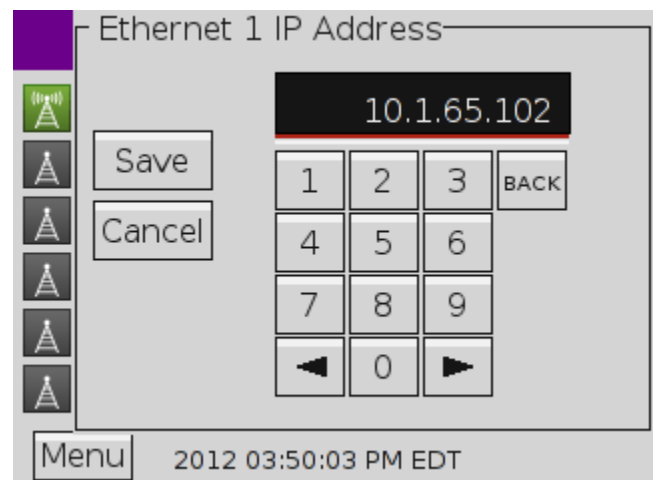
System Menu

The **System** menu provides controls to restart and shutdown the EASyCAP® unit. Operators can also generate RWT messages from this menu.

Restart – Restarts (reboots) the EASyCAP® unit.

Shutdown – Shuts down the EASyCAP® unit. Turn the power switch off after the system has completed shutdown (power is not automatically removed).

Encode RWT – Generates a RWT message. FIPS codes for the RWT are configured through the Web Interface (EAS Options).

Cancel – Closes the **System** menu.
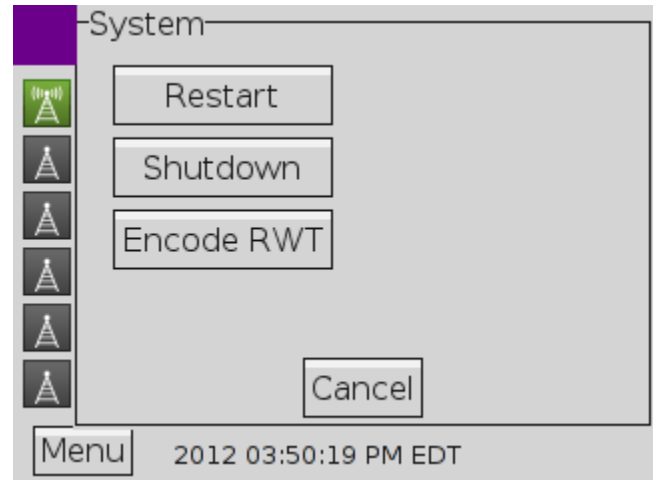
Front Panel Menu

The **Front Panel** menu allows some customization of the colors and styles used for the LCD and on-board menu. Select from four themes.

Theme <N> – Select the theme for the LCD and menu (see sample of themes below).

Cancel – Closes the **Front Panel** menu.

Configuration
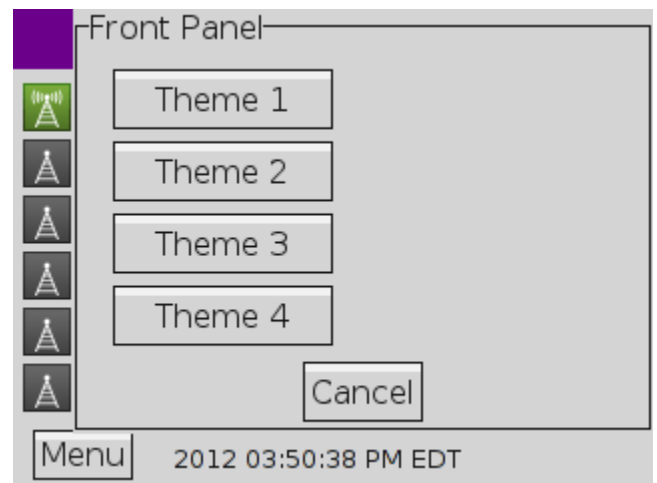
System Login
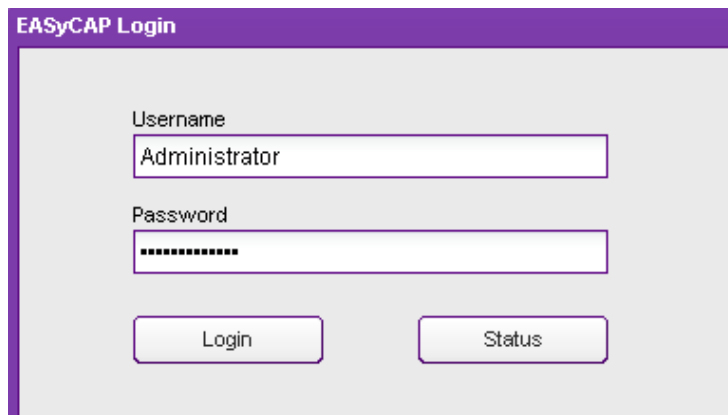
A web server is provided to manage the EASyCAP® Encoder/Decoder. The web interface can be configured to use HTTP on port 80 and HTTPS (secure) on port 443. The EASyCAP® is shipped from the factory with both secure (HTTPS) and non-secure (HTTP) interfaces enabled. We recommend using Chrome or Firefox web browsers.

The following should be noted when using the secure web server:

- The certificate shipped with the EASyCAP® Encoder/Decoder is not signed by a trusted certificate authority, so web browsers will display a security alert about the certificate when connecting for the first time. At this point, acknowledge the security alert and continue to the site even though the certificate isn't trusted.

- When using Mozilla Firefox, the web browser will retain the security setting for the next time you connect the server. If you are using Chrome or Internet Explorer, the security alert will be displayed every time that you connect to the web server. To disable the security alert, install a trusted certificate for the web server from the Web Configuration screen or install the EASyCAP® certificate on your PC. To install the EASyCAP® certificate on your PC from Internet Explorer, click on the **Certificate Error** message (next to the URL), click **View Certificates**, then click **Install Certificates**.

Perform the following steps to login to the EASyCAP® Encoder/Decoder:

1. Enter http:// followed by the IP address of the EASyCAP® Encoder/Decoder into the URL bar of the web browser and then press **Enter** on your keyboard. Enter https:// followed by the EASyCAP® address to login to the secure web server on port 443.

2. The **EASyCAP® Login** screen will appear. Enter the username and password for the desired user account and then press the **LOGIN** button. The factory default user account has a username and password of *Administrator*.

> ⚠️ **CAUTION**
>
> ***If an error message appears warning you to change your password, open the Administration/User Accounts screen and change your account password.***

EASyCAP Status Information

Status information about the EASyCAP system, CAP sources, EAS sources, and configuration can be viewed without logging in by pressing the **Status** button. Access to the status information screen prior to login can be enabled or disabled from the **Web Configuration** screen. If this feature is disabled, the **Status** button will be disabled and greyed out.

The **System Information** tab shows general information such as host name, system type, software versions, part number, serial number, installed hardware, last login, memory usage, temperatures, and fan status.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.

EASyCAP Status

| System Information | Alert Tab | EAS Sources | CAP Sources | Message Deliveries | Configured Locations |

Component	Description
Hostname	EzCap21
System	EASyCAP IPTV
Software Version	18.10
Product	EASyCAP I6020
Part Number	2011421500
Serial Number	00115
Machine Key	XPIdecVLIB8QSZ9Yx8C/
Operating System	Debian GNU/Linux 8
OS Updates Package	Linux Updates Version 18.10
Kernel	Linux 3.16.0-6-amd64
Last Login	10/17/18 06:27:46 PM Administrator logged in from remote address 10.1.65.10
Total Memory	1951204 kB
Available Memory	856760 kB
Total Disk Space	29928500 kB
Available Disk Space	26525512 kB
CPU Temperature	45 C
Mainboard Temperature	35 C
Fan 1	OK

[Refresh]   [Close]

The **Alert** tab shows the status of alert message playback.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.
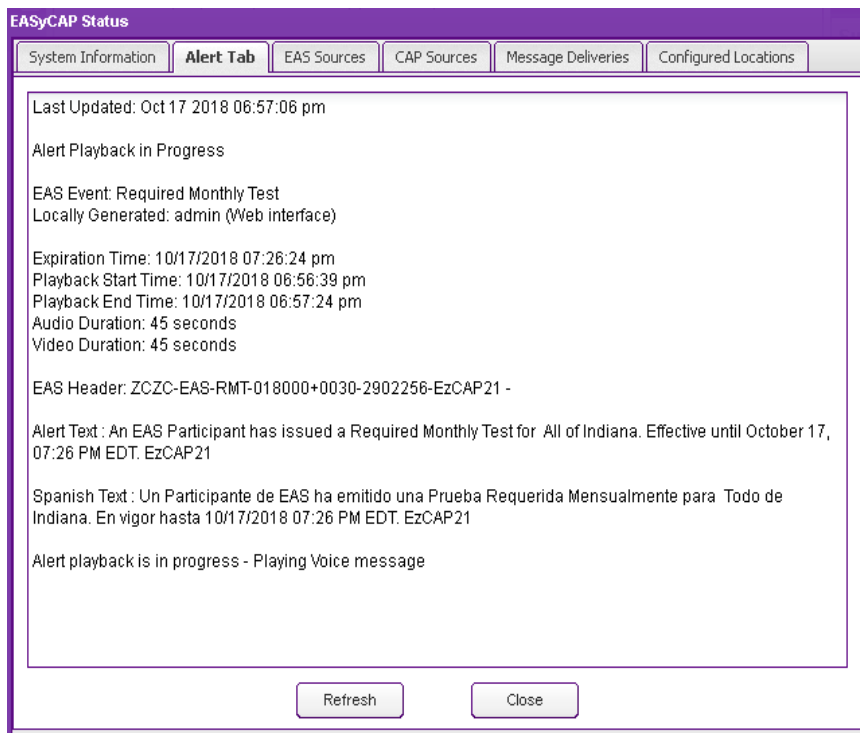
The **EAS Sources** tab shows the status of all audio inputs configured to monitor for EAS messages.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.
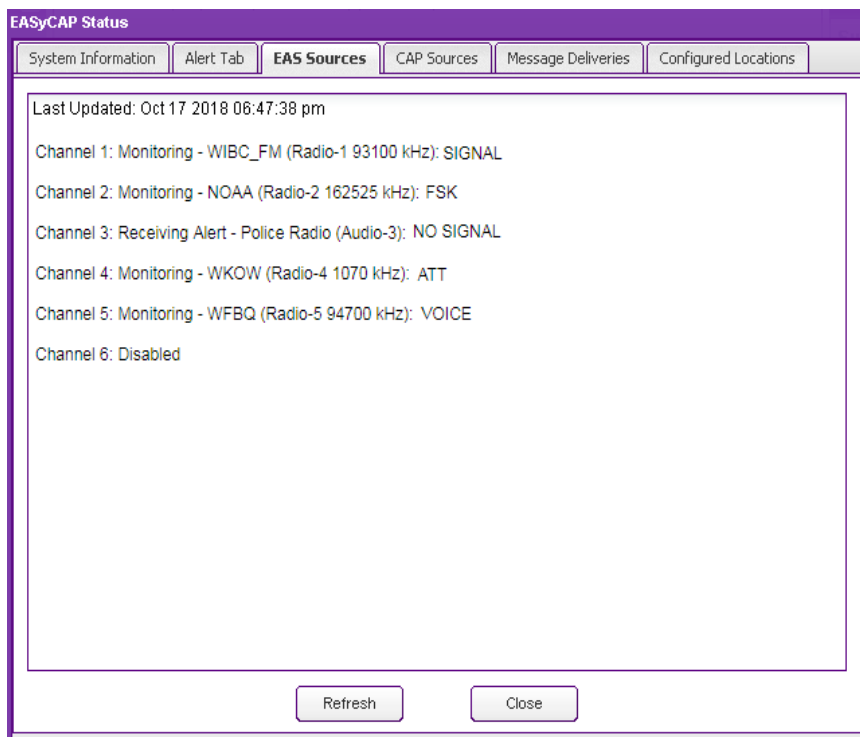
The **CAP Sources** tab shows the status of all configured CAP feeds.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.
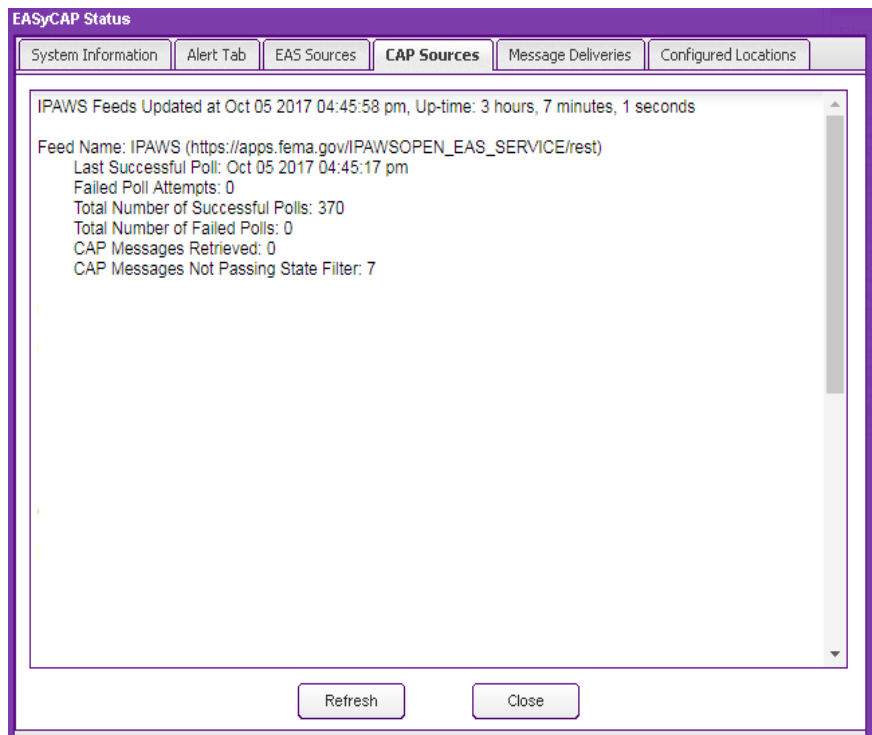
The **Message Deliveries** tab shows all configured devices and servers that will receive alerts from the EASyCAP.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.
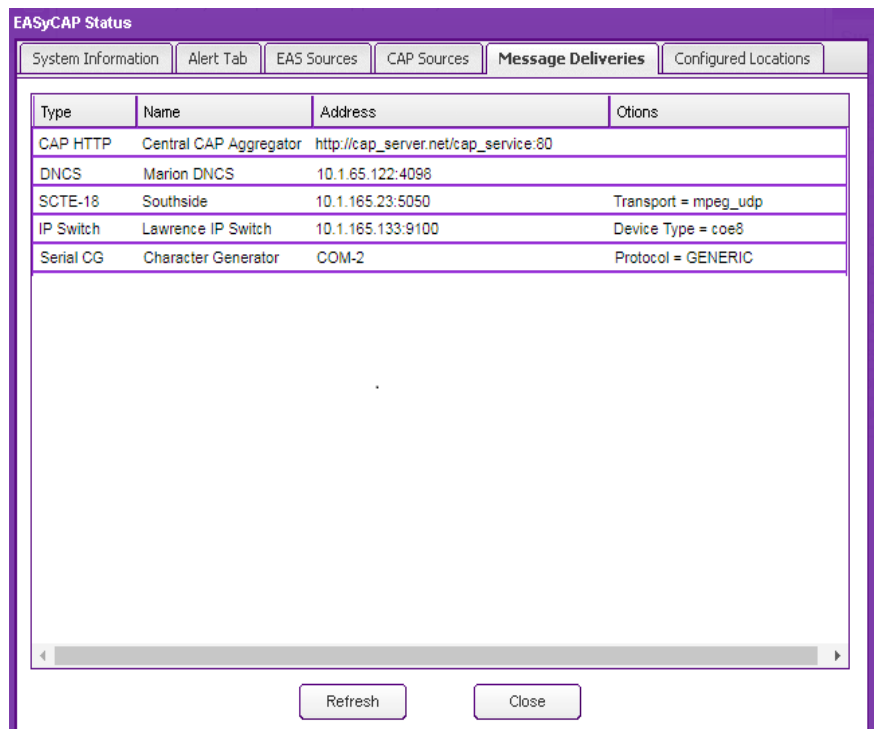
The **Configured Locations** tab shows all configured locations, which are used to determine which alerts are processed.

Press the **Refresh** button to update the status information.

Press the **Close** button to return to the **Login** screen.

FIPS ▲	County / User	State
017000	All of Illinois	Illinois
018000	All of Indiana	Indiana
018003	Allen	Indiana
018005	Bartholomew	Indiana
018011	Boone	Indiana
018013	Brown	Indiana
018023	Clinton	Indiana
018047	Franklin	Indiana
018057	Hamilton	Indiana
018059	Hancock	Indiana
018063	Hendricks	Indiana
018089	Lake	Indiana
018093	Lawrence	Indiana
018097	Marion	Indiana
018105	Monroe	Indiana
018113	Noble	Indiana
018119	Owen	Indiana
018121	Parke	Indiana
018123	Perry	Indiana

EASyCAP Status — tabs: System Information | Alert Tab | EAS Sources | CAP Sources | Message Deliveries | **Configured Locations**

Refresh   Close

EASyCAP User Interface Homepage

After logging into the system, the homepage will be displayed as shown below.
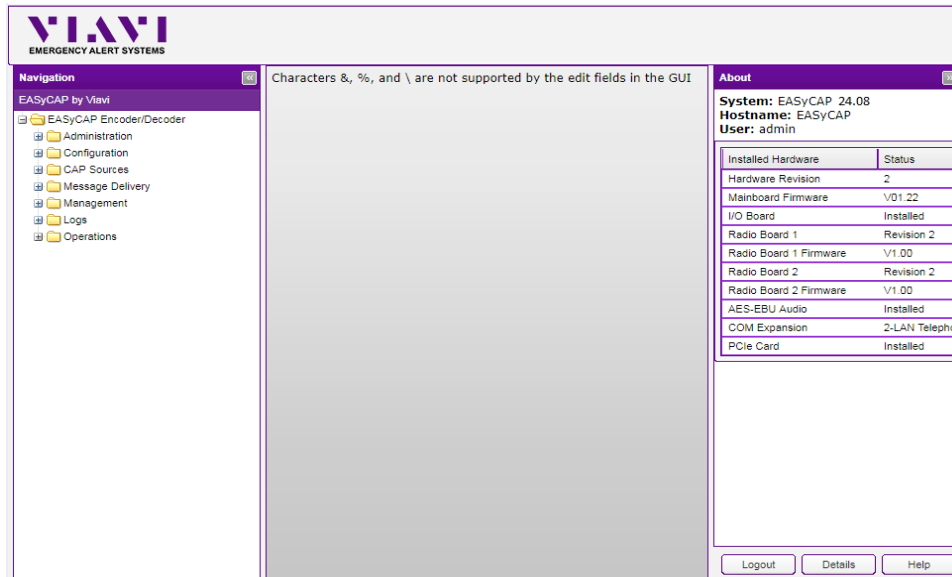
The following items can be viewed from the homepage:

About – This area on the right side of the homepage shows the EASyCAP® Encoder/ Decoder software version, installed hardware, and current login user name.

Logout – Click this button to logout of the system.

Details – Displays information about the EASyCAP® Encoder/Decoder, including installed hardware, system information, and network information.

Help – Displays the EASyCAP® Encoder/Decoder Operation Manual.

Navigation – The bar on the left hand side of the homepage is used to navigate to each of the pages. The pages are sorted into folders/categories according to function; **Administration**, **Configuration**, **CAP Sources**, **Message Delivery**, **Management**, **Logs,** and **Operations**. Select the plus (+) sign to expand a category and select the minus (-) sign to collapse a category. To view a page, select the corresponding link inside each folder.

Navigation

EASyCAP by Viavi

- EASyCAP Encoder/Decoder
  - Administration
  - Configuration
    - Audio/Tone Volume
    - Audio/Radio Sources
    - Date/Time
    - EAS Events
    - EAS Options
    - General Purpose I/O
    - Lead-In/Background/Lead-Out
    - MPEG-DASH
    - MPEG Stream
    - Network Interfaces
    - Playback Options
    - Selected Locations
    - Video Output
    - Web Configuration
  - CAP Sources
  - Message Delivery
    - Atom CAP Server
    - CAP HTTP Delivery
    - DCM
    - DNCS/Evertz
    - IP Switches
    - Minerva
    - SCTE-18
    - Serial Devices
  - Management
  - Logs
  - Operations

Administration Folder

In the Navigation bar, click the **+** sign next to the Administration folder to expand the folder.
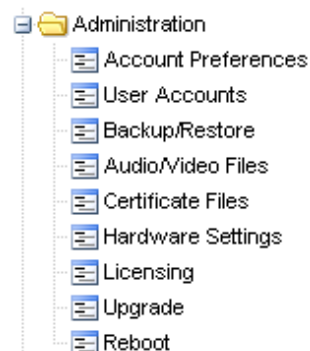
Account Preferences

To setup the user account preferences for the EASyCAP®, click **Account Preferences** in the Administration folder. The account preferences are used to customize password aging and complexity. To comply with recommendations from the CSRIC EAS Security Best Practices, users should be required to change their passwords periodically, and weak passwords should be prevented.

Request passwords to be changed after xx days – When enabled, users will be prompted to change their password after a configurable number of days (30 - 365) and a warning will appear every time a user logs in with an expired password.

Minimum password length – Enter the minimum number of characters allowed for passwords (4 - 32).

Passwords require an uppercase and lowercase character – When enabled, all passwords must include at least one uppercase character and at least one lowercase character.

Passwords require at least one number – When enabled, passwords must include at least one number (0 - 9).

Passwords cannot be the same as username – When enabled, passwords are not allowed to be the same as the username.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

User Accounts

To setup the user accounts for the Encoder/Decoder, click **User Accounts** in the Administration folder. The **User Configuration** window will be displayed as shown.

> **NOTE**
>
> ***Below is the default user account shipped from the factory:***
> ***User Name: Administrator***
> ***Password: Administrator***
> ***PIN: 2345***

Select User – Select a user account from the dropdown list.

Add button – Create a new user account.

Delete button – Delete the selected user account. A confirmation page will be displayed. Click **Yes** to delete the user account or **No** to exit without deleting the user.

User Settings

Username – Enter the username for the Account. The username must be unique and cannot be changed after the account is created. To change the username of an existing account, delete the account and create a new account.

> **NOTE**
> *The username can only include alphanumerics. It cannot include any spaces or special characters.*

Password – Enter the password for the user account. The password must be between 4 and 32 characters long, and must adhere to the password complexity rules setup in the account preferences.

Confirm Password – Enter the password again for verification.

> **NOTE**
> *The password cannot include spaces or any of the following characters: &, %, ', ", /, or \.*

PIN – Enter the PIN (Personal Identification Number) for the User account into this field. The PIN must be between 4 and 8 digits (numeric digits only) and must be unique.

Confirm PIN – Enter the PIN again for verification.

Description – Enter a description for this user account.

Locations

Check the locations for the selected user account. These locations are used when the user generates EAS messages. At least one location must be configured if the selected user has permission to use the Telephone interface.

Roles

Configuration – Allow the user to make changes to the EASyCAP® configuration. This role must be enabled for any user that needs access to the front panel menu.

Configure Users – Allow the user to make changes to all user accounts. Note that any user can change their own password and PIN at any time regardless of the user account role.

Upgrade Software – Allow the user to upgrade the EASyCAP® Encoder/Decoder software.

System Tests – Allow the user to perform calibration and system tests.

Generate EAS – Allow the user to generate EAS messages.

Generate Messages – Allow the user to generate custom (not EAS) messages.
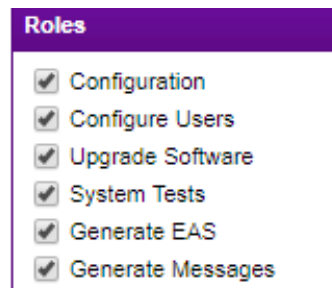
Permissions

Front Panel – The user is allowed to access the front panel menu.

Web Server – The user is allowed access to the Web Server GUI interface.

Web API – The user is allowed access to the Web API interface. The **Web API** includes REST and CGI interfaces for monitoring status and performing specific operations.

Telephone Access – The user is allowed access to the touch-tone telephone interface.

Abort from Telephone – The user is allowed to abort messages in progress from the touch-tone telephone interface.
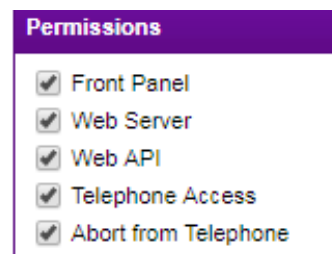
Select the **Save** button to save changes to the User Account.

Select the **Close** button to close the User Configuration screen.

Select the **Help** button to view the User Accounts section of the operational manual.

If changes were not saved before selecting **Close**, a dialog will be displayed. Select **No** to return to the User Configuration screen, or **Yes** to exit without saving changes.

Backup/Restore Configuration

To Backup or Restore the EASyCAP configuration, select the **Backup/ Restore Configuration** link in the **Administration** folder.

Optional configuration files to backup/restore – Select optional configuration to backup or restore. When restoring a configuration, these optional configurations must be present in your backup file in order for them to be restored.

Backup/Restore Configuration

Optional files to backup/restore
- [ ] Network Configuration
- [ ] NTP Configuration
- [ ] Certificate Files
- [ ] Debug Logs (Backup Only)

Backup Configuration

Press the Backup button to backup the current configuration. After the backup is created, a download link will be displayed. Click the link to download the backup file to your computer.

[Backup]

Restore Configuration

Press the Browse (or Choose File) button to select an archive file and then press the Restore button to restore the configuration. Reboot the unit to make the settings take effect.

Backup File: [Choose File] No file chosen

[Restore]

User Accounts, Web API, Date, and Time settings are not backed up or restored. You will need to configure these settings.

[Close] [Help]

> **Network Configuration** – Backup or restore the network configuration.
>
> **NTP Configuration** – Backup or restore the NTP configuration.

Certificate Files – Backup or restore the certificate files that were configured for the EASyCAP through the Web Interface.

Debug Logs – This option is provided to backup debug logs for troubleshooting purposes. It's normally used to send troubleshootiing information to VIAVI technical support. The debug logs are not used in the restore process.

Click the **Backup** button to backup the current EASyCAP® configuration. After the Save dialog is displayed, navigate to the desired directory on your PC and click **Save**.

Click the **Browse** (or **Choose File**) button to restore a configuration backup. Select the desired configuration backup file and click **Open.** Then click the **Restore** button. A dialog will appear asking if you want to reboot. The restored configuration will not take effect until the EASyCAP® is rebooted.

Click **Close** to exit the **Backup/Restore Configuration** screen.

Click **Help** to view the **Backup/Restore** section of the operational manual.

> **NOTE** *User Accounts, Web API, Date, and Time settings are not backed up or restored.*

Audio/Video Files

To delete, load, and view audio and image files, select the Audio/Video **Files** link. These files can be configured as background images for video outputs. They can also be used for lead-in and lead-out messages.

Audio Files – List of the audio files that have been uploaded. Select a file to preview or delete it.

Preview Audio – Click this link to listen to the selected audio file.

Upload New File – Press this button to upload an audio file (WAV or MP3 formats only). An **Upload Audio File** window will be displayed. Press the **Browse** (or **Choose File**) button, select the file, and then press the **Upload** button.

Delete Selected File – Press this button to delete the selected audio file.

Image Files – List of the image files that have been uploaded. Select a file to preview or delete it.

Preview Image – Click this link to view the selected image file.

Upload New File – Press this button to upload an image file (JPG format only). An **Upload Image File** window will be displayed. Press the **Browse** (or **Choose File**) button, select the file, and then press the **Upload** button.

Delete Selected File – Press this button to delete the selected image file.

Close – Press this button to close the window.

Help – Press this button to view the Audio/Video Files section of the operational manual.
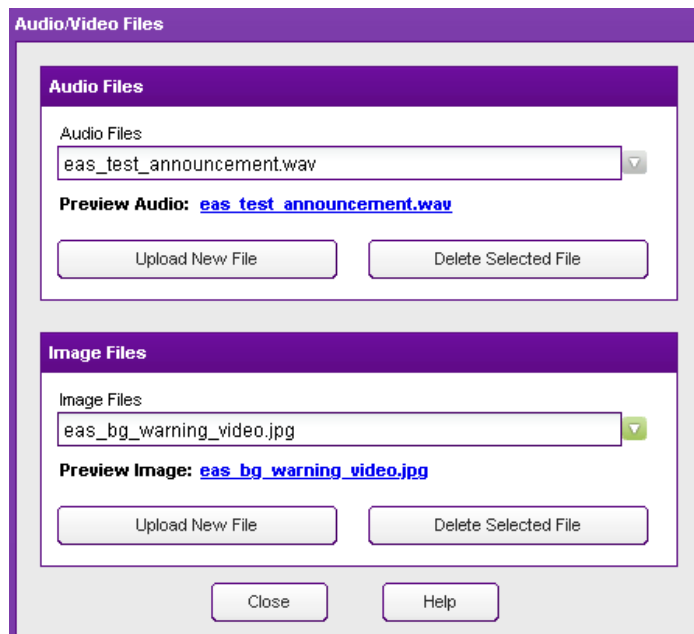
Certificate Files

To delete, load, and view certificate files, select the **Certificate Files** link. Web Server certificates, client certificates, and Certificate Authority certificates used to verify servers are maintained from this screen.

Certificate Files – This combo-box shows a list of the certificates that have been uploaded. Select a certificate to view its properties or to delete it.

View Certificate Information – Click this link to view information about the selected certificate.

Delete Certificate – Press this button to delete the selected certificate.

Type of Certificate to Upload

> **PEM (base-64) encoded X.509 Certificate** – Select this option if uploading a Certificate Authority public certificate or certificate chain, which is used for identity verification when connecting to external servers. The certificate must be a PEM (base-64) encoded file.

> **PKCS12 (PFX) Certificate with Private Key** – Select this option if uploading a certificate with a public/private key pair for use by the EASyCAP Web Server, or for connections that require a client certificate. The certificate must be a password protected PKCS#12 or PFX formatted file.

Certificate Password – Enter the password for the PKCS#12 or PFX file that will be uploaded.

Upload Certificate – Press this button to upload a certificate file. If it's a PKCS#12 or PFX file, make sure to enter the files password first. A **Certificate File Upload** window will be displayed. Press the **Browse** (or **Choose File**) button, select the certificate file, and then press the **Upload** button.

Close – Press this button to close the window.

Help – Press this button to view the Certificate Files section of the operational manual.

Hardware Settings

To setup fan control select the **Hardware Settings** link in the **Administration** folder.

Fan turn-on temperature – Select the temperature threshold that will turn on the case fans. This should be left at the default (35 C). If the EASyCAP is installed in a well ventilated office where fan noise needs to be minimized, a higher temperature can be configured.
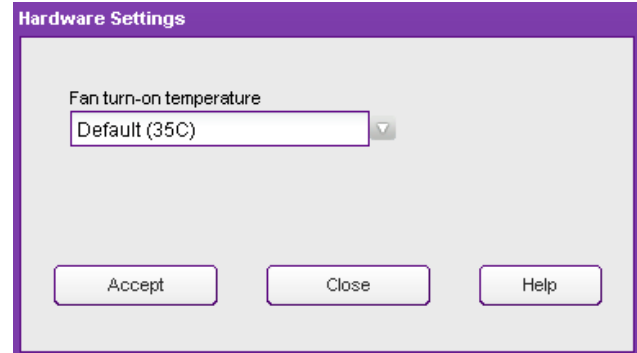
Select the **Accept** button to save changes to the configuration.

Select the **Close** button to discard changes and close the **Hardware Settings** screen.

Licensing

To view and add Licenses, select **Licensing** in the **Administration** folder.

All installed licenses will be displayed.

To add a license, contact EAS Customer Support and provide them with the EASyCAP serial number and the **Machine Key** shown on this screen. They will provide a **License Code**. Enter this code into the **License Code** field and click the **Add** button.

NOTE: Reboot the EASyCAP after adding a new license in order for the licensed feature to become available.
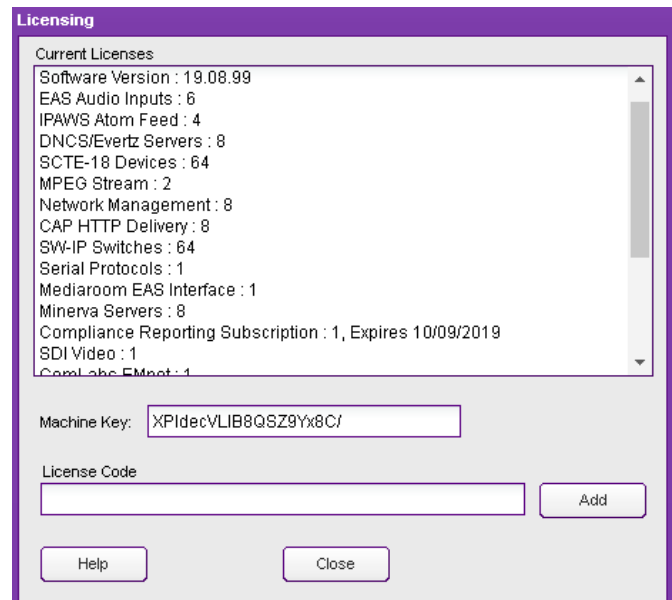
The EASyCAP serial number can be found by pressing the **Details** button in the lower right hand corner of the screen. An **About Viavi EASyCAP** window will be displayed. Click on the **System Info** tab to find the serial number.

Upgrade

To upgrade the EASyCAP software, select the **Upgrade** link in the **Administration** folder.

> **NOTE** ***You should enable SSH on one of the Network Interfaces during software upgrades. SSH can be used to troubleshoot and correct problems in case errors occur during the upgrade.***

Press the **Begin EASyCAP Upgrade** button to start the software upgrade. This will begin a step-by-step process to guide you through the upgrade.

The **Manual Upgrade** button is provided to manually copy the upgrade package file to the EASyCAP if there are issues with uploading it from a web browser.

The **Software Upload** screen is shown after beginning the upgrade. Press the **Browse** (or **Choose File**) button. An **Open** (or **File Upload**) dialog box will appear. Choose the upgrade file and press the **Open** button. Then press the **Upload** button to upload the file to the EASyCAP®.

After the file is uploaded, package information and instructions will be shown. Press the **Upgrade EASyCAP Firmware** button to install the upgrade or select the **Close** button to exit without upgrading.

After the upgrade has completed, you will be prompted to reboot the EASyCAP. Always reboot after installing an upgrade.

EASyCAP Encoder/Decoder User's Guide
Document 0010340001, Rev. 24.08   Aug 2024
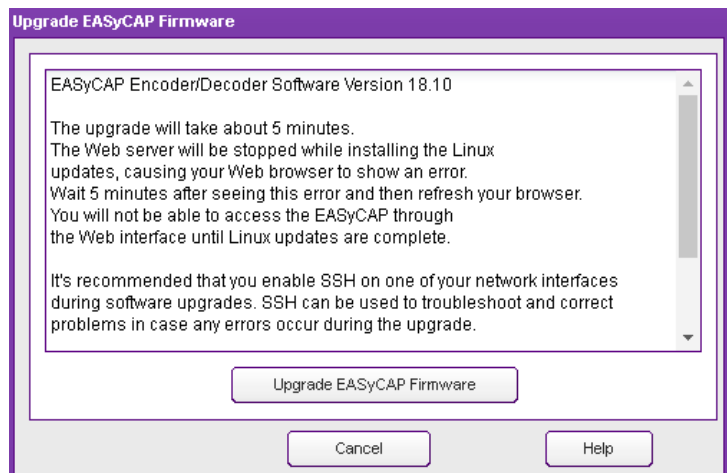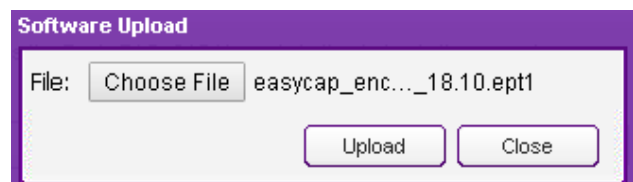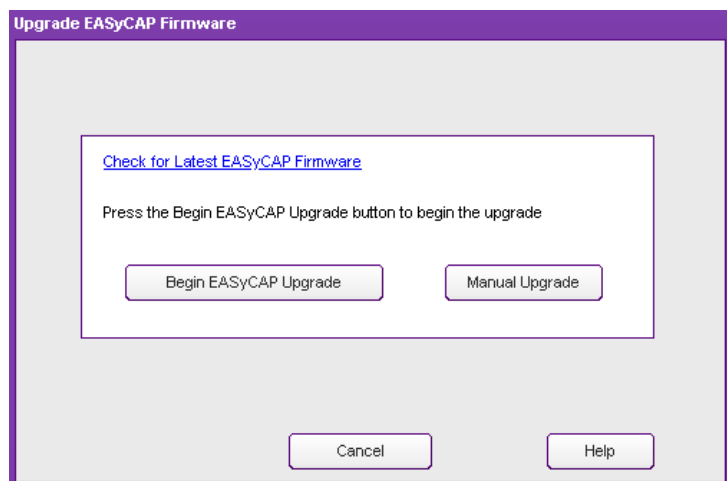
Reboot

To reboot the EASyCAP Encoder/Decoder, select **Reboot** in the Administration folder. The **Reboot** dialog box will appear. Click **Reboot** to restart the EASyCAP® Encoder/ Decoder. Click **Cancel** to exit without rebooting the EASyCAP Encoder/Decoder.

Reboot?

Are you sure you want to reboot the system?

Reboot   Cancel
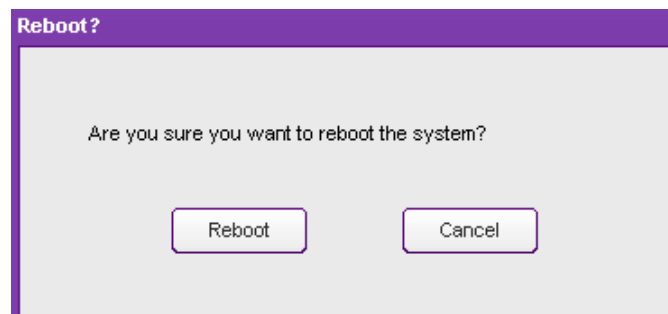
Configuration Folder

Expand the **Configuration** folder in the Navigation bar by clicking the **+** sign next to the **Configuration** folder.
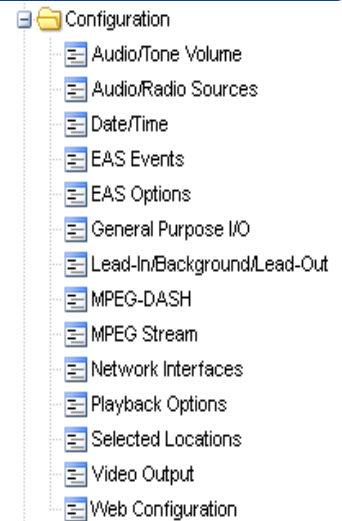
Audio/Tone Volume

To setup the Audio/Tone Volume for the Encoder/Decoder, click **Audio/Tone Volume**. The **Audio Volume Settings** window will appear.

Volume Settings

Speaker Volume – Enter the output volume of the front panel speaker and line output (0-100). The default is 80.

Master Volume – Enter the maximum possible output volume (0-100) of all EASyCAP® audio outputs, with the exception of the front panel speaker. The desired volume of the alert voice audio should be used in determining the Master Volume setting (default is 40).

The Attention tone includes an 853Hz tone and a 960Hz tone. These tones are additive and need be set to the same output amplitude.

853 Hz ATT Low Tone – Sets the volume (0-100) for the 853 Hz tone that's used to generate the Attention tone (The default is 80). This setting should be set to half the desired Attention tone volume and should be the same volume as the 960 Hz tone.

960 Hz ATT High Tone – Sets the volume (0-100) for the 960 Hz tone that's used to generate the Attention tone (The default is 80). This setting should be set to half the desired Attention tone volume and should be the same volume as the 853 Hz tone.
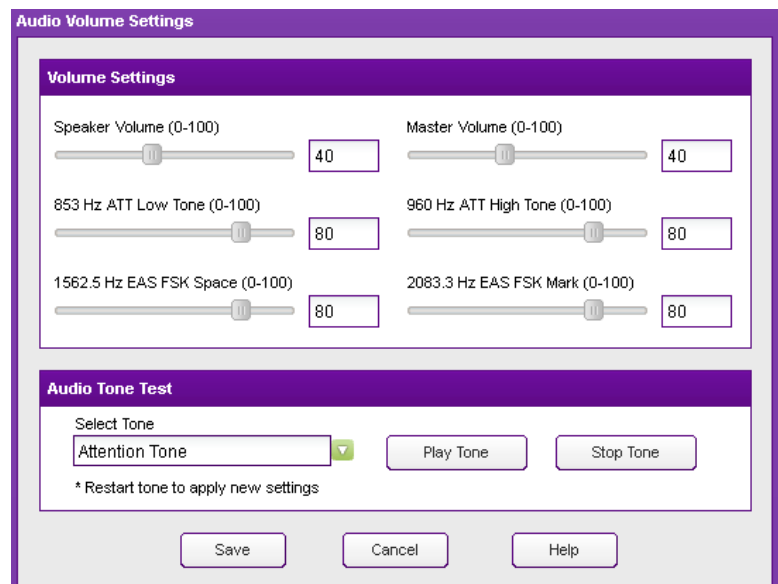
The generated EAS FSK uses 1562.5 Hz for its space frequency and 2083 Hz for its mark frequency. Theses tones are not additive, only one is used at a time. Set these two tones to the desired output amplitude, making sure they have the same amplitude.
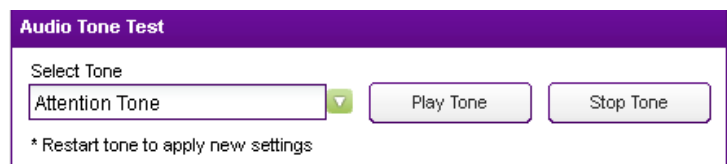
1562.5 Hz EAS FSK Space – Sets the volume (0-100) for the EAS FSK Space frequency (The default is 80). Set this to the desired volume of the generated EAS FSK and make sure its output amplitude is the same as the 2083 Hz tone.

2083 Hz EAS FSK Mark – Sets the volume (0-100) for the EAS FSK Mark frequency (The default is 80). Set this to the desired volume of the generated EAS FSK and make sure its output amplitude is the same as the 1562.5 Hz tone.

Audio Tone Test

The Audio Tone Test is provided to allow the operator to calibrate the generated tones and setup the EASyCAP® audio output levels to match the normal program audio volume. During the test, the selected tone will be generated at the configured volume. The audio will be present at all of the EASyCAP® audio outputs and the program audio switch will be activated.

Select Tone – Select the desired tone/output to test from the drop-down menu.

Master Volume – Used to setup and test the Master volume, a 1050 Hz tone will be generated at the configured Master volume.

Attention Tone – Used to setup and test the 853 Hz and 960 Hz tones. An Attention tone will be generated at the configured volumes for the 853 Hz and 960 Hz tones.

853 Hz (ATT Low Tone) – Used to setup and test the 853 Hz tone, an 853 Hz tone will be generated at the configured volume. This tone is combined with the 960 Hz tone to make the Attention Tone, and will therefore be at half the amplitude of the Attention Tone.

960 Hz (ATT High Tone) – Used to setup and test the 960 Hz tone, a 960 Hz tone will be generate at the configured volume. This tone is combined with the 853 Hz tone to make the Attention Tone, and will therefore be at half the amplitude of the Attention Tone.

1562.5 Hz (EAS FSK Space) – Used to setup and test the 1562.5 Hz tone (EAS FSK Space frequency). A 1562.5 Hz tone will be generate at the configured volume. The volume will be equivalent to the generated EAS FSK.

2083.3 Hz (FSK Mark) – Used to setup and test the 2083 Hz tone (EAS FSK Mark frequency). A 2083 Hz tone will be generate at the configured volume. The volume will be equivalent to the generated EAS FSK.

Play Tone – Click this button to begin the audio tone test.

Stop Tone – Click this button to stop the audio tone test. It will stop the tone and return the program audio switch to passing normal program audio.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

> **CAUTION**
>
> *Your normal program may be interrupted during the audio test. The program audio switch will be activated and the test tone will be present at all of the EASyCAP® audio outputs.*

> **NOTE**
>
> *Any changes made to volume settings while a test is playing will not be reflected in the test. The test must be stopped, and the Play Tone button clicked again to reflect those changes.*

Audio/Radios Sources

To configure the Audio Input Settings, click the **Audio/Radio Sources** link.

Audio Input Channel – Select which audio input to configure from the drop-down menu.

Audio Input Source

Audio Source – Select the audio input source from the dropdown menu as **Disabled**, an **External Audio Input** (analog audio), or an **Internal Radio Receiver**.

Source Name – Enter a descriptive name to identify the audio input. This name will be shown on the Front Panel LCD and in the Logs to identify the input channel. It's also used by the Compliance Reporting module to determine if this channel received all of the required EAS tests and messages.

Compliance Reporting – The Compliance Reporting module uses this setting to determine if the channel needs to be included in the compliance analysis. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

Disabled – This channel will not be analyzed for compliance.

Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week.

Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

Radio Settings

If the audio input is set to Internal Radio Receiver, the following Radio Settings apply:

Radio Band – Select the radio band (AM, FM, or NOAA) from the drop-down menu.

Station – Enter the frequency of the radio station.

Monitor and Test Audio

The operator can monitor the selected audio input and test the configured radio station by selecting the audio output(s) to use for monitoring the audio input.

Speaker – When checked, audio from the selected input will be routed to the front panel Speaker and the Line Output.

Audio Outputs – When checked, audio from the selected input will be routed to the Audio Outputs (the two balanced audio outputs available on the back panel of the EASyCAP®).

Audio Switch – When checked, the Program Audio switch will be activated, passing the audio from the selected input to the output terminals of the Audio Switch.

> **NOTE**
> ***Checking Audio Switch may interrupt your normal program audio.***

Test Audio Input Settings – Press this button to test the audio input settings. If a radio station is configured, it will tune to the selected station and pass the audio to the selected monitor output.

Preview Audio – This button allows you to monitor audio inputs remotely. Press this button to preview the last 15 seconds of audio from the selected audio source.

Accept – Press this button to save changes to the audio input settings and close the window.

Cancel – Press this button to discard changes made to the configuration and close the window.

Advanced – Press this button to view and edit the **Radio Receiver Signal Detection Settings** for the selected audio input.

> **NOTE**
> ***Only Audio Inputs that are configured will be monitored for EAS alerts.***

Radio Receiver Signal Detection Settings

The operator can adjust the signal detection parameters. These settings should normally be left at the defaults. The software will setup default parameters for each audio input based on its configuration and the type of installed radio board. Signal detection is used to show the status of the audio inputs on the front panel and the Web interface, as well as to send network management alarms. It will not affect the EAS monitoring of audio inputs.

Use Audio Peak Meter – When checked, a software peak meter is used to determine the presence of signal based on audio amplitude. This is the only signal detection that can be used for an external audio input. If enabled for a radio input, it will be used in addition to the signal strength indicator.

Use Received Signal Strength Indicator (RSSI) – When checked, the received signal strength of the configured radio station will be used to determine the presence of signal. This is not applicable for an external audio input. If the audio peak meter is also enabled, the RSSI and audio amplitude are both analyzed to determine the presence of signal.

Minimum RSSI Value – When configured to use RSSI, this sets the minimum RSSI value for determining if the signal is present. If the measured RSSI is lower than this value, the signal will be considered bad.

Check RSSI – Press this button to measure the RSSI of the selected input. The RSSI value will be displayed above the button.

Close – Press this button to close the **Radio Receiver Signal Detection Settings** screen.
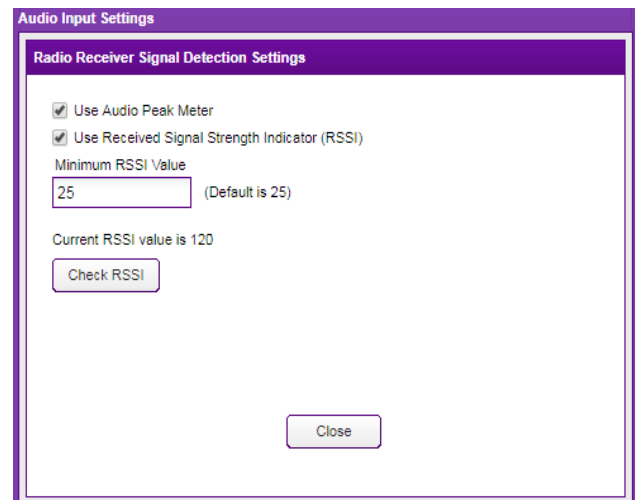
Date/Time

To configure the Date/Time Settings for the EASyCAP® Encoder/Decoder, click the **Date/Time** link from the **Configuration** folder.

The following settings can be adjusted:

NTP Servers – Enter the URL or IP address of the Network Time Protocol servers. Click **Set NTP Servers** to save the changes.

Use Aggressive Time Correction – When enabled, time correction occurs within seconds of the EASyCAP powering up and checks for time corrections more frequently than when the option is disabled.

Time Zone – Select the time zone from the dropdown list. Click **Set Time Zone** to save the changes to the time zone.

Date & Time Settings
NTP Servers
0.us.pool.ntp.org · 1.us.pool.ntp.org
2.us.pool.ntp.org · 3.us.pool.ntp.org
☑ Use Aggressive Time Correction · Set NTP Servers
Time Zone
Eastern · Set Time Zone
Date & Time
Month: October · Day: 18 · Year: 2018
Hour: 11 · Minute: 26 · Set Date/Time
Close · Help

Month – Select the current month from the dropdown list.

Day – Select the current day from the dropdown list.
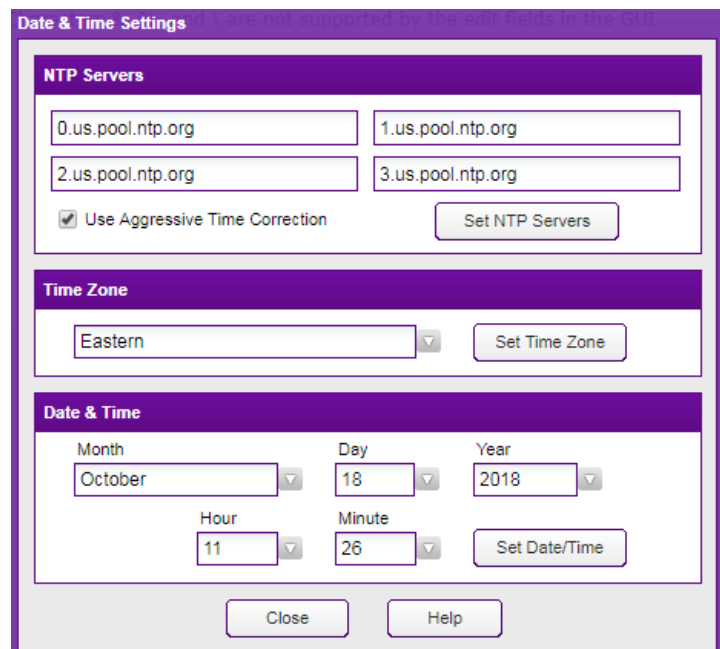
Year – Select the current year from the dropdown list.

Hour – Select the current hour from the dropdown list.

Minute – Select the current minute from the dropdown list.

Set Date/Time – Click the **Set Date/Time** button to apply the date and time settings.

Click **Close** when you have made all necessary adjustments.

> **NOTE**
>
> *During initial configuration time and date should be set manually. Afterwards, if an NTP server is configured the date and time will automatically synchronize with the NTP server.*

> **NOTE**
>
> *If the time changes more than 15 minutes, the session will timeout and you will need to log back into the Web interface.*

EAS Events

To configure EAS Events for the Encoder/Decoder, select the **EAS Events** link.

Click an event in the list to View and Edit its settings. The settings will be displayed in the **Event Settings** box on the right side of the window.

- **Enable Event** – Select this checkbox to enable the event. If the event is not enabled, the log will show when this type of event is received, but it will not be transmitted. The event can be manually generated regardless of whether it's enabled. Always enable the EAN.

- **Process as a Live Event** – Select this option to treat this event as a live message (similar to an EAN). If enabled, the alert will be transmitted immediately after receiving the EAS Header and waiting a short time for the Attention Tone. The voice message will not be recorded before transmission begins. An EAN is always treated as a live event.

- **DNCS/Evertz configured as a force-tune** – Select this option to treat this event as a force-tune when notifying DNCS/Evertz equipment. The audio file will not be delivered and termination messages will be delivered to end the force-tune. This option needs to be enabled for live events.

> ⚠ **CAUTION**
>
> *Live events may include part of the received Attention Tone in the transmitted voice message.*

> ⚠ **CAUTION**
>
> *Live events will not have an audio file available for delivery to downstream equipment, which may prevent some equipment from presenting the event properly.*

- **SCTE-18 Priority** – Select the priority from the dropdown menu. This priority will be included in messages delivered to SCTE-18 recipients.

- **Event Type** – Select the type of event from the dropdown menu. The event type is used by some equipment to display different colors during message playback.

Broadcast Application Only

- **Manual Mode Delay (Broadcast Application only)** – Select the number of minutes to delay from the dropdown menu. When the Encoder/Decoder is in Manual mode, the alert playback will be delayed this amount of time, allowing the operator or automation equipment to confirm and begin the message playback. If the event is set to Indefinite, it will be allowed to expire while waiting for confirmation, otherwise the event will automatically begin playback if it is not confirmed or cancelled within the delay time. Note that the alert playback will automatically begin before the event expires regardless of the configured delay, unless it is set to Indefinite.

Options for an EAN Event Only

Two additional options are shown for the EAN event.

- **Activate All Equipment** – All downstream equipment will be activated, regardless of the configured location routing.

- **Require PEP Originator Code** – When enabled, an EAN will only be accepted if the Originator code is "PEP" (the EAN must be originated by a Primary Entry Point System).

An option to **Prevent Multiple Tests** is available for Required Monthly Test and Required Weekly Test events (see testing rules in 47CFR11.61).

For a monthly test, the **Prevent Multiple Tests** option can be configured to prevent multiple RMT's from being transmitted during the month, where a month is considered to be midnight of the first day of the month until 11:59:59 of the last day of the month.

- **Disabled** – Don't prevent multiple monthly tests.

- **RMT has been sent** – Do not retransmit a received monthly test if an RMT was already transmitted during the month.

- **Any Alert with voice has been sent** – Do not retransmit a received monthly test if an alert that includes an attention tone and voice message was already transmitted during the month.

For a weekly test, the **Prevent Multiple Tests** option can be configured to prevent multiple RWT's from being transmitted during the week, where a week is considered to be Sunday at midnight until Saturday at 11:59:59.

- **Disabled** – Don't prevent multiple weekly tests.

- **RWT has been sent** – Do not retransmit a received weekly test if an RWT was already transmitted during the week.

- **RWT or RMT has been sent** – Do not retransmit a received weekly test if an RWT or an RMT was already transmitted during the week.

- **Any Alert has been sent** – Do not retransmit a received weekly test if an alert was already transmitted during the week.

Press the **Accept** button to save changes to the EAS Events configuration, or press the **Close** button to exit without saving changes.

EAS Options

To configure EAS Settings of the Encoder/Decoder, select the **EAS Options** link in the **Configuration** folder. The **EAS Settings** window will be displayed.

EAS Settings

- **EAS Originator** – Select the appropriate originator code for your system, this is normally set to "EAS Participant."

- **Station ID** – Enter your station identification or call letters (up to 8 characters).

- **Check for CAP alerts** – Enter the number of seconds to wait before checking for a CAP version of a legacy EAS message. When a legacy EAS message is received from an audio input, the software will wait this many seconds and then poll IPAWS for a CAP version of the message. If a CAP version of the message is avaialble, it will be retransmitted rather than the legacy EAS message.

- **Wait for CAP alerts to be downloaded** – Enter the number of seconds to wait for CAP messages to be downloaded after receiving a legacy EAS message. When the software checks for a CAP version of a legacy EAS message, it will wait this many seconds for the CAP poll to complete. If CAP messages can't be downloaded within this time, the legacy EAS message will be retransmitted. Polling CAP feeds is normally a quick process, but occasionally network delays occur and this setting ensures that there are not significant delays in retransmitting alerts.

- **Time to Wait for EOM** – Enter the number of seconds to wait for an EOM after EAS Header Text has been received (120-240 seconds). This should be left at the default 150 seconds. The software will account for additional time required for EAS FSK and Attention tone. Note that the audio voice message will always be truncated to 2 minutes regardless of this setting (to prevent problems with downstream equipment).

- **Transmit alerts that timed out while waiting for an EOM** – Enable this option to transmit alerts that timed out while waiting for an EOM. This setting defaults to disabled, which will discard alerts that timed out while waiting for an EOM.

RWT Locations

Locations for Locally Generated Required Weekly Tests – Select the locations that are included in locally generated Required Weekly Tests. This includes weekly tests that are randomly generated and originated from the front panel or telephone interface.

EASyCAP Encoder/Decoder User's Guide

Random RWT

Settings to configure automatic generation of Required Weekly Tests. It's preferred that you manually generate a weekly test once a week, on a different day and at a different time, so that you can confirm that it activates your system correctly. If this is not practical, you can setup the EASyCAP® to automatically generate weekly tests at random times.

Enable or disable Random Weekly Tests using the combo box at the top of the screen. The following options are available.

- **Disable Random Weekly Tests** - Disable automatic weekly tests.

- **Enable Random Weekly Tests using a weekly schedule** - Enable automatic weekly tests. A configured span of days and hours is used to determine the times when weekly tests can be generated.

  - Select the span of days using the **From Day** and **To Day** combo boxes. A span of at least two days must be configured.

  - Two time slots can be configured using the **Enable Time Slot 1/2** checkboxes and the **from**/**to** hour combo boxes. A span of at least 2 hours is required.

- **Enable Random Weekly Tests using a daily schedule** - Enable automatic weekly tests. Two time slots per day can be setup as allowable times to generate the tests.

  - Using the **From Day** combo box, select each day that weekly tests can be generated and then setup the hours for that day using the **Enable Time Slot 1/2** checkboxes and the **from**/**to** hour combo boxes. At least two days must be configured with a span of at least 2 hours for each day.

Current settings for random weekly tests - This text box shows the configuration for random weekly tests. It's updated as settings are changed.

Settings for a Broadcast application

Automatic/Manual Mode – Select the mode of operation from the dropdown menu.

> **Automatic Mode** – Alerts are automatically forwarded when they're received. Select this option if you want to automatically forward alerts as they're received or if the system is not manned.
>
> **Manual Mode** – When an alert is received, the EASyCAP® will wait for operator confirmation before beginning the alert playback. The amount of time to wait is configured per event on the EAS Events screen. This should only be selected if the station is manned or automation equipment is connected and configured to confirm the alert playback.
>
> **Scheduled** – Automatically switches between Automatic and Manual mode per the configured schedule.

Manned days and hours – Provides the ability to setup a schedule for when the EASyCAP® runs in Manual mode. This is configured by selecting the day and the hours that the station is manned. Two shifts can be configured per day.

Current settings for automatic/manual mode - This text box shows the automatic/ manual mode configuration. It's updated as settings are changed.

General Purpose I/O Settings

To configure the functions and timing used by the general purpose inputs and outputs, select the **General Purpose IO** link from the **Configuration** folder.

General Purpose Inputs Tab

- **Abort Alert Function** – Select the general purpose input used to abort alert message playback. The default setting is GPI-1. When this input is closed (shorted), any EAS message in progress will be stopped. The EASyCAP will attempt to stop all video and audio replacement equipment and then return to monitoring for incoming alert messages. This input is edge-triggered. Holding it closed will not continuously abort messages.

- **Generate RWT Function** – Select the general purpose input used to generate a Required Weekly Test. The default setting for this function is None. This input is edge-triggered. Holding it closed will not continuously generate Required Weekly Tests.
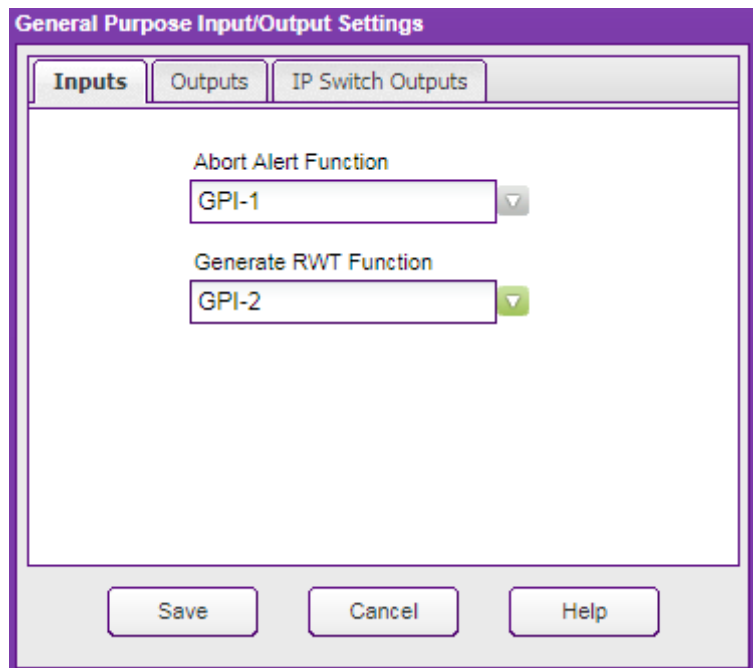
The following two functions are only available for Broadcast applications and will not be available for Cable or IPTV applications.

- **Trigger Alert Playback Function** – Select the general purpose input used to trigger a pending alert message that's waiting for confirmation. This input is only used when the EASyCAP is in manual mode. When an alert message is ready for transmission, it will wait for user confirmation. When this input is closed (shorted), it causes the pending EAS message to begin transmission, regardless of the state of the hold-off input. This input is edge-triggered. Holding it closed will not continuously trigger messages.

- **Hold-off Alert Playback Function** – Select the general purpose input used to hold off alert message playback. This input is only used when the EASyCAP is in manual mode. It is normally used by automation equipment to hold off alert message playback. When closed (shorted), this input will prohibit pending EAS messages from transmitting. When the input is opened, pending EAS messages will begin transmission, regardless of the state of the Trigger Alert GPI.

EASyCAP Encoder/Decoder User's Guide

> **NOTE** *Only one function can be assigned to a general purpose input.*

General Purpose Outputs Tab

- **General Purpose Output 1** – Select the function for General Purpose Output 1.

- **General Purpose Output 2** – Select the function for General Purpose Output 2.

- **General Purpose Output 3** – Select the function for General Purpose Output 3.

- **General Purpose Output 4** – Select the function for General Purpose Output 4.

| Inputs | **Outputs** | IP Switch Outputs |

General Purpose Output 1
Transmitting Audio

General Purpose Output 2
Transmitting

General Purpose Output 3
Time Adjusted

General Purpose Output 4
Live Event Active

General Purpose Output 5
None

General Purpose Output 6
None

TTL 1 will follow Output 1 and TTL 2 will follow Output 2

- **General Purpose Output 5** – Select the function for General Purpose Output 5. Note that this output is not available for Series 30 hardware.

- **General Purpose Output 6** – Select the function for General Purpose Output 6. Note that this output is not available for Series 30 hardware.

Available General Purpose Outputs Functions

- **Alert Ready –** Activates when an alert has been received and is waiting for operator confirmation before being transmitted.

- **Transmitting Audio –** Activates when alert audio playback is in progress. This is used to activate audio distribution and routing equipment during EAS activations in order to replace the normal program audio with the alert audio.

- **Transmitting** – Activates when alert playback is in progress (audio and video). This is used to activate audio and video distribution and routing equipment during EAS activations in order to replace the normal program audio and video with the alert information.

- **Live Event Active –** Activates when an EAN or a Live Event is in progress.

- **Time Adjusted** – Activates a configurable number of seconds before or after the alert audio and video playback begins and deactivates a configurable number of seconds before or after the alert playback ends. It is used to trigger equipment that requires time to acquire the EAS audio/video, create an MPEG stream, or send commands across a network.

> **NOTE** *The timing for Time Adjusted outputs is configured from the Configuration/Playback Options window.*

IP Switch Outputs Tab

The functions assigned to the IP Switch outputs will apply to all configured IP switches. Note that some supported IP switches only provide three outputs.

- **Output 1 –** Select the function for IP Switch Output 1.

- **Output 2 –** Select the function for IP Switch Output 2.

- **Output 3 –** Select the function for IP Switch Output 3.

- **Output 4 –** Select the function for IP Switch Output 4.

- **Output 5 –** Select the function for IP Switch Output 5.

- **Output 6 –** Select the function for IP Switch Output 6.

- **Output 7 –** Select the function for IP Switch Output 7.

- **Output 8 –** Select the function for IP Switch Output 8.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

Lead-In/Background/Lead-Out

Background images can be configured for each type of event and video output.

Audio, images, and text can be setup for lead-in and lead-out messages, which are presented before and after each type of event. Note that a license is required for the lead-in and lead-out messages.

The software will determine which background image and lead-in/lead-out message to use based on the following order of precedence:

1. Media is configured for the specific event (ie. Tornado Warning)
2. Media is configured for the severity of the event (ie. Warning)
3. Default media is configured

> **NOTE**
>
> ***Audio and image files can be loaded and deleted from the Administration | Audio/Video Files screen.***

- **Event Type** – Select the type of event to configure. The **Default** event settings are used when the specific event or severity is not configured.

- **Enable Lead-In** – Enable or disable all configured lead-in messages.

- **Enable Lead-Out** – Enable or disable all configured lead-out messages.

Setup the background image to show during an alert message

1. Select the event or severity from the **Event Type** combo box.

2. Select the **Message** tab.

3. Select the desired video output tab.
   Note that each video output used will need to be configured.

4. Select an image from the **Select Image** combo box.

- A **Preview Image** link will be shown below the combo box to allow the configured image to be viewed from your web browser.

Setup the media to present during lead-in and lead-out messages

1. Select the event or severity from the **Event Type** combo box.

2. Select the **Lead-In** or **Lead-Out** tab.

3. Select the desired video output tab. Note that each video output used will need to be configured.

4. Select an image from the **Select Image** combo box.

   • A **Preview Image** link will be shown below the combo box to allow the configured image to be viewed from your web browser.

5. Select the desired language tab. Note that each language used will need to be configured.

6. Select an audio file from the **Select Audio** combo box.

   • A **Preview Audio** link will be shown below the combo box to allow you to listen to the configured audio from your web browser.

7. Enter the minimum duration (in seconds) to show the lead-in/lead-out message. Note that the duration will be longer if the configured audio duration is longer.

8. Enter the text to display during the lead-in or lead-out message.

Click **Save** to save configuration changes, or click **Cancel** to exit without saving changes.

MPEG-DASH

The EASyCAP can provide MPEG-DASH HTTP Streaming media. Live and VOD profiles are supported. The streaming media can be used by Middleware and smart devices for presenting the alert messages audio and video.
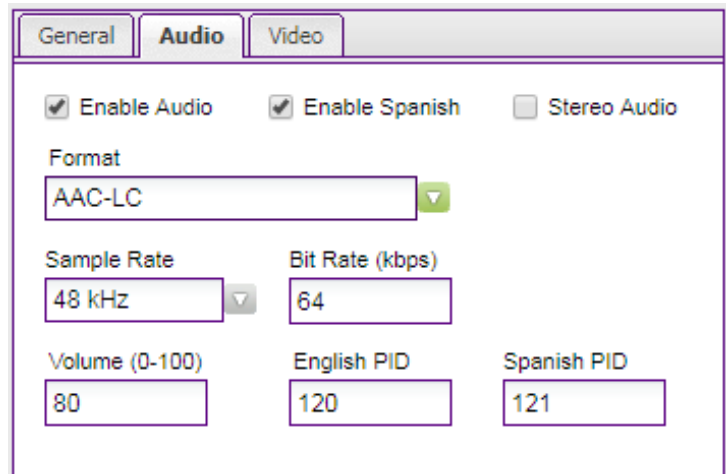
General Tab

- **Enable MPEG-DASH** – Enable or disable the MPEG-DASH media.

- **Require HTTPS Access** – If enabled, a secure connection (HTTPS) must be used to access the MPEG-DASH media.

- **Use Common Intermediate Format (CIF)** – If enabled, the Common Intermediate Format (CIF) will be used to produce the DASH manifest.

- **Use MPEG-2 Transport Stream Segments** – If enabled, the DASH media segments will use an MPEG-2 Transport Stream container. If disabled, the DASH segments will use an ISO BMFF container.

- **Manifest Name** – Enter the name that will be used for the DASH manifest. The default is "manifest.mpd".

- **Segment Duration** – Enter the duration for the DASH segments in seconds. The EASyCAP® will attempt to use the configured duration, however it will ensure that segments start with an I-Frame (or random access point). The allowable segment duration range is 2-10 seconds.

- **Address** – Enter the address of the EASyCAP hosting the DASH manifest. The URL must start with "http://" or "https://". For example: http://easycap.viavi.net.
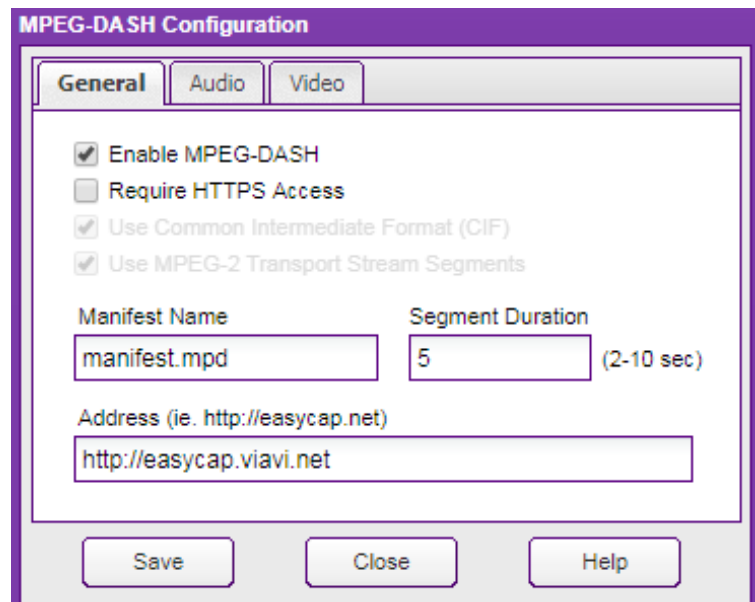
Audio

- **Enable Audio** – Enable or disable the HTTP stream audio.

- **Enable Spanish** – Enable Spanish audio media. When enabled, a separate Spanish manifest (and media) will be produced.

- **Stereo Audio** – If enabled, the audio will be stereo. If disabled, the audio will be mono.

- **Format** – Select the audio format. Allowable formats are: AAC-LC, AAC-HEv1, and AAC-HEv2.

- **Sample Rate** – Enter the audio sample rate (8000-48000 Hz).

- **Bit Rate** – Enter the audio bitrate in kbps (16-256 kbps).

- **Volume** – Enter the volume for the audio (0 to 100). The default is 80.

- **English PID** – Enter the PID for the English audio.

- **Spanish PID** – Enter the PID for the Spanish audio.

Video

- **Enable Video** – Enable or disable the HTTP stream H.264 video.

- **Enable Spanish Video** – Enable Spanish video media. When enabled, a separate Spanish manifest (and media) will be produced.

- **Show Event Text** – If enabled, the title and event name will be shown at the top of the video. The title is configured on the **Video Out** screen.

- **Show Text Outline** – If enabled, text will include a dark outline around the characters.

- **Profile** – Select the video profile.

- **Width** – Enter the video width (200-900).

- **Height** – Enter the video height (150-600).

- **Frame Rate** – Select the video frame rate (23.976-30, interlaced or progressive).

- **I-Frame Interval** – Enter the distance between I-Frames (every 1 to 10 seconds).

- **Maximum Bit Rate** – Enter the maximum video bitrate in kbps (30-8000).

- **Minimum Bit Rate** – Enter the minimum video bitrate in kbps (30-8000).

- **English PID** – Enter the PID for the English video.

- **Spanish PID** – Enter the PID for the Spanish Video.

Click **Save** to save configuration changes, or click **Close** to exit without saving changes.

MPEG Stream

The EASyCAP can stream MPEG-2 from any of the built-in Ethernet ports. Two simultaneous streams are supported, and the first stream can be duplicated to a different address or physical interface. The MPEG audio and video is encapsulated in RTP or an MPEG-2 transport stream and can be delivered to a unicast or multicast address. The MPEG stream can be used to create an "EAS Details" channel, eliminating the need for an external MPEG encoder.

Select MPEG Stream – Select the MPEG stream to view or edit. Two streams can be configured, depending on the installed MPEG license.

Pre-Roll – The stream will start this many seconds before EASyCAP begins playback. It is provided to help compensate for synchronization of the MPEG display due to processing or grooming delays.

MPEG Stream

- **Address** – Enter the unicast or multicast address for the MPEG stream.

- **Port** – Enter the UDP port for the MPEG stream.

- **Multicast TTL** – Enter the time-to-live for the MPEG stream.

- **Interface** – Select the Ethernet interface to use for the MPEG stream. When set to "Default", network settings will determine which interface to use.

- **Network ID** – Enter the original network ID of the transport stream.

- **Program Map ID** – Enter the program map PID.

- **Program Number** – Enter the program number.

- **Transport Stream ID** – Enter the transport stream ID.

- **Enable Null Packet Stuffing** – When enabled, null packets are inserted into the stream to maintain a constant bitrate..

- **Use RTP Protocol** – Enable this option to use RTP rather than an MPEG-2 transport stream.

- **Stream Alerts Only** – When enabled the MPEG stream is only present during the playback of EAS messages. When disabled the MPEG stream will always be present.

Duplicate Stream

- **Enable Duplicate Stream** – Enable a duplicate stream that can be configured for a different address, port, or physical interface.

- **Address** – Enter the unicast or multicast address for the duplicated stream.

- **Port** – Enter the UDP port for the duplicated stream

- **Interface** – Select the Ethernet interface to use for the uplicated stream. When set to "Default", network settings will determine which interface to use.
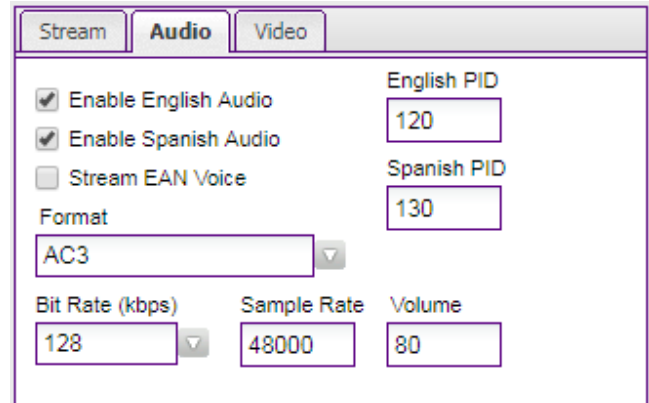
> ⚠️ **CAUTION**
>
> ***The address, port, or interface of the duplicate stream must be different than the primary MPEG stream.***

Audio

- **Enable Audio** – Enable or disable audio for the MPEG stream.

- **Enable Spanish Audio** – Enable/disable streaming Spanish audio in the event a Spanish voice message is included with the EAS/CAP message.

- **Stream EAN Voice** – Enable/disable streaming the EAN voice message. If this option is disabled, only the FSK and attention tone audio will be streamed for an EAN.

- **Format** – Select the audio stream format as MP2, MP3, AAC, or AC3.

- **Bit Rate** – Select the audio stream bitrate.

- **Sample Rate** – Enter the sample rate for the audio (8000-48000 Hz).

> 📝 **NOTE** *If the bit rate is set to 16 kbps, the sample rate must be 8000 Hz.*

- **Volume** – Enter the volume for the audio (0 to 100). The default is 80.

- **English PID** – Enter the PID for the English audio.

- **Spanish PID** – Enter the PID for the Spanish audio.

> ⚠️ **CAUTION** *If using Mediaroom:*
> *Stream 1 must be used for the audio stream that's used for the Mediaroom interface.*

Video

- **Enable Video** – Enable or disable MPEG video for the MPEG stream.

- **Enable Video for EAN** – Enable/disable video for an EAN. If video is disabled, this option provides the ability to stream video only for an EAN, which can be useful for systems that must force-tune to another channel during an EAN.

- **Format** – Select the video format.

- **Language** – Select the text language that's used to generate the video (English, Spanish, English followed by Spanish).

- **Width** – The width of the video.

- **Height** – The height of the video.

- **Frame Rate** – Select the video frame rate (29.97, 30, or 60, interlaced or progressive).

> **NOTE**
> ***Common Standard Definition Settings:***
> ***Width x Height: 640x480, 704x480, or 720x480***
> ***Frame Rate: Interlaced 29.97 FPS or Progressive 30 FPS***

> **NOTE**
> ***Common High Definition Settings:***
> ***720p: 720x1280 Progressive 60 FPS***
> ***1080i: 1080x1920 Interlaced 60 FPS***

- **PID** – Enter the PID for the video.

MPEG-2 video and compression options:

- **Bit Rate** – Enter the video bitrate in kbps.

- **GOP Distance** – Enter the distance between reference frames (I or P). For example, a distance of 3 would result in 2 B frames between reference frames. The default is 3.

- **GOP Length** – Enter the distance between I frames (1-30, 30 is the default).

Press the **Save** button to save changes or the **Close** button to exit without saving.

Network Configuration

> **CAUTION**
> *Regardless of the network settings of the EASyCAP® Encoder/Decoder, a properly fire walled connection to the Internet is critical for the safe operation of this equipment. In addition, use of a reputable Internet provider and DNS Service may minimize risks associated with Internet access.*

> **CAUTION**
> *Hand editing the interfaces file may result in failure of the SSH and the Web interfaces. Use the Web Interfaces or front panel menu to change your network settings.*

> **NOTE**
> *Ethernet 1 and 2 are 1000 BASE-T ports.*
> *Ethernet 3 and 4 are 100 BASE-T ports (on an optional board).*
> *Use ports 1 and 2 for multicast and high bandwidth traffic.*

> **NOTE**
> *Ethernet ports 1-4 are equivalent to Linux devices eth0 - eth3. If an interface is referenced in an IProute command or script, make sure to use eth0 for Ethernet 1, eth1 for Ethernet 2, etc.*

The EASyCAP® ships from the factory with the following network settings.

- Ethernet 1 is set to IP address 10.1.65.103 with a Subnet mask of 255.255.0.0.
- Ethernet 2 is set to IP address 192.168.1.102 with a Subnet mask of 255.255.255.0.
- Ethernet 3 is set to IP address 192.168.2.102 with a Subnet mask of 255.255.255.0.
- Ethernet 4 is set to IP address 192.168.3.102 with a Subnet mask of 255.255.255.0.
- HTTP, HTTPS, and SSH is enabled on both ports.

To setup the network settings for the EASyCAP®, select the **Network Interfaces** link.

The EASyCAP® Encoder/Decoder must be configured for network connectivity that allows Internet access to retrieve CAP messages and access to downstream equipment that is required to deliver alerts to subscribers. Additionally, management of the EASyCAP® Encoder/Decoder is provided by a Web Server, so inbound connections on port 443 and/or port 80 will be necessary.

Single Network Connection – The EASyCAP® Encoder/Decoder may be configured with only one Ethernet port enabled, relying on the system network for all connections to the Internet, required equipment, and web client (for management). In this configuration, the internal network is responsible for any necessary routing and security. In a very simple network of this kind, a router/gateway would allow outbound connectivity to the Internet while other equipment and a web client (PC) would be on the same IP subnet as the EASyCAP® Encoder/Decoder and therefore directly accessible.

Dual Network Connection – The EASyCAP® Encoder/Decoder may be configured with two Ethernet interfaces enabled allowing (typically) one interface to be used to access the Internet, while the other interface is used to access equipment and a web client (for management). In this configuration one interface may be configured with a default gateway pointing to an Internet router, while the other interface is either on the same subnet with the required equipment, or is configured with a (narrow) gateway to the equipment.

Two additional Ethernet interfaces can be added by installing an optional communications expansion board. These ports can be used to allow the Encoder/Decoder access to additional networks. These ports are 10/100 BaseT and should be used for connections that do not require high speeds.
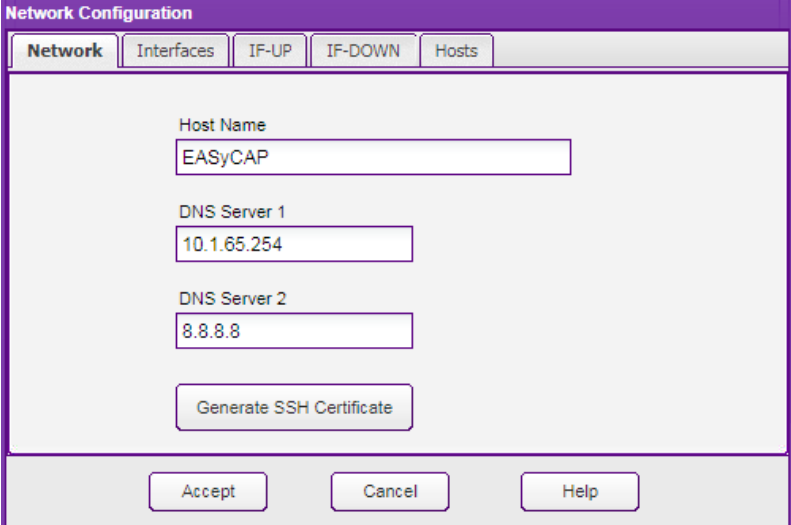
Network Tab

Host Name – Enter the host name of the EASyCAP® Encoder/Decoder in this field.

DNS Server 1 – Enter the primary DNS server address in this field.

DNS Server 2 – Enter the secondary DNS server address in this field.

Generate SSH Certificate – Generate a new certificate for the SSH interface.

Interfaces Tab

Interface – Select the network interface to view or edit from this drop-down menu.

Disable Interface – Select this checkbox to disable the selected network interface.

Use DHCP – Select this checkbox to allow DHCP to automatically assign the address, subnet mask, and gateway to the selected network interface.

> ⚠️ **CAUTION**
>
> ***Use of DHCP on any interface may result in IP and gateway conflicts with the other interface, DNS conflicts, and other conflicts and ambiguities resulting in unreliable communication on both interfaces. Also, use of DHCP will enable the configuration HTTPS interface on all interfaces, regardless of the Allow Web Server settings for the interfaces.***

Allow Web Server – Select this option to allow access to the Web Server from the selected network interface.

Allow SSH – Select this option to allow SSH access from the selected network interface.

IP Address – Enter the IP address for the selected interface.

Subnet Mask – Enter the subnet mask for the selected interface. Together with the IP address, this determines the subnet of the interface.

MAC Address – The MAC address of the selected network interface.

Disable Gateway – Disables the Gateway and Network Mask settings.

Default Gateway – Sets the Gateway to the widest possible network mask, making it the default when no narrower network exists on any interface.

> ⚠️ **CAUTION**
>
> ***Enabling a default gateway on more than one interface will result in unreliable communications.***

Gateway – Enter the address of the router used to communicate with IP addresses that are not on the selected interfaces subnet, but are within the interfaces network. The **Gateway** IP address must be on the selected interfaces subnet.

Network Mask – Applying the **Network Mask** to the **Gateway** address will determine which addresses are routed through the **Gateway**. This determines the address range of the network in a manner similar to the way a Subnet Mask and IP Address determines what addresses are on the subnet.

Multicast Start Address and **Multicast Mask** – Enter the start address and mask for the multicast addresses that should be routed through the selected interface.

Default Multicast Address – Select this option to use the selected interface for multicast traffic that is outside of the multicast address range configured on other interfaces.

No Special Configuration – Select this option to disable any special configuration for multicast addresses on the selected interface.

IF-UP Tab

Custom IF-UP Script – This script provides a means for experienced users to hand-edit routes when a given interface is brought online. The $IFACE variable identifies the interface (eth0 or eth1). For example:
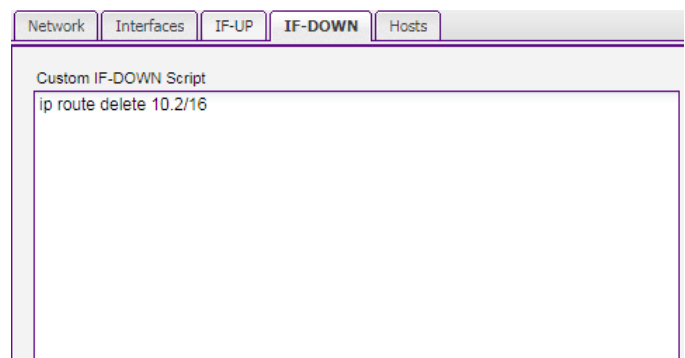
if ["$IFACE" = eth0]; then
  ip addr add 10.2.10.5/24 brd + dev eth0
if

IF-DOWN Tab

Custom IF-DOWN Script – This script allows re-routing or removal of routes when an interface is going offline. The $IFACE variable identifies the interface going offline.

> **NOTE** *The IProute2 Utility Suite (IP command) is recommended for IF-UP and IF-Down scripts.*

Hosts Tab

Additions to hosts file – Enter any additional lines required in the hosts file. Do not enter lines for the hostname and localhost, this information will be added automatically.

Select the **Accept** button to save the network configuration.

Select the **Close** button to exit without saving changes to the configuration.

> **NOTE** *If the EASyCAP IP address changed, you will need to close and then reopen your browser to login to the EASyCAP at the new IP Address.*

Playback Options

To setup audio, text, and timing options, select the **Playback Options** link from the **Configuration** folder.

Message Playback Settings

- **Pad Beginning** – Enter the number of seconds to pad the start of playback. This adds silence to the beginning of audio and a static display to the video.

- **Pad Ending** – Enter the number of seconds to pad the end of playback, appending silence to the audio and a static display to the video.

- **Wait *n* seconds between messages** – Enter the number of seconds to wait between ending one message and starting the next message.

Force-tune Timing

These timing adjustments are provided for synchronization with systems that require time to encode MPEG streams and/or deliver downstream force-tune messages. For example, systems that use SCTE-18 messages to cause Set-tops to force-tune to an alternate channel.

- **Start Adjustment** – Enter the number of seconds to adjust delivery of messages to downstream equipment. A negative value causes force-tune messages to be sent before the EASyCAP® begins playback (static analog video is displayed and analog audio is silent before messages are sent). A positive value causes them to be sent after playback begins.

- **End Adjustment** – Enter the number of seconds to adjust the ending of messages delivered to downstream equipment. A negative value causes downstream messages to end before the EASyCAP® ends playback, and a positive value causes messages to end after playback has ended.

General Purpose Outputs Timing

These timing adjustments are not applicable to Broadcast applications. They only apply to the **Time Adjusted** general purpose outputs. The adjustments are provided for synchronization with systems that require time to encode MPEG streams and/or deliver downstream messages, such as with an OM-1000.

- **Start Adjustment** – Enter the number of seconds to adjust activation of **Time Adjusted** outputs. A negative value activates outputs before the EASyCAP® begins playback (static analog video is displayed and analog audio is silent before activation). A positive value activates outputs after playback begins.

- **End Adjustment** – Enter the number of seconds to adjust the deactivation of **Time Adjusted** outputs. A negative value deactivates outputs before the EASyCAP® ends playback, and a positive value deactivates outputs after playback has ended.

Audio/Text Options

- **Local Audio Playback** – Select the language for the audio played through the EASyCAP onboard audio outputs and audio switches. If this is set to **Disabled**, no audio will be played through the onboard audio outputs.

- **Use Text-to-Speech if audio is missing** – When this box is selected, the EASyCAP® will generate speech from the text included in the alert message. Text-to-speech will only be generated if the message does not include audio.

- **Use Short RWT Text** – When selected, a short message will be used for Required Weekly Tests. For example: "A Required Weekly Test has been issued by an EAS Participant".

- **Include Station ID** – When selected, your station identification (or Call Sign) will be included at the end of the alert text.

- **Disable Local General Purpose I/O** – When selected, the EASyCAP onboard general purpose outputs will not be used (they will never be activated).

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

Selected Locations

The **Location Configuration** screen is used to configure which EAS messages are processed, based on the areas affected by the alert. The selected Locations are used to determine which EAS alerts need to be processed. If no locations are selected, no alerts will be processed.

Adding Locations

First select a State from the Select a State dropdown box. Then, from the **Available Counties** grid, select the checkbox(es) that corresponds to the area(s) that you wish to add. Add the counties to the **Selected Locations** list by selecting the right arrow button.

Removing Locations

From the **Selected Locations** grid, select the checkbox(es) that correspond to the location(s) to remove. Press the left arrow button to remove the selected locations.

Configuring Subdivisions and polygons

Click in the **Coverage Area** column in the **Selected Locations** grid. A screen will appear to configure subdivisions and polygons for the selected location.

Polygons must be entered as latitude,longitude pairs separated by whitespace. At least four coordinate pairs must be entered. The first and last pair must be the same. Polygons are not used to filter incoming alerts. They are only provided so that they can be included in outbound CAP messages delivered by the CAP HTTP Delivery feature.

Select the **Save** button to save changes, or select the **Cancel** button to exit without saving.

Video Out

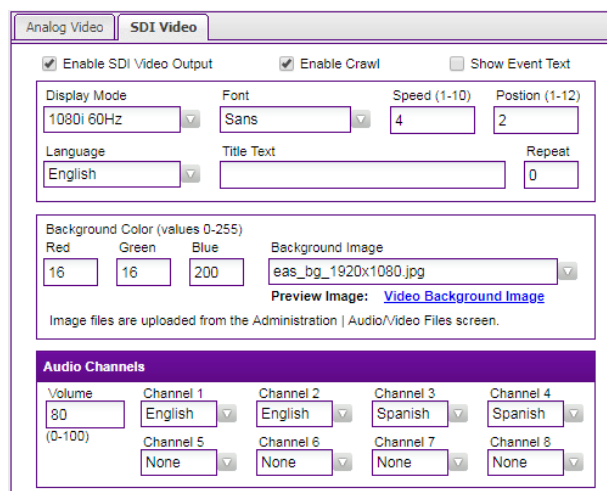Configure the analog and SDI video outputs.

Analog Video

- **Enable Analog Video Output** – Enable or disable the analog video output.

- **Analog Video Output Always On** – Select this option to provide a constant analog video source. This will activate the video switch on startup and leave it active. Note that the Series 30 Hardware does not include a video switch.

- **Show Event Text** – Select this option to display the name of the event (for example "Tornado Warning").

- **Show page numbers at the bottom of the screen** – Select this option to display page numbers at the bottom of the screen rather than at the top of the screen.

- **Font** – Select the font used for text.

- **Repeat** – Enter the number of times to repeat the alert text on the video output (0-9). The text will always be repeated as many times as necessary to make it last at least as long as the audio, regardless of the configured repeat value.

- **Speed** – Enter the speed of the video message in characters per second (default is 12).

- **Language** – Select the text language that's used to generate the video (English, Spanish, or English followed by Spanish).

- **Title Text** – Enter text to use as a title. If configured, the title will be displayed at the top of the video screen.

- **Background Color** – Enter the default background color as RGB values (0-255). The default background color will be shown when a background image is not available.

- **Background Image** – Select a background image for the analog video. This image will be displayed when there are no messages active.
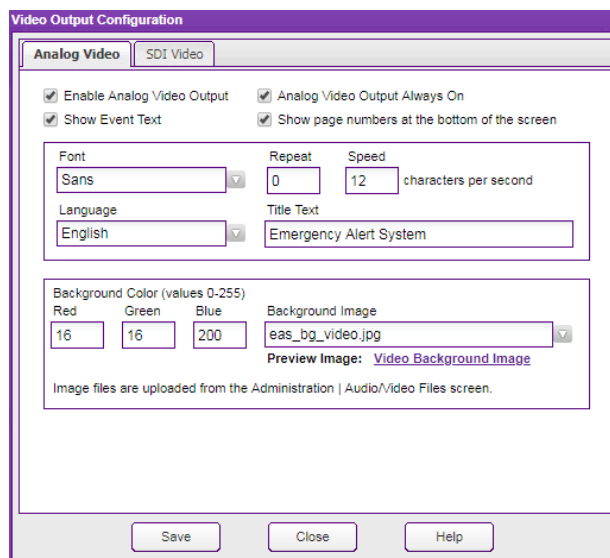
SDI Video

- **Enable SDI Video Output** – Enable or disable the SDI video output.

- **Enable Crawl** – Enable the video crawl to scroll the message text.

- **Show Event Text** – Select this option to display the name of the event (for example "Tornado Warning").

- **Display Mode** – Select the display mode for the SDI video. Options include: 480i, 720p, and 1080i (at 59.94 or 60 Hz).

- **Font** – Select the font used for text.

- **Speed** – Enter the speed of the video message in characters per second, where 1 is the slowest and 10 is the fastest (default is 4).

- **Position** – Enter the position of the text crawl, where 1 is the top of the screen and 12 is the bottom of the screen (default is 2). Note that this setting only applies to crawl text.

- **Language** – Select the text language that's used to generate the SDI video (English, Spanish, English followed by Spanish).

- **Title Text** – Enter text to use as a title. If configured, the title will be displayed at the top of the video screen.

- **Repeat** – Enter the number of times to repeat the alert text on the video output (0-9). The text will always be repeated as many times as necessary to make it last at least as long as the audio, regardless of the configured repeat value.

- **Background Color** – Enter the default background color as RGB values (0-255). The default background color will be shown when a background image is not available.

- **Background Image** – Select a background image for the SDI video. This image will be displayed when there are no messages active.

- **Audio Volume** – Select the volume for the embedded audio (default is 80).

- **Audio Channels** – Select the language for each embedded audio channel. Disable the audio channel by selecting **None**.

> **NOTE**
> *480i supports 2 embedded audio channels.*
> *720p and 1080i support 8 embedded audio channels.*

Web Configuration

Configure the Web Services.

Main Tab

Color Theme – Click the radio button on the color theme you want to use. Click **Test** to view the color theme. Click **Set Cookie** to save the theme in a cookie for your local browser, which overrides the configured global theme of the Web Service, allowing each user to have their own preference. Click Save to save the global theme for the Web Service.

Session Timeout – Enter the number of minutes of inactivity that causes the current session to end.

Status Timer – Enter the number of seconds for the Status Monitor screen to poll for status updates.

Status Timeout – Enter the number of minutes that the Status Monitor screen can be active. After this timeout period the session will end, forcing a user logoff.
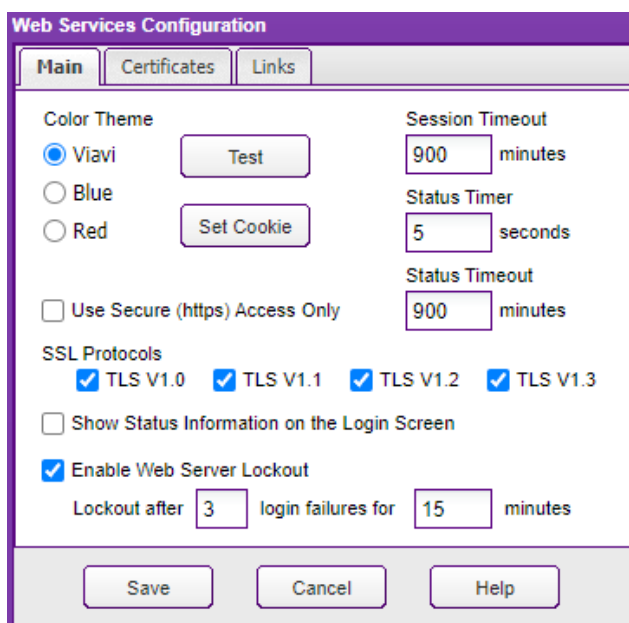
Use Secure (https) Access only – When enabled, only Secure (HTTPS) access to the EASyCAP® is allowed.

SSL Protocols – Select the allowable SSL protocols that can be used to connect to the EASyCAP Web Interface.

- **TLS V1.0** – Allow TLS V1.0 to be used for connecting to the Web Interface.

- **TLS V1.1** – Allow TLS V1.1 to be used for connecting to the Web Interface.

- **TLS V1.2** – Allow TLS V1.2 to be used for connecting to the Web Interface.

- **TLS V1.3** – Allow TLS V1.3 to be used for connecting to the Web Interface.

Show Status Information on the Login Screen – When enabled, a **Status** button will be accessible from the **Login** screen that allows operators to view status and configuration information without having to login.

Web Server Lockout – If enabled, the Web server interface will be locked out for a configured amount of time after a configurable number of failed login attempts.
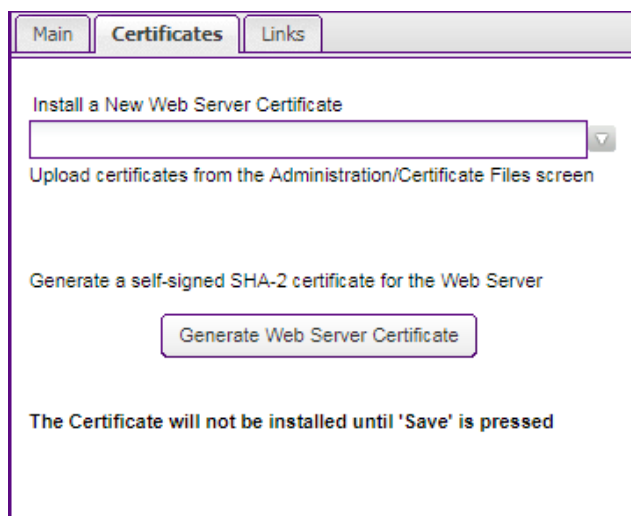
Certificates Tab

Install a New Web Server Certificate
– To install a new certificate for the
EASyCAP Web Server, the certificate
must first be uploaded from the
Administration/Certificate Files screen.
After the certificate has been uploaded,
select it from this combo-box.

Generate Web Server Certificate –
Generate a self-signed SHA-2 certificate
for the EASyCAP Web Server.

Note that the **Use Secure Access Only**
option will be disabled when a new certificate is configured to allow HTTP access until
the certificate can be tested. The new certificate will not be installed until the **Save**
button is pressed.

Links Tab

The **address used for File Links** and
Web Service Links configures the
address used for links that are included
in outgoing Emails and SNMP. These
addresses must begin with "https://" (or
"http://"), for example "https://easycap1.
trilithic.net". If you do not want File or
Web Service links to be included in
Emails or SNMP, leave the setting blank.

Press the **Save** button to save configuration changes and install or generate a new Web
Server certificate if configured. Press the **Cancel** button to exit without saving changes.

CAP Sources

Expand the **CAP Sources** folder in the Navigation bar by clicking the **+** sign next to the **CAP Sources** folder.
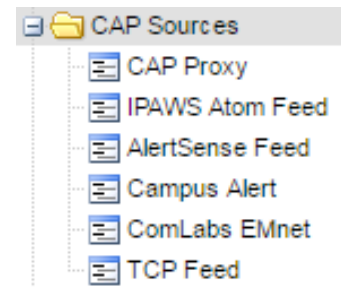
CAP Proxy Configuration

To configure CAP Proxy Servers, select the **CAP Proxy** link. The **CAP Proxy Configuration** setup page will be displayed.
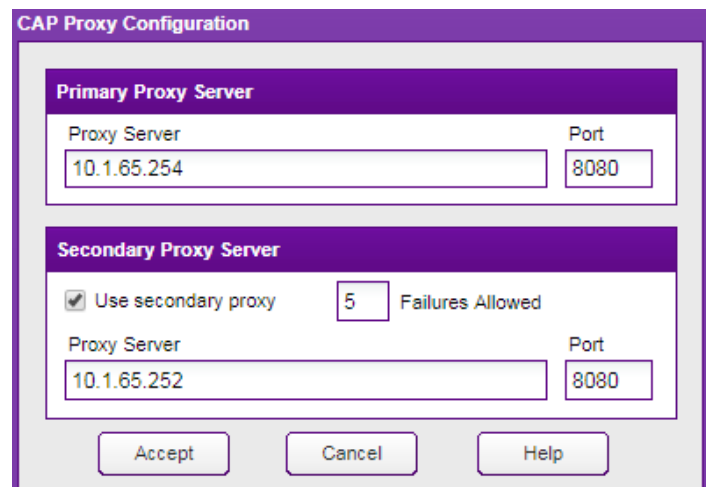

> **Primary Proxy Server** – This HTTP/HTTPS Proxy Server is used to retrieve CAP messages and audio files. Enter the Proxy Server as a fully qualified domain name or an IP address. Also enter the correct TCP port to use for the Proxy Server.

> **Use secondary proxy** – Select this option to use a secondary proxy if the primary proxy fails. When enabled, if a configurable number of sequential failures occur while polling a CAP source, the software will failover (or fall back) to the alternate proxy. Note that any unexpected response from a CAP source will be considered a failure.

> **Failures Allowed** – Enter the number of failures allowed before failing over to the alternate proxy (the default is 5).

> **Secondary Proxy Server** – This HTTP/HTTPS Proxy Server is used as an alternate proxy when the CAP source cannot be polled through the primary proxy. It is only used when the **Use secondary proxy** option is enabled. Enter the proxy server as a fully qualified domain name or an IP address. Also enter the correct TCP port to use for the secondary proxy server.

Select the **Accept** button to save changes to the CAP Proxy configuration or select the **Cancel** button to exit without saving the changes.
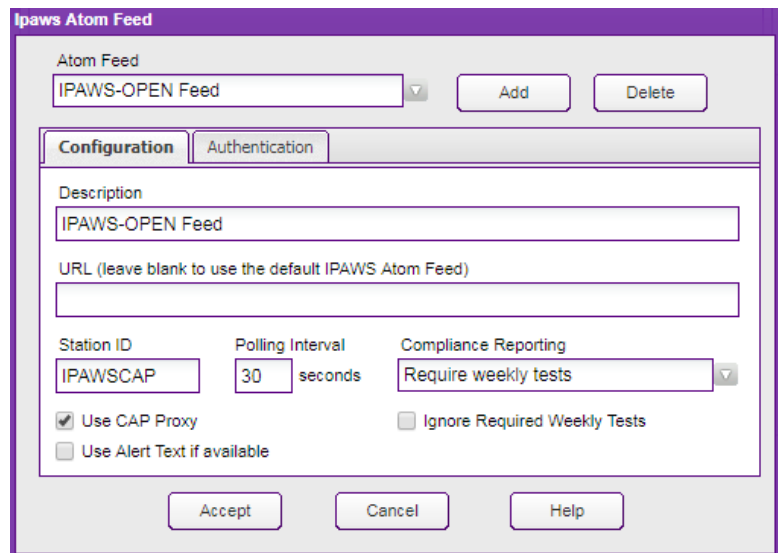
IPAWS Atom Feed

The IPAWS Atom feed allows the EASyCAP® to retrieve CAP messages from the FEMA IPAWS Open Atom feed (or similar CAP Atom feeds).

Atom Feed – Select a feed from the drop-down menu to view/edit.

- **Add** – Add a new Atom feed.
- **Delete** – Delete the selected Atom feed.

IPAWS Atom Feed Configuration

- **Description** – Enter a description for this feed.
- **URL** – Enter the URL of the Atom feed into this field. Leave blank to use the default IPAWS Open Atom Feed URL.
- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.
- **Polling Interval** – Enter the time in seconds between requests for new messages.
- **Compliance Reporting** – The Compliance Reporting module uses this setting to determine if the channel needs to be included in the compliance analysis. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

  Disabled – This channel will not be analyzed for compliance.

  Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

  Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week. This is the recommended setting for IPAWS-OPEN, which currently only sends weekly tests.

  Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

- **Use CAP Proxy** – Enable this option to use the configured CAP proxy servers.

- **Use Alert Text if available** – Enable this option to use the alert_text provided in the CAP message rather than generating alert text locally. If the alert_text element is not present, it will always be generated locally. This can be helpful with the translation of time information when monitoring alerts from different time zones.

- **Ignore Required Weekly Tests** – Enable this option to prevent transmission of Required Weekly Tests received from this feed. Receipt of the RWT will be logged, but it will not be transmitted.

Authentication

- **Use Default PIN** – If enabled, the default PIN for the IPAWS Open Atom feed is used.

- **Username** – If applicable, enter the username for the feed. FEMA's IPAWS Open Atom feed does not require a username, and this field should normally be left blank. If a username is configured, Basic authentication will be used.

- **Password or PIN** – Enter the password or PIN required to access the feed.

- **Confirm Password/PIN** – Enter the password/PIN again for verification.

- **Check Server Certificate** – Verify the IPAWS Atom feed Web Service certificate against the certificate authority. Certificates can be added and deleted from the **Administration >> Certificate Files** screen.

- **Signature Verification –** Select the type of verification to use for digital signatures included in the CAP messages.

  Do Not Verify Signatures – Ignore the CAP messages digital signature.

  Log Warning if Signature is Invalid – Log a warning if the digital signature is invalid.

  Reject Message if Signature is Invalid – Reject messages when the digital signature is invalid.
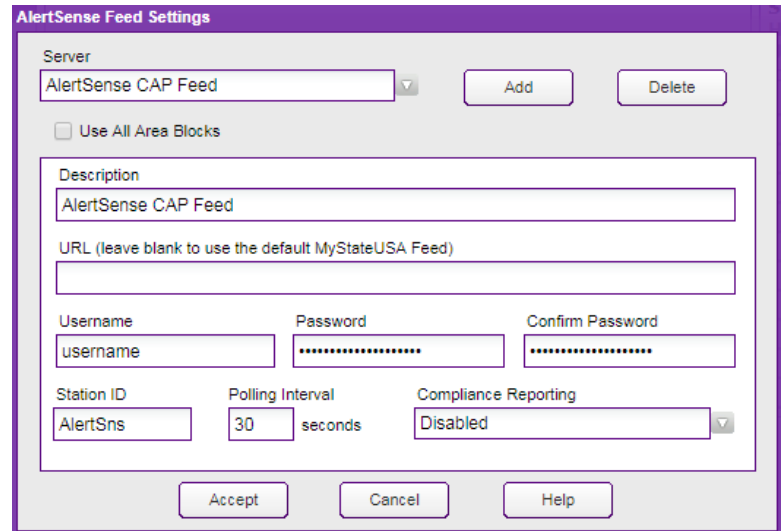
Press the **Accept** button to save changes, or **Cancel** to exit without saving.

AlertSense Feed

The AlertSense feed allows the EASyCAP® to retrieve CAP messages from AlertSense CAP servers or servers that use a similar HTTP interface.

Server – Select a feed from the drop-down menu to view and edit.

- **Add button** – Add a new feed.
- **Delete button** – Delete the selected feed.

AlertSense Feed Settings

- **Use All Area Blocks** – Select this option to process all <area> blocks within a CAP message. If disabled, only the first <area> block is processed. Disable this option to comply with current CAP to EAS implementation guidelines.

- **Description** – Enter a description for this feed.

- **URL** – Enter the URL of the AlertSense Feed into this field. Leave this field blank to use the default AlertSense URL.

- **Username** – Enter the username assigned by the CAP source administrator.

- **Password** – Enter the password assigned by the CAP source administrator.

- **Confirm Password** – Enter the password again for verification.

- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.

- **Polling Interval** – Enter the number of seconds between requests for new CAP messages.

- **Compliance Reporting** – Select the type of analysis done by the Compliance Reporting module for this feed. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

  Disabled – This channel will not be analyzed for compliance.

  Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

  Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week. This is the recommended setting for IPAWS-OPEN, which currently only sends weekly tests.

  Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

Press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

Campus Alert Feed

The Campus Alert feed allows the EASyCAP® to retrieve CAP messages from Omnilert, Rave Mobile Safety, and CAP servers with a similar HTTP interface. These CAP messages are not IPAWS compliant, and are used to distribute alerts that effect a local area (like a college campus).

Server – Select a feed from the drop-down menu to view and edit.

- **Add** – Add a new feed.
- **Delete** – Delete the selected feed.

Feed Settings

- **Description** – Enter a description for this feed.
- **Use alerts envelope** – Select this checkbox if the feed uses an alerts envelope that can include more than one CAP message.
- **Polling Interval** – Enter the time in seconds between requests for new CAP messages.
- **URL** – Enter the URL. The CAP xml file should be included in the URL (for example "http://www.myuniversity.edu/alert.xml").
- **Compliance Reporting** – Select the type of analysis done by the Compliance Reporting module for this feed. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

  Disabled – This channel will not be analyzed for compliance.

  Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

  Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week.

  Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

- **Compliance Reporting** – Select the type of analysis done by the Compliance Reporting module for this feed. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

  Disabled – This channel will not be analyzed for compliance.

  Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

  Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week. This is the recommended setting for IPAWS-OPEN, which currently only sends weekly tests.

  Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

Press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

TCP Feed

To setup TCP feeds, select the **TCP Feed** link from the **CAP Configuration** folder.

Server – Select a TCP feed from the drop-down menu to view and edit its settings.

- **Add button** – Add a new feed.

- **Delete button** – Delete the selected feed.

TCP Feed Settings

- **Use All Area Blocks** – Select this option to process all <area> blocks within a CAP message. If disabled, only the first <area> block will be processed. This should be disabled in order to comply with current CAP to EAS implementation guidelines.

- **IP Address** – Enter the IP Address of the TCP feed into this field.

- **Port** – Enter the TCP port number.

- **Description** – Enter a description for this feed.

- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.

- **Compliance Reporting** – Select the type of analysis done by the Compliance Reporting module for this feed. Note that this setting will only be accessible if the EASyCAP is licensed for Compliance Reporting.

    Disabled – This channel will not be analyzed for compliance.

    Enabled, no requirements – This channel will be analyzed for EAS compliance, but it is not required to receive weekly or monthly tests.

    Require weekly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week.

    Require monthly tests – This channel will be analyzed for EAS compliance. The analysis will flag this channel as not compliant if weekly tests are not received each week or monthly tests are not received each month.

Press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

Message Delivery Folder

Expand the **Message Delivery** folder in the Navigation bar by clicking the **+** sign next to the folder.
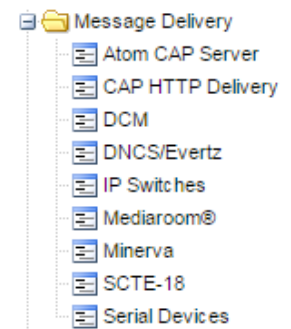
Atom CAP Server

The Atom CAP Server feature provides a CAP feed similar to the FEMA IPAWS Open Atom feed, allowing downstream Encoder/Decoders to retrieve IPAWS compliant CAP messages from the EASyCAP®. This feature provides the ability to transfer CAP and EAS messages to other EASyCAP® Encoder/Decoders. Messages received via EAS are formatted into IPAWS compliant CAP messages and then made available on the Atom feed.

Select the **Atom CAP Server** link from the **Message Delivery** folder to setup the server.

Enable Atom CAP Server – Enable or disable the Atom CAP Server.

Include EAN Messages – Include EAN messages on the Atom feed.

- If the EAN is received from an EAS source, the audio stream URI will reference an audio stream hosted by the EASyCAP®.
- EAN messages received from CAP sources will not be available on this feed.
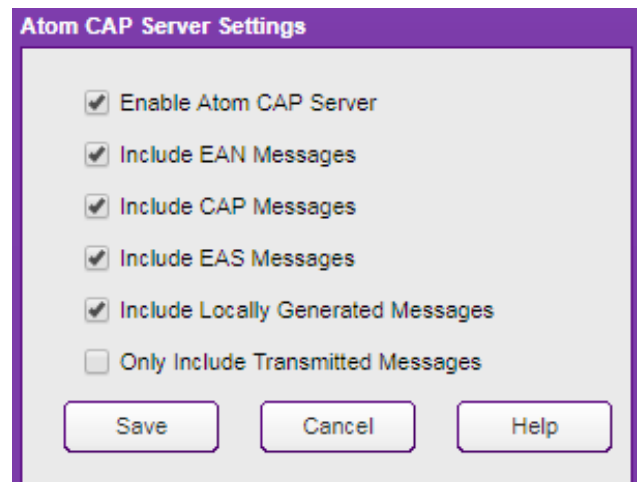
Include CAP Messages – Include message received via CAP sources on the Atom feed.

Include EAS Messages – Include message received via EAS sources on the Atom feed. This includes messages received via audio and radio sources, Network Receivers, and EASyPLUS Encoder/Decoders.

Include Locally Generated Messages – Include message that were locally generated (by an operator or the random weekly test generator) on the Atom feed.

Only Include Transmitted Messages – When enabled, messages must be transmitted by the EASyCAP before they are put on the Atom feed.

Press **Accept** to save configuration changes or **Cancel** to exit without saving any changes.

Configure user accounts for the Atom CAP Server:
At least one user account needs to be configured to allow access to the **Atom CAP Server**. The user account must have the **Web API** permission enabled in order to login to the **Atom CAP Server**.

Enable the Atom CAP Server Web API:
Enable the Atom CAP Server Web API on the **Management | Web API Settings** screen.

Configuring clients to receive messages from the Atom CAP Server:
The client side configuration is similar to configuring FEMA's IPAWS Open Atom feed.

1) Add an IPAWS Atom Feed.

2) The URL is configured as the HTTPS address of the EASyCAP® followed by "EASYCAP_EAS_SERVICE/rest". For example, if the EASyCAP address is 192.168.1.71, the URL is: https://192.168.1.71/EASYCAP_EAS_SERVICE/rest.

3) Enter the username and password of the user account that was setup for the **Atom CAP Server.** The server uses Basic Authentication, therefore the username and password are required.

> **NOTE** *The network must be configured to allow port 80 traffic from the Atom CAP Server to the Client in order to receive live audio for an EAN.*

CAP HTTP Delivery

The CAP HTTP Delivery feature provides the ability to deliver EAS and CAP messages to HTTP/HTTPS servers. Alert messages are formatted into IPAWS compliant CAP messages prior to delivery. CAP messages and audio are delivered via a single HTTP Post, using multipart form data.

Server – Select a server from the drop-down menu.

Add button – Add a new server.
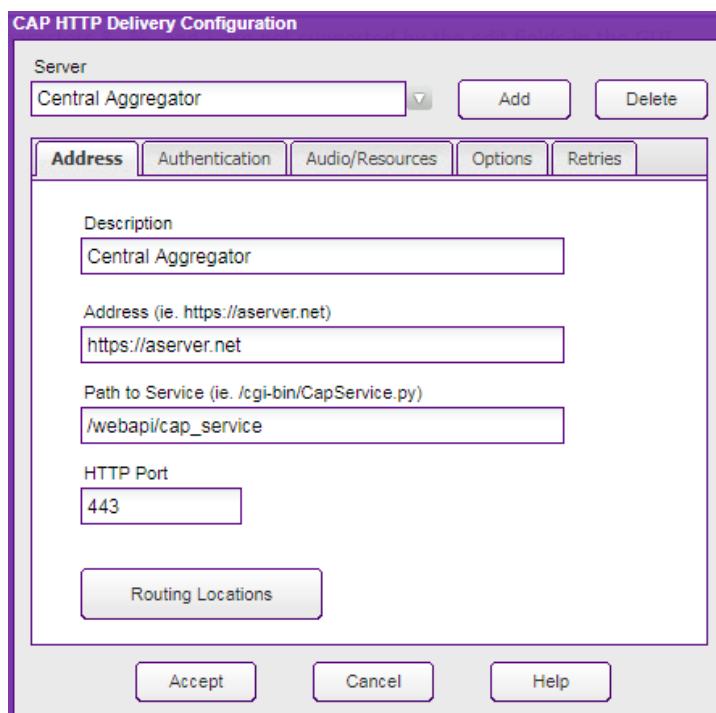
Delete button – Delete the selected server.

Address Tab

Description – Enter a descriptive name for this server.

Address – Enter the protocol (http or https) and hostname or IP address of the server. For example: http://aserver.net.

Path to the Service – Enter the path to the web service. For example: /webapi/cap_service.

HTTP Port – Enter the HTTP or HTTPS port for the server. This will normally be port 80 for HTTP, or port 443 for HTTPS.

> **NOTE**
>
> ***The Address, HTTP Port, and Path to Service are combined to form the URL. If Address is http://aserver.net, HTTP Port is 80, and Path to Service is /webapi/cap_service, then the combined URL would be http://aserver.net:80/webapi/cap_service.***

Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced. Select the locations that are serviced by the server or select All Locations to disable location routing and deliver all messages to the selected device.

Click **Accept** to save changes to the Routing Locations configuration or click **Cancel** to exit the **Routing Locations** window without saving changes.
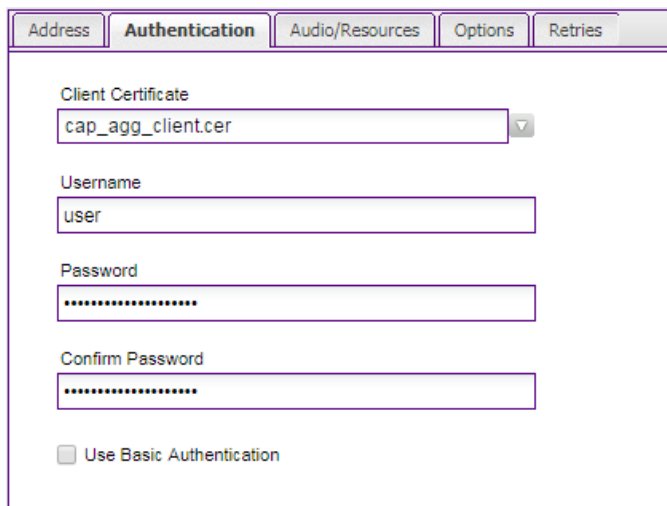
Authentication Tab

Client Certificate – If a client certificate is required, select the certificate from this combo-box. Use the **Administration/ Certificate Files** screen to upload new certificate files.

Username – Enter the username to login to the HTTP service. If this field is left blank, the login information will not be included in the communications.

Password – Enter the password to login to the HTTP service. If this field is left blank, the login information will not be included in the communications.

Confirm Password – Enter the password again for verification.

Use Basic Authentication – Enable Basic Authentication. If disabled, login information will be included in the multipart/form-data.

Audio/Resources Tab

Audio File Type – The audio file format is configurable as WAV or MP3.
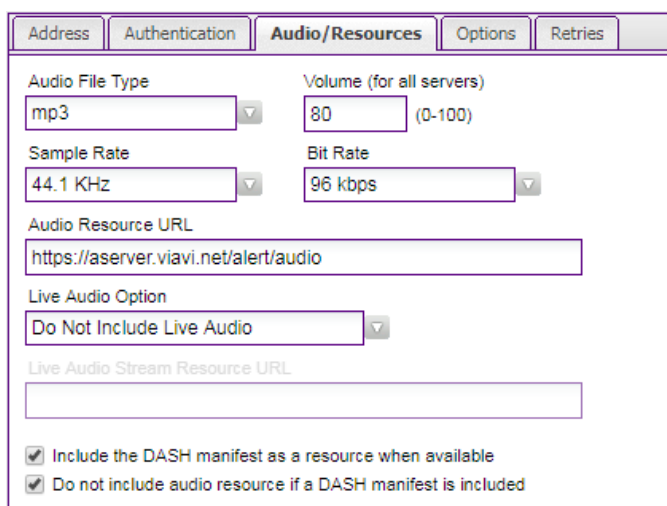
Volume – Enter the audio file volume (0-100).

Sample Rate – Select the sample rate for the audio files.

Sample Size – This setting is only available if the audio type is WAV. The audio sample size can be 8 or 16 bit.

Bit Rate – This setting is only available for MP3 audio. Select the bit rate of the audio. The default bit rate is 96kbps.

Audio Resource URL – This setting is used to construct the CAP message audio resource URI. The CAP message audio resource URI is constructed by appending the audio filename to the text that is configured here.

Live Audio Option – Live messages (like an EAN) cannot deliver audio as a file. This setting provides the following options for handling live audio.

Do Not Include Live Audio – There will not be an audio file delivered, nor will there be an audio resource in the CAP message. This is the default.

Deliver FSK Audio Only – An audio file that only contains the EAS FSK and Attention tone will be delivered, and the CAP message will include an audio resource URI referencing this file. This can be useful for systems that force-tune to another channel, but due to synchronization difficulties, can't guarantee that the EAS tones will be heard after the force-tune.

Include Audio Stream Resource URL – The CAP message will include the Live Audio Stream URL (described below) as the audio resource. The audio stream referenced must be supplied by the system or reference a known audio source.

Live Audio Stream Resource URL – This setting is only available if the Live Audio Option is set to "Include Audio Stream URL". In this case, the text configured here will be used for the CAP message audio resource URI when a live message is sent.

Include the DASH manifest as a resource when available – If enabled, this option will include the DASH manifest as a resource when it's available.

Do not include audio resource if a DASH manifest is included – If enabled, the audio resource will not be included in the CAP message if a DASH manifest is present.

Options Tab

Do not deliver weekly tests (RWT) – Select this option to prevent required weekly tests (RWT) from being delivered to the selected server.

Do not deliver monthly tests (RMT) – Select this option to prevent required monthly tests (RMT) from being delivered to the selected server.

Do not deliver Emergency Action Notifications (EAN) – Select this option to prevent Emergency Action Notifications (EAN) from being delivered to the selected server.

Do not deliver locally generated messages – If enabled, prevents messages that are generated locally (by an operator or automatic RWT generator) from being delivered to the selected server.

Do not deliver weekly tests received from CAP sources – If enabled, prevents weekly tests that are received from CAP sources from being delivered to the selected server.

Send cancellations for non-EAN events – Select this option to deliver CAP Cancellations for events other than an EAN. If disabled, CAP Cancellations will only be delivered for an EAN.

Remove State codes from weekly tests – Select this option to remove all State codes from the message before delivering it to the selected server. If there are no location codes left after removing the State codes, the message will not be delivered. The audio and display text will not be altered. If a state code is removed from the message, the display text will still show the state, and the EAS audio FSK will include the state codes.

Include the sender's address in the CAP source element – Include the IP address of the EASyCAP (and EASyPLUS) that received the message in the <source> element.

Include the sender's address in the CAP sender element – Include the IP address of the EASyCAP (and EASyPLUS) that received the message in the <sender> element.

Include configured polygons - Select these options to include polygon elements when messages are received for CAP, EAS, or locally generated sources. When enabled, CAP messages will include the configured polygon for each FIPS code. One polygon element will be included per FIPS code (if a polygon has been configured for the FIPS).

Include Spanish when available – Include a Spanish info block if Spanish information is available.

Use Configured Locations Only – Select this option to include only those areas configured in the Selected Locations screen.

Expand State to County Codes – Select this option to expand state-wide location codes into the configured county codes within the state. Note that the decision to send (or not send) messages based on routing locations is made prior to expanding state codes.
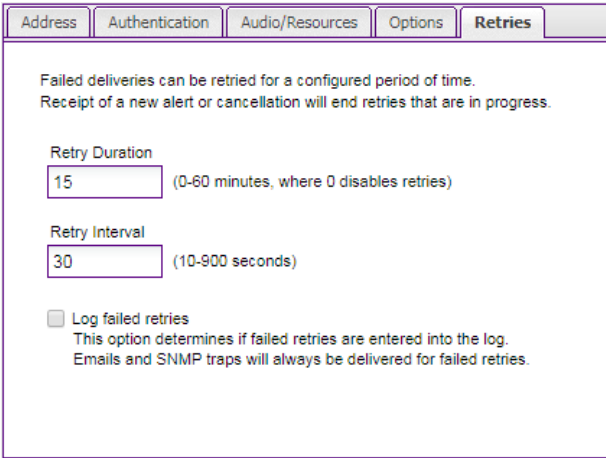
Retries Tab

Configure if and how failed deliveries are retried. If a new message or cancellation is received while retrying a failed delivery, the failed delivery will no longer be retried and the new message or cancellation will be processed.

Retry Duration – Enter the number of minutes (0-60) to retry delivering the message when delivery failures occur. Enter 0 to disable retries.

Retry Interval – Enter the number of seconds (10-900) to wait between delivery retries.

Log Failed Deliveries – If enabled, all failed retries will be logged, otherwise only the first error is logged.

Select the **Accept** button to save changes or the **Cancel** button to exit without saving.

DCM

To configure DCM recipients, select the **DCM** link in the **Message Delivery** folder.

DCM Server – Select a DCM Server from the dropdown menu.

> **Add button** – Add a new DCM Server.
>
> **Delete button** – Delete the selected DCM server.

Description – Enter a descriptive name for the selected DCM Server.

Language – Select the language for the text (English, Spanish, English followed by Spanish).

IP Address – Enter the IP address of the DCM server.

Port – Select the TCP port used to communicate with the DCM server. The default port is 80.

Login – Enter the login username for the server.
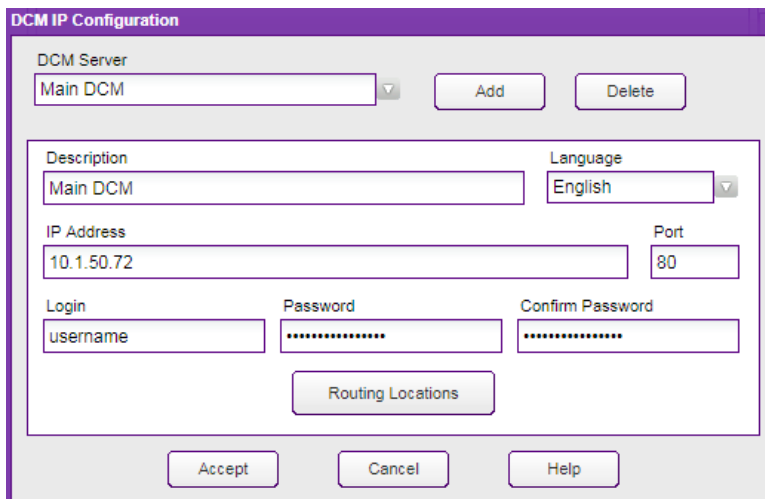
Password – Enter the password for the server.

Confirm Password – Enter the password again for verification.

Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced. Select the locations that are serviced by the DCM server or select All Locations to disable location routing and deliver all messages to the selected device.

> Click **Accept** to save changes to the Routing Locations configuration or click **Cancel** to exit the **Routing Locations** window without saving changes.

Click **Accept** to save your changes or click **Cancel** to exit the without saving changes.

DNCS/Evertz

To configure message delivery to DNCS/Evertz devices, select the **DNCS/Evertz** link in the **Message Delivery** folder.

DNCS Server – Select the server from the dropdown menu.

> **Add button** – Add a new DNCS Server.
>
> **Delete button** – Delete the selected DNCS server.
>
> **Audio Volume** – Set the audio file volume (0-100).
>
> **Use Force-tune Timing Adjustments** – Select this option to use the force-tune time adjustments (from the Playback Options screen) when the message is processed as a live event.

Description – Enter the name to display for this DNCS Server.

Language – Select the language for the audio and text. If **English + Spanish** is selected, the audio will be English and the text will be English followed by Spanish.

IP Address or URL – Enter the IP Address or URL of the DNCS Server.

Port – Enter the TCP port of the DNCS. The default port is 4098.

FTP Username – Enter the username required to login to the FTP server.

FTP Password – Enter the password required to login to the FTP server.

Confirm Password – Enter the password again for verification.

FTP Files Path – If different from the root path, enter the path where files need to be transferred.

Audio File Properties – Select the audio file properties from the dropdown menu. The default is 5.5kHz, 8bit.

Use SFTP – Select this option to use a secure SFTP server rather than an FTP server.

FTP Only (no TCP) – If enabled, the TCP socket message will not be delivered, so only the audio and text files are transferred. This could be used for archiving systems or equipment that only needs the audio and text files.

Use Abort Messages – If enabled, EAT/EOM termination messages will be delivered when an operator manually aborts a message.

Use EOM Termination – If enabled, an EOM termination message will be delivered to the selected server to end a force-tune.

Use EAT Termination – If enabled, an EAT termination message will be delivered to the selected server to end a force-tune.

Use EAS Duration – Select this option to include the EAS duration in the socket message. A value of zero will be used for the duration if this option is not selected.

Do Not Deliver EAN – Select this option to prevent EAN messages from being delivered to the selected DNCS/Evertz server.

Include text file with live events – Select this option to include the alert text file with a live event. Normally a live event causes a force-tune and the text is not needed.

Use Configured Locations Only – Select this option to include only those areas configured in the Selected Locations screen.

Expand State to County Codes – Select this option to expand state-wide location codes into the configured county codes within the state. Note that the decision to send (or not send) messages based on routing locations is made prior to expanding state codes.

Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the server. Select the locations that are serviced by the DNCS server or select All Locations to disable location routing and deliver all messages to the selected server.

> Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations selections.

Click **Accept** to save changes the configuration or click **Cancel** to exit the window without saving changes.

IP Switches

To configure IP Switches, select **IP Switches** in the **Message Delivery** folder.

IP Switch – Select an IP Switch from the dropdown menu.

> **Add** – Add a new IP Switch.
>
> **Delete** – Delete the selected IP Switch.
>
> **Deactivate outputs every <*n*> minutes** – Enter the number of minutes to wait between (periodically) deactivating the

outputs on all configured IP switches. Enter zero (0) to disable periodic deactivations.

Description – Enter the name to display for this IP Switch.

Type – Select the type of IP switch. Note that older iPIO-8 switches may use the COE-8 protocol.

IP Address – Enter the IP address of the IP Switch.

Port – Enter the TCP Port number which is used to communicate with the IP switch (the default setting is 9100).

Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the switch.

> Select the locations that are affected by the IP switch or select All Locations to disable location routing and deliver all messages to the selected switch. Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations selections.

Click **Accept** to save your changes or click **Cancel** to exit the **IP Switches** window without saving changes.
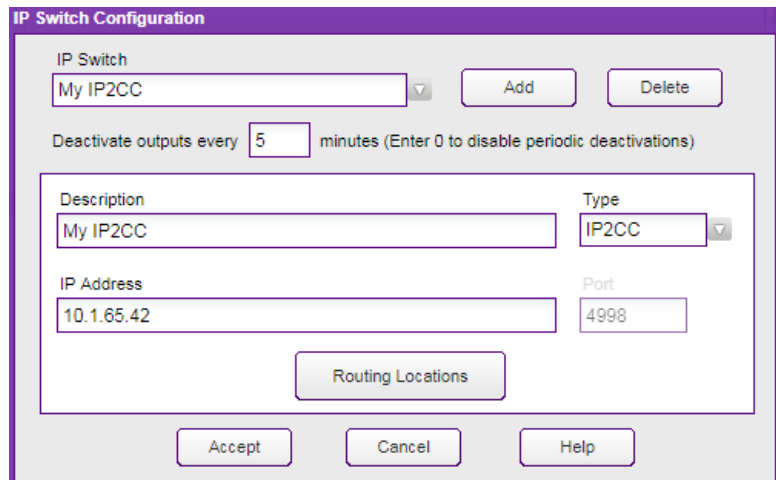
IP Switch output functions are configured on the Configuration/General Purpose IO screen.

Mediaroom® Settings

The Mediaroom® delivery feature provides the ability to deliver EAS and CAP messages to Mediaroom systems. Alert notifications are delivered to the Mediaroom V2.0 EAS Web Service. Alert text is overlaid onto the clients (set-top boxes) and the alert audio is streamed from the EASyCAP to the clients. Redundancy is supported to allow multiple EASyCAP Encoder/Decoder's to send alert messages to the same server. The Mediaroom® delivery feature requires a license and is only available for EASyCAP Encoder/Decoder IPTV models.

Web Service Tab

EAS Web Service

Enable EAS Web Service – Enable delivery to the Mediaroom server.

Description – Enter the name to display for the server.

Mediaroom® EAS Web Service URL – Enter the URL for the V2.0 EAS Web service.

Redundancy

Multiple EASyCAP Encoder/Decoders can send alerts to a single Mediaroom server. In order to make this work properly, the Encoder/Decoders must coordinate with one another to guarantee that alert messages don't overlap.

EASyCAP is Master – Select this check-box if this EASyCAP is the master, or if only one EASyCAP is used.

Master Address – Enter the IP address of the master EASyCAP.

Master Port – The TCP port used to communicate with the Master (default is 59914).

Abort/Test – Press this button to send an EOM (end of message) notification to the Mediaroom® server. The EOM notification will abort a message that's in progress. This can be used to test the connectivity to the Web service and to manually abort a message.

> **NOTE** *When configuring the audio stream for Mediaroom, make sure to select the first stream and do not enable video.*

Authentication Tab

Certificates

Check Server Certificate – Verify the EAS Web Service certificate against the certificate authority.

Use Client Certificate – Use a client certificate for authentication.

Client Certificate – Select the client certificate used by the EASyCAP for authentication.

Basic Authentication

Use Basic Authentication – Enable basic authentication. If enabled, it will be used

> **NOTE**
>
> ***Certificates can be managed (uploaded, deleted, and viewed) from the Administration / Certificate Files screen.***

even if a client certificate is used.

Username – Enter the username for basic authentication.

Password – Enter the password for basic authentication.

Confirm Password – Enter the password again for verification.

Options Tab

Timing

Alert Start Delay – Enter the number of seconds required to guarantee that the alert notification is received by all clients (the default is 75).

EAN Repeat Interval – Enter the number of seconds between repeating EAN notifications. This time must be greater than the **Alert Start Delay** (default is 150).

Repeat EOM to end EAN – Enter the number of times to repeat the EOM (end of message) when ending an EAN. This is provided to ensure that all clients end the EAN.

Crawl Speed – Enter the crawl speed of the clients text display in characters per second.

Crawl Pre Delay – Enter the number of seconds that the client waits between showing the alert text and starting the crawl.

Crawl Post Delay – Enter the number of seconds that the client waits after the crawl finishes before removing the alert text.

> **NOTE** ***Crawl settings provide timing information to the EASyCAP so that it can determine how long the text will be displayed by the clients. They do not affect the clients display.***

General

Do Not Deliver EAN – Select this option to prevent EAN messages from being delivered to Mediaroom.

Send EOM to Abort Level 2 Alerts – Select this option to deliver an EOM notification to abort level 2 alerts.

Ensure Spanish Text is Available – Select this option to copy the English text into the Spanish text element when a CAP message does not include Spanish.

Send Event Code in the extData field – Select this option to populate the extData field with the EAS Event code. If this option is disabled, the extData field is populated with the Event Type (except for an EOM or EAT, which populates the EAS Event code).

Use Configured Locations Only – Select this option to include only those areas configured in the Selected Locations screen.

Expand State to County Codes – Select this option to expand state-wide location codes into the configured county codes within the state.

> **NOTE** *Use Configured Locations Only and Expand State to County Codes options will not alter the audio or display text. They will only alter the locations in the alert notification delivered to the EAS Web Service.*

Click **Accept** to save changes to the configuration, or click **Cancel** to exit without saving changes.

Minerva Configuration

To configure message delivery to Minerva servers, select **Minerva** in the **Message Delivery** folder.

Minerva Server – Select the server from the dropdown menu.

> **Add button** – Add a new Minerva server.
>
> **Delete button** – Delete the selected Minerva server.
>
> **Use Force-tune Timing Adjustments** – Select this option to use the force-tune time adjustments (from the Playback

Options screen) for messages delivered to Minerva servers.

Description – Enter the name to display for this Minerva Server.

Language – Select the language for the text (English, Spanish, English followed by Spanish).

IP Address – Enter the IP address of the Minerva Server in this field.

Port – Enter the TCP port used to communicate with the Minerva server (default port number is 4670).

Token – Enter the "token" for the EASyCAP® into this field. The "token" is used by the Minerva server to determine which Encoder/Decoder sent the message. The default is 1.

Routing Locations – Click this button to open the **Routing Locations** window.

> The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the device. Select the locations that are affected by the server or select All Locations to disable location routing and deliver all messages to the selected server. Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations.

Click **Accept** to save your changes or click **Cancel** to exit the window without saving changes.

SCTE-18 Configuration

To configure SCTE-18 devices, select **SCTE-18** in the **Message Delivery** folder.

SCTE-18 Server – Select the SCTE-18 device from the dropdown menu.

> **Add button** – Add a new SCTE-18 device.
>
> **Delete button** – Delete the selected SCTE-18 device.
>
> **Copy Group Settings** – Copies settings from the group to the selected SCTE-18 device. Make sure the correct group is selected in the Group edit box before copying settings.

> **Use Force-tune Timing Adjustments** – Select this option to use the force-tune time adjustments (from the Playback Options screen) for SCTE-18 messages.
>
> **Multicast TTL** – Enter the Multicast TTL for SCTE-18 messages.

Description – Enter the name to display for this device.

Transport Type – Select the digital transport protocol used to deliver SCTE-18 messages to the selected device.

> **NOTE**
>
> ***Vecima uses UDP MPEG packets but it's listed as a separate transport type because it requires a special sequence.***
> ***If Vecima is selected but the Vecima Descriptor is not configured, the transport type will revert back to MPEG UDP Packets when the configuration changes are saved.***

IP Address or URL – Enter the IP address or URL of the selected device.

Port – Enter the UDP port number for the selected device (default UDP port is 5050).

PID – Enter the PID for SCTE-18 messages delivered to this device. The PID is not used if the Transport Type is set to DOCSIS Set-top Gateway. The default PID for in-band devices is 1FFB, the default PID for out-of-band devices is 1FFC.

MTU – Enter the MTU for SCTE-18 messages delivered to this device. The MTU is only used for devices with the Transport Type set to DOCSIS Set-top Gateway. The default MTU is 1500.

Language – Select the language for the text (English, Spanish, English followed by Spanish).

Repeat Rate – Enter the interval for repeating SCTE-18 messages. Repeated messages are exact duplicates - the MPEG continuity_counter and SCTE-18 sequence_number will not be incremented. Repeats are used to guarantee devices receive the message and for devices that come online after the initial message was delivered. Messages will not be repeated if this is set to zero.

Repeat new messages – Enter the number of times to repeat the initial SCTE-18 message in order to establish an MPEG stream. The MPEG continuity_counter will be incremented for each packet sent.

Group – Enter a Group number (0-64) for the selected SCTE-18 Device, where a value of zero means the device is not included in any group. SCTE-18 Groups are provided to simplify the configuration process by allowing you to associate several SCTE-18 devices so that their configuration can be managed as a group. Assign the same Group number to devices that will be configured similarly. Then you can apply configuration changes to all of the devices in a group, or import settings from a group into a device. The group settings include all configuration except the device Description, IP address, port, and locations.

Out-of-band Source ID – Enter the out-of-band source information for the EAS Details Channel and Audio.

In-band Channels – Enter the Major and Minor Channel that represent the virtual channel number of the EAS Details channel. This only applies to in-band SCTE-18 messages. The system operator is responsible for providing PSIP support for the EAS Details channel.

Send Message Twice – Select this option to send the alert to the SCTE-18 device twice, incrementing the sequence_number on the second delivery. This helps to insure that the devices do not discard the alert due to a duplicate sequence_number.

Used discontinuity indicator – Select this option to include a discontinuity indicator at the beginning of each SCTE-18 transmission.

Exclude Event start time – Select this option to set the SCTE-18 event start time field to zero.

Exclude alert text – Select this option to prevent the alert text from being included in the SCTE-18 message.

Duration based on audio – Select this option to base the alert message time remaining on the length of the audio. If this is not selected, the alert message time remaining will be based on the length of the audio and video crawl, whichever is longer.

Disable Abort messages – Select this option to prevent abort messages from being sent to the device when an operator manually aborts a message.

Use Configured Locations Only – Select this option to include only those areas configured in the Selected Locations screen.

Expand State to County Codes – Select this option to expand state-wide location codes into the configured county codes within the state. Note that the decision to send (or not send) messages based on routing locations is made prior to expanding state codes.

Apply changes to all servers in the group – When checked, changes to the configuration will be saved to all devices in the group.

Descriptors – Click this button to open the **SCTE-18 Descriptors** window.

> **Descriptor Type** – Select the type of descriptor from the dropdown menu.
>
> > **Custom Descriptor** – The custom descriptor type is provided to enter descriptors not defined or supported in the GUI. When entering a custom descriptor you must enter the raw binary data that goes into the descriptor. The data is entered as hexadecimal values. All of the descriptor data, including the descriptor_tag and descriptor_length, must be included.

SCTE-18 Descriptors

Descriptor Type

Custom - enter raw descriptor data

Custom Descriptor

Enter the data to be included in the SCTE-18 descriptors
Enter the data as hexadecimal values (0 = '00', 10 = '0A', 255 = 'FF')
Supply only the data contained in the SCTE-18 descriptor() field

1C0E12131415161718191A1B1C1D1E1F

Show configuration   Accept   Cancel

In-band Details Channel Descriptor – Click this checkbox if you want to use the in-band details channel descriptor. Enter the **RF Channel** and the **Program Number**.

In-band Exceptions Descriptor – In this box is a table of RF Channels and the associated Program Numbers. To add a new entry to the table, enter the **RF Channel** and the **Program Number**, then click **Add**. To delete an entry, click the item in the table you want to delete so it is highlighted, then click **Delete**.

Vecima Audio & Force-tune Descriptor – The Vecima descriptor is used to inform the CableVista where to find the EAS Details MPEG stream. The Vecima descriptor cannot be used if the Transport Type is set to DOCSIS Set-top Gateway.

> **IGMPv2 Group Address** – Enter the IGMP version 2 group multicast address.
>
> **IGMPv3 Group Source Address** – Enter the IGMP version 3 group source multicast address.
>
> **EAS Audio Stream PID** – Enter the PID for the EAS audio stream (16-8190).
>
> **EAS Channel UDP port** – Enter the UDP port for the EAS Details channel (256-65535).
>
> **Physical GigE Port** – Enter the physical GigE port used (1 or 2).
>
> **Details Channel Program Number** – Enter the program number for the EAS Details channel (1-65535).

Click **Show Configuration** to view the descriptor as a hexadecimal string, which can be useful to copy the descriptor into the StrataSync UI.

Click **Accept** to save changes to the descriptor or click **Cancel** to exit the **SCTE-18 Descriptors** window without saving selections.

Exceptions – Click this button to open the **SCTE-18 Exceptions** window.

> **Add an exception** – Enter the Source ID and press the Add button (Minor Channel is not used).
>
> **Add an in-band exception** – Check the In-band exception reference, enter the Major and Minor channel numbers, and then press the Add button.
>
> **Delete an exception** – Click the exception in the list that you want to delete so it is highlighted, then press the Delete button.
>
> Click **Show Configuration** to view the descriptor as a hexadecimal string, which can be useful to copy the descriptor into the StrataSync UI.

Click **Accept** to save changes to the exceptions or click **Cancel** to exit the **SCTE-18 Exceptions** window without saving selections.

Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the device.

Select the locations that are affected by the device or select All Locations to disable location routing and deliver all messages to the selected device.

Click **Accept** to save the selected routing locations or click **Cancel** to exit the **Routing Locations** window without saving the selected locations.

Serial Devices

To configure Serial Devices, select **Serial Devices** in the **Message Delivery** folder. The **Serial Devices** window will be displayed.

Serial Device – Select the type of serial device from the dropdown menu.

> **Add** – Add a new serial device.

> **Delete** – Delete the selected serial device.

Description – Enter a name to display for this Serial Device.
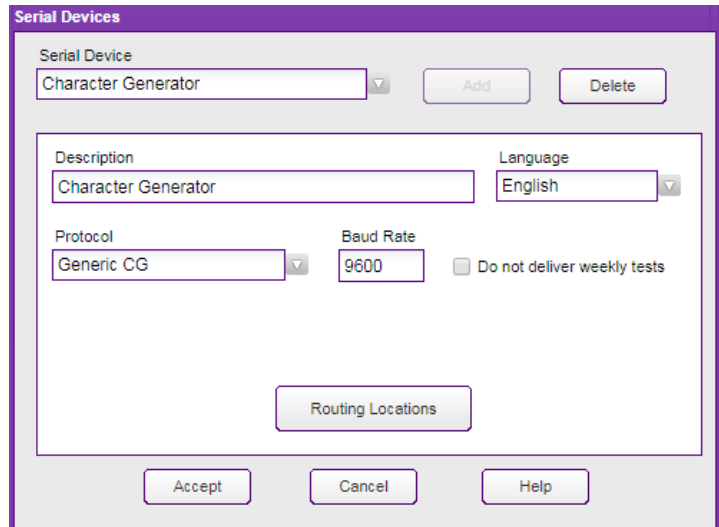
Language – Select the language for the text (English, Spanish, English followed by Spanish).

Protocol – Select the protocol used to communicate with the device from the dropdown menu. The Chyron and Star-8 CG protocols provide configuration for the Crawl Position and number of Crawl Repeats. Chyron protocol also allows the Crawl Speed to be configured.

Baud Rate – Enter the serial baud rate.

Routing Locations – Click this button to open the **Routing Locations** window. Click the checkboxes to select locations and areas. Click **Accept** to save the selected locations or click **Cancel** to exit the **Routing Locations** window without saving the selected locations.

Click **Accept** to save your changes or click **Cancel** to exit the window without saving changes.

Management Folder

Expand the **Management** folder in the Navigation bar by clicking the **+** sign next to the folder.
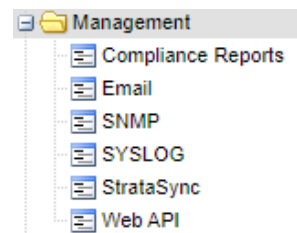
Compliance Reports

The **Compliance Reports** feature requires a license, which must be renewed annually. It analyzes the EASyCAP logs to determine compliance with EAS regulations. Reports are automatically generated at the end of each week and at the end of each month. Each EAS and CAP source that's configured for **Compliance Reporting** is analyzed to determine if all required tests (or equivalent messages) have been received. The EASyCAP is also analyzed to make sure that all required messages are transmitted. The reports are sent to all Email recipients that have been configured to receive **Compliance Reports**.

Configure Email recipients to receive reports by going to the **Management | Email** screen and enabling **Compliance Reports** for each recipient that should receive reports.

Configure the EAS and CAP sources to analyze for compliance by going to the configuration screen for each source and selecting the appropriate **Compliance Reporting** setting.

To view or configure Compliance Reports, select the **Compliance Reports** link from the **Management** folder.

Settings Tab

Enable Compliance Reports – Enable or disable the Compliance Reports feature.

This EASyCAP is acting as a remote radio receiver – Enable this option for EASyCAP Encoder/Decoders that do not transmit alerts to the public. This is typically only applicable for units installed to remotely receive radio stations and relay alerts to upstream EASyCAP Encoder/Decoders.

EASyCAP Encoder/Decoder User's Guide
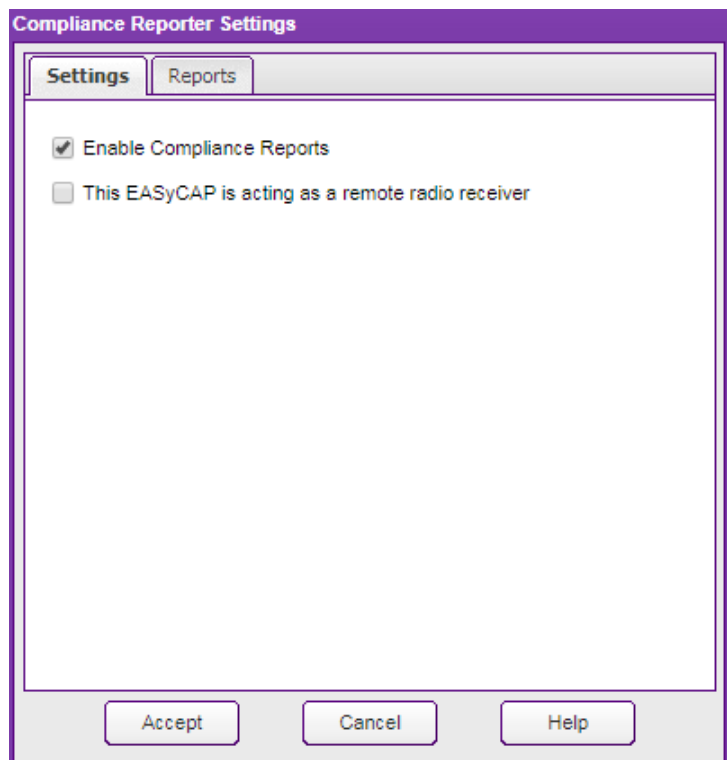
Reports Tab

Setup the report time period using the **Month**, **Day**, and **Year** edit-boxes. This date will be used to determine the start and end dates for the weekly and monthly reports.

This Week, **Last Week**, **This Month**, and **Last Month** buttons will set the **Month**, **Day**, and **Year** edit-boxes to the selected time period.

Generate Weekly Report – Generates a weekly compliance report for the configured time period. The report will be shown in a new browser window (pop-ups must be allowed). If **Generate Calendar** is checked, a Calendar will also be generated and a link to the Calendar file will be shown below the button.

Generate Monthly Report – Generates a monthly compliance report for the configured time period. The report will be shown in a new browser window (pop-ups must be allowed). If **Generate Calendar** is checked, a Calendar will also be generated and a link to the Calendar file will be shown below the button.

Check for Problems – Generate a report to identify problems with the configuration and reception. Configuration will be checked to verify that required events are enabled, locations are selected, and that EAS and CAP sources are setup. It will also verify that messages were received from the configured EAS and CAP sources.

Press the **Accept** button to save changes to the configuration or choose **Cancel** to exit without saving configuration changes.

Email

This feature provides the ability to deliver Email notifications to a list of recipients. To view or configure Email, select the **Email** link from the **Management** folder.

Email Server Settings

> **Use Viavi's Hosted Email Server** – Enable this checkbox to use Viavi's hosted Email server.
>
> **Security** – Select the security required for the connection.
>
> > **Connection Not Secure** – The connection to the SMTP server will not use security protocols.
> >
> > **Negotiate Secure Connection** – A secure connection will be used when the SMTP server reports that it supports TLS.
> >
> > **Require Secure Connection** – A secure connection will always be used to connect to the SMTP server. Select this setting when using GMail.

SMTP Port – Enter the SMTP port (default is 25). If using GMail set the port to 465

SMTP Server – Enter the SMTP server URL.

Email Address for Outgoing Mail – Enter the Email address used for outgoing mail.

Username – Enter the username required to login to the SMTP server.

Password – Enter the password required to login to the SMTP server.

Confirm Password – Enter the password again for verification.

Heartbeat Rate – Enter the number of hours between heartbeat Emails.

> ⚠️ **CAUTION**
> *You must have an active support license to use the Viavi Hosted Email Server, and it will be limited to 100 Emails a day. Note that if your support license expires, Emails will not be sent until an updated support license is installed.*

> 📌 **NOTE**
> *If using a GMail SMTP server, the GMail account will need to be configured to "Allow less secure apps". See GMail support for more details.*

Email Recipients

Email Recipient – Select the Email recipient to edit or view from the drop-down box.

Add – Add a new Email recipient.

Delete – Delete the selected Email recipient.

Type of Recipient – For normal Email recipients, select Standard Email, otherwise choose the appropriate SMS/MMS provider.

Email Address – Enter the Email address of the recipient. For SMS/MMS, enter the recipient's phone number, including area code.

Description – Enter a name to display for this Email recipient.

Heartbeat and Startup Notifications – Select this option to deliver heartbeat and startup Emails to the selected recipient.

CAP Source Status Notifications – Select this option to deliver an Email when the connection to a CAP source is lost.

EAS Source Status Notifications – Select this option to deliver an Email when an EAS source loses audio signal, or when an EAS source detects an audio signal.

Message Delivery Error Notifications – Select this option to send an Email when a message cannot be delivered to an external device (server, character generator, switch).

System Error Notifications – Select this option to send an Email when a system error occurs, for example when a critical process becomes unresponsive.

Message Playback Notifications – Select this option to send an Email when message playback begins.

Weekly Logs – Select this option to send an Email every Sunday at midnight containing the previous weeks logs.

Compliance Reports – Select this option to send Compliance Reports at the end of each week and at the end of each month (a valid Compliance Report license is required).

Login Attempts – Select this option to deliver an Email when an attempt is made to login to the EASyCAP Web Server.

Press the **Test** button to send a test Email to all configured recipients.

Press the **Accept** button to save changes to the configuration or choose **Cancel** to exit without saving changes.

SNMP

The EASyCAP® SNMP feature is MIB-II (RFC 1213) compliant and supports the HOST-RESOURCES (RFC 2790) MIB, UCD-SNMP MIBs, and the EASyCAP® MIB. The SNMP feature requires a Network Management License.

To configure SNMP, select the **SNMP** link from the **Management** folder.

SNMP Agent Settings

    Enable SNMP Agent – Enable SNMP.

    USE TCP Transport – Select this option to use a TCP transport for SNMP GET and SET operations. UDP is the recommended transport.

    Allow Abort Operations – Select to allow users to Abort (and Confirm) messages via SNMP SET operations.

    Allow EAS Origination Operations – Select to allow users to originate EAS messages via SNMP SET operations.

    Agent Port – Enter the SNMP Agent port (default is 161).

    Heartbeat Rate – Enter the number of minutes between heartbeat traps.

    Read-Only Community – Enter the community string for read-only access.

    Read-Write Community – Enter the community string for read and write access.

    System Location – Enter the system location for the MIB-II system group.

    System Contact – Enter the system contact for the MIB-II system group.

SNMP Trap Recipients

Trap Recipient – Select the SNMP Trap recipient to edit or view.

Add – Add a new Trap recipient.

Delete – Delete the selected Trap recipient.

Description – Enter a name to display for this Trap recipient.

IP Address or URL – Enter the IP address or URL for the selected Trap recipient.

Port – Enter the port used for sending SNMP Traps (default is 162).

Community – Enter the community string for Traps delivered to the selected recipient.

Heartbeat and Startup Notifications – Select this option to deliver heartbeat and startup Traps to the selected recipient.

Hardware Monitoring Notifications – Select this option to send hardware monitoring alarms, for example a fan failure or over temperature condition.

System Notifications – Select this option to send system information and error Traps, for example when a user logs into the web server.

EAS/CAP Source Status Notifications – Select this option to deliver a Trap when the connection to a CAP source is lost, when an EAS source loses audio signal, and when an EAS source detects an audio signal.

Message Delivery Notifications – Select this option to send a Trap when a message is successfully delivered to an external device (server, character generator, switch).

Message Delivery Error Notifications – Select this option to send a Trap when a message cannot be delivered to an external device (server, character generator, switch).

Message Playback Notifications – Select this option to send an EMail when message playback begins.

Rejected Alert Notifications – Select this option to send a Trap when a received alert message is rejected.

Press the **EASyCAP MIB** link to view the EASyCAP MIB.

Press the **Accept** button to save changes to the configuration or choose **Cancel** to exit without saving changes.

SYSLOG

The SYSLOG feature adds the ability to send syslog messages to remote servers for monitoring and centralized logging. Syslog cannot be used for the EAS log required by the FCC. A Network Management License is required.

General Settings

> **Enable SYSLOG** – Enable SYSLOG to send syslog logs to the configured recipients.

> **Enable EASyCAP Debug Log** – Enable debug log files to help with troubleshooting.

Enable Web Server Error Log – Enable the Web Server error log.

Enable Web Server Access Log – Enable the Web Server access log, which will include information about client requests and access to the EASyCAP Web Server.

Enable MPEG-DASH access log – Enable the MPEG-DASH access log, which will include information about client requests for MPEG-DASH manifests and media.

Heartbeat Rate – Enter the number of minutes between heartbeat messages.

SYSLOG Recipients

> **SYSLOG Recipient** – Select the SYSLOG recipient to edit or view.
>> **Add** – Add a new SYSLOG recipient.
>> **Delete** – Delete the selected SYSLOG recipient.

> **Description** – Enter a name to display for this SYSLOG recipient.

> **IP Address or URL** – Enter the IP address or URL for the selected SYSLOG recipient.

> **Port** – Enter the port used for sending SYSLOG messages (default is 514).

> **Log Priorities** – Set the desired log priority for each syslog facility. Log messages with the configured priority and higher will be delivered to the recipient. Set the priority to **none** to disable logs for that facility.

Press **Accept** to save configuration changes or choose **Cancel** to exit without saving.

Web API

The Web API feature provides interfaces to several Web Services and Atom feeds. An Atom CAP Server or Network Management license is required. Note that a user account must be configured with permission to use the **Web API** and the Web Service clients must use these login credentials. For details on available Web Services see the EASyCAP® Web API document.

Enable the Atom CAP Server – Enable the **Atom CAP Server** to provide an IPAWS Open style Atom feed that includes all received EAS, CAP, and locally generated messages. Requires an Atom CAP Server license.

Enable the Alert Log Web Service – When enabled, a Web Service is available to allow https clients to retrieve logs in text and JSON format. Requires a Network Management license.

Enable the Operations Web Service – When enabled, a Web Service is available to allow https clients to perform operations like aborting a message in progress or confirming a pending message. Requires a Network Management license.

Enable the Status Web Service and Atom Feed – When enabled, a Web Service is available to https clients to retrieve status information about message activations and CAP/EAS sources. An Atom feed is also provided, allowing any standard RSS or Atom feed software to be used to monitor the status of message activations and CAP/EAS sources. Requires a Network Management license.

Press the **Save** button to save any configuration changes. You may need to refresh your Web Browser after pressing **Save** because the Web Server was restarted.

Press the **Close** button to exit the Web API Settings window.
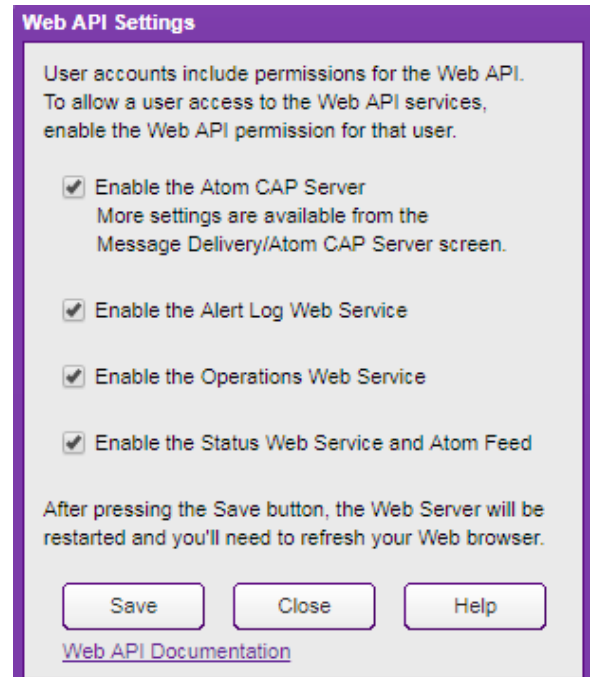
Logs

Expand the Logs folder in the Navigation bar by clicking the + sign next to the Logs folder.
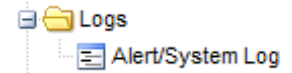
Alert/ System Log

To view the alert and system logs of the EASyCAP®, select the **Alert/System Log** link in the **Logs** folder.

Log Options

The **Options** tab provides settings to configure the type of information that will be included in the log

Alert Logs to View

These settings determine what type of messages will be included in the alert log.

CAP messages – Enable this option to include CAP messages.

EAS messages – Enable this option to include EAS messages.

Locally Generated – Enable this option to include messages that were manually generated by an operator, or automatically generated Required Weekly Tests.

Duplicate messages – Enable this option to include duplicate messages.

Expired messages – Enable this option to include expired messages.

Alerts rejected because events not configured – Enable this option to include messages that were not transmitted because the alert event was not configured.

Alerts rejected because locations not configured – Enable this option to include messages that were not transmitted because the alert did not include any configured locations.

CAP Updates – Enable this option to include CAP Update messages.

CAP Cancellations – Enable this option to include CAP Cancellation messages.
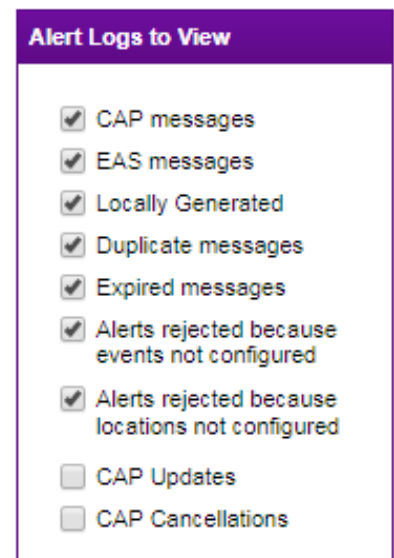
Optional Log Information

These settings determine what optional information to include in the alert log.

CAP Identifier elements – Enable this option to include the CAP Sender, Identifier, and Sent elements.

Show all time details – Enable this option to include detailed time information for all receive and transmit operations.

Successful Deliveries – Enable this option to include information about messages that were successfully delivered to downstream clients.
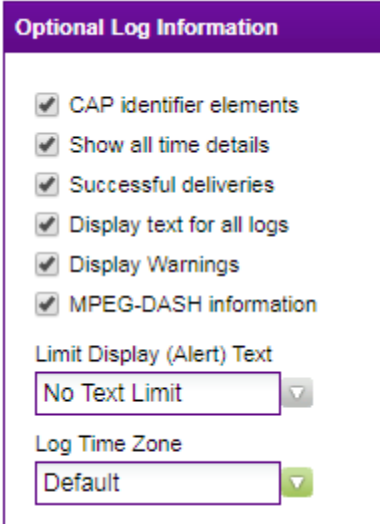
Display text for all logs – Enable this option to display the alert text for all messages. If disabled, alert text will only be shown for messages that were transmitted.

Display Warnings – Enable this option to include warnings that occurred during message processing, for example the audio could not be retrieved and so text-to-speech was used.

MPEG-DASH Information – Enable this option to include information about MPEG-DASH media produced for alert messages.

Limit Display (Alert) Text – Specify the maximum length of the alert text that's included in the logs.

Log Time Zone – Specify which time zone to use for the log. This should normally be left at Default, which will use the time zone of the EASyCAP.

System Logs to View

These settings determine what type of messages will be included in the system log.
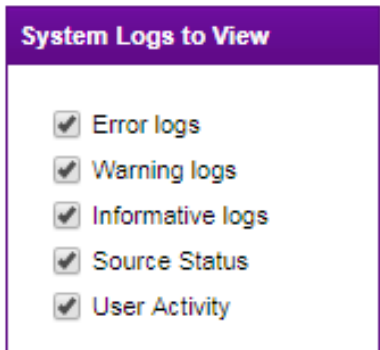
Error logs – Enable this option to include error messages.

Warning logs – Enable this option to include warning messages.

Informative logs – Enable this option to include non-critical informative messages.

Source Status – Enable this option to include EAS and CAP source status messages.

User Activity – Enable this option to include information about user activity, for example login attempts and failures.

Alert Log

Select **Alert Log** from the **Log Type** drop-down list to view a log of alert messages.

Set the time period of the log by selecting the **Start Date** and **End Date**.

Press the **Update** button to create and view the log.

Buttons are provided to quickly create and view logs for today, this week, last week, this month, and last month. The **Start Date** and **End Date** will be entered automatically.
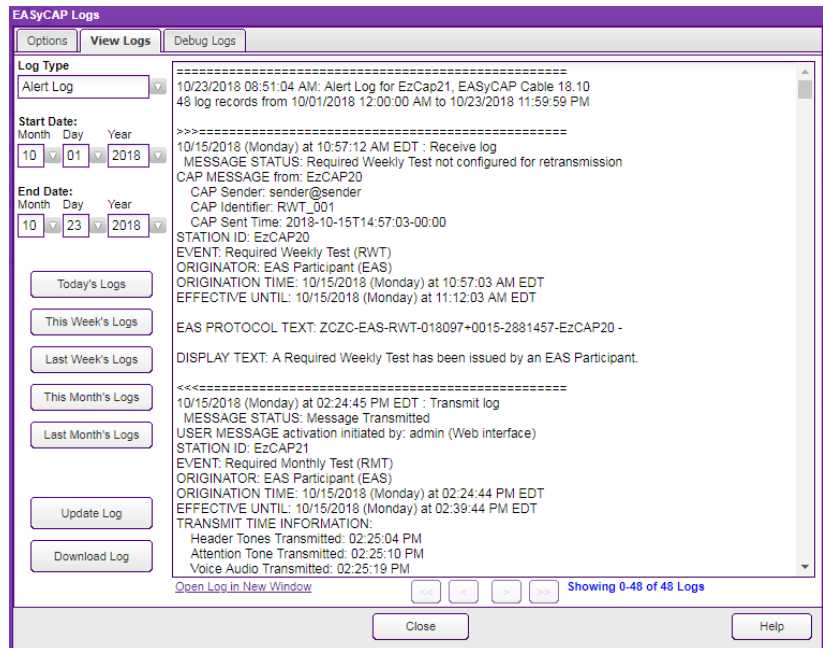
The alert log will be displayed as shown above. One hundred log records are displayed at a time. Use the << (First), < (Previous), > (Next), and >> (Last) buttons to navigate through all of the log records.

Click the **Open Log in New Window** link to view the log text in a separate browser window.

Press the **Download** button to download a copy of the alert log as an ASCII text file.

System Log

Select **System Log** from the **Log Type** drop-down list to view a log of general system and application information.

Set the time period of the log by selecting the **Start Date** and **End Date**.

Press the **Update** button to create and view the log.

Buttons are provided to quickly create and view logs for today, this week, last week, this month, and last month. The **Start Date** and **End Date** will be entered automatically.
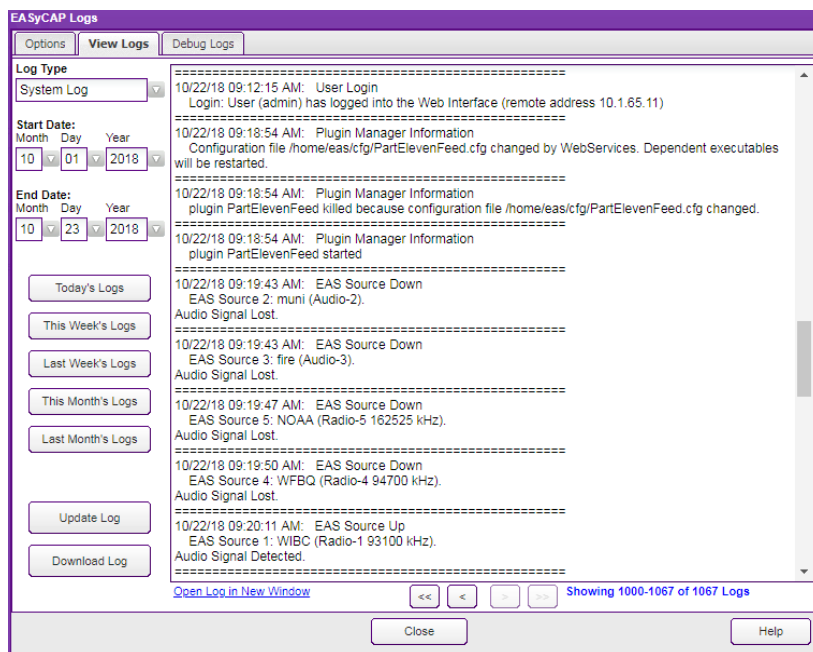
The system log will be displayed as shown above. One hundred log records are displayed at a time. Use the << (First), < (Previous), > (Next), and >> (Last) buttons to navigate through all of the log records.

Click the **Open Log in New Window** link to view the log text in a separate browser window.

Press the **Download** button to download a copy of the system log as an ASCII text file.

Click **Close** to close the **EASyCAP Logs** screen.

Debug Logs

Select the **Debug Logs** tab to view available debug, access, and error logs.

> **NOTE**
> *Debug, error, and access logs will not be available until they are enabled from the SYSLOG configuration screen.*

Select Debug Log - Select a debug, error, or access log to view. The following logs may be available.

    EASyCAP Receive Debug - Includes debug information from processes that receive EAS and CAP alert messages.

    EASyCAP Transmit Debug - Includes debug information from processes that deliver alert messages to downstream servers and devices, such as SCTE-18 and DNCS recipients.

    Web Server Error Log - Includes information about Web Server errors.

    Web Server Access Log - Includes information about client access to the Web Server.

    MPEG-DASH Access Log - Includes client requests for MPEG-DASH manifests and media.

View Debug Log - Display the selected log. The log will be shown in a new window, so you may need to configure your Web browser to allow popups.
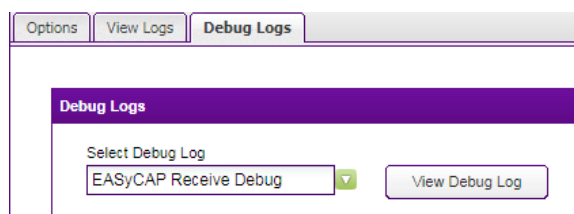
Operations

Expand the **Operations** folder in the Navigation bar by clicking the **+** sign next to the folder.
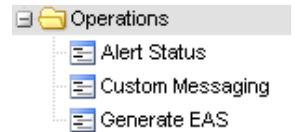
Alert Status Monitor

To view the Alert Status Monitor of the Encoder/Decoder, select **Alert Status** in the **Operations** folder. The **Alert Status Monitor** window will be displayed. This window has three tabs; Alert Status, EAS Input Status, and IPAWS Atom Feed Status.
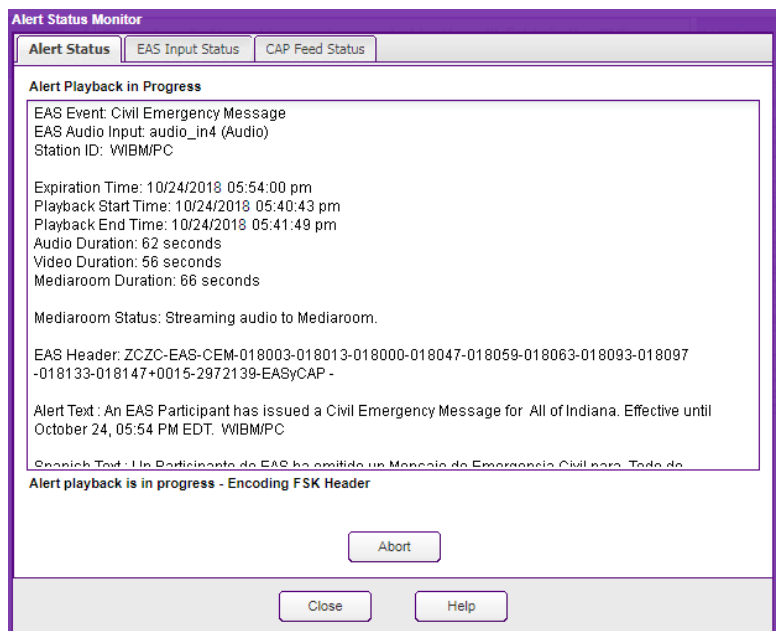
Alert Status Tab

The **Alert Status** screen provides the current status of EAS activations as well as a means to abort the current alert message. The status shown in your Web Browser is periodically updated. You can configure how often to update the status information by going to the **Web Services Configuration** screen and changing the value for the Status Timer.

During an EAS activation, the operator can view information about the alert in progress, including: EAS Event; EAS header text; expiration time; audio duration; and alert text.

An **Abort** button is provided to allow the operator to abort the alert that's in progress.

EAS Input Status Tab

The EAS Input Status tab displays the date and time that the Monitor was last updated and displays the status of each input channel. The same information shown on the front panel LCD can be viewed here.
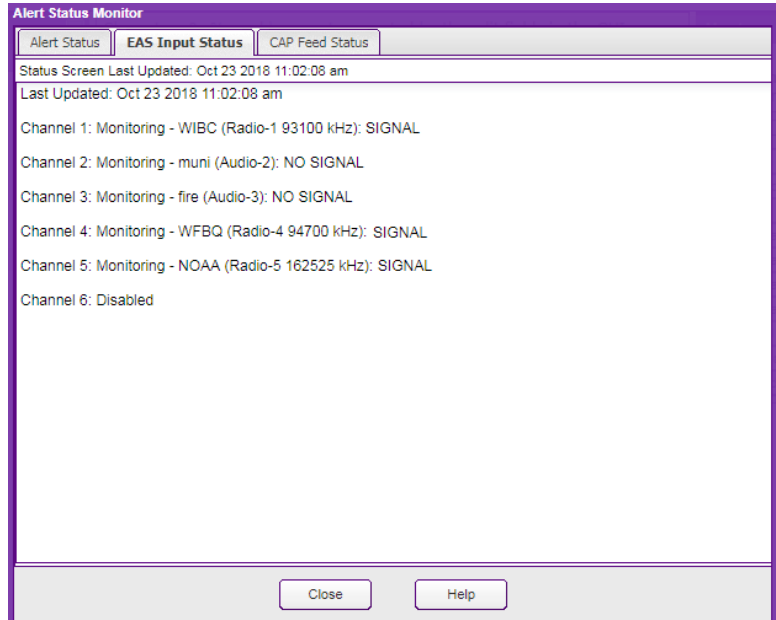
CAP Feed Status Tab

The CAP Feed Status tab displays the date and time that the Monitor was last updated and displays the status of each configured CAP feed.
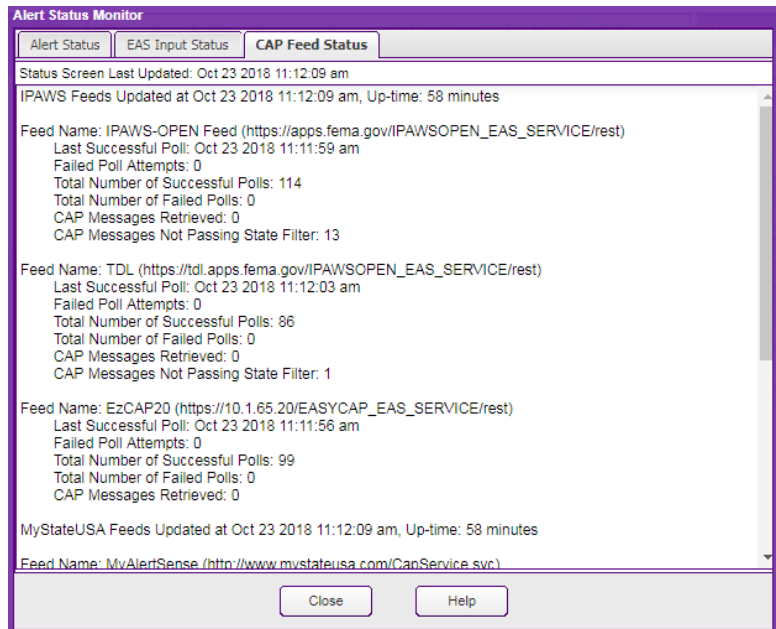
Click **Close** to close the **Alert Status Monitor** window.

Custom Messaging

To generate custom messages, click **Custom Messaging** in the **Operations** folder. The **Custom Messaging** window will appear. Note that the EASyCAP® must be licensed for Custom Messaging.

- **English/Spanish Text Message** – Enter a custom text message in English and Spanish in the text box for the desired language. The text is limited to 1750 characters. Do not use characters &, %, or /.

- **Upload English/Spanish Audio** – Upload an audio file for the message. Press the **Upload English Audio** or **Upload Spanish Audio** button. The **Audio File Upload** window will be displayed. Press the **Browse** (or **Choose File**) button to select an audio file and then press the **Upload** button. A **Preview Audio** link will appear after audio has been uploaded to allow you to listen to the audio from your web browser.

- **No Audio - Text Only** – Select this check-box to guarantee that audio is not played during the custom message. If text-to-speech is enabled, this option will prevent it from being generated.

Load Default Message – Press this button to load the default custom text and audio that were previously saved.

Save Default Message – Press this button to save the custom text message and audio file that are currently loaded. These files are saved with your user account so that they can be loaded later. The default audio file can also be used when originating a message from a telephone.

Press the **Start Message** button to start the custom message.

Press the **Close** button to exit the **Custom Messaging** window.

Generate EAS

To generate EAS messages, click **Generate EAS** in the **Operations** folder. The **Generate EAS Messages** window will appear.

- **EAS Event** – Select the EAS event that you want to generate from the dropdown menu.

- **Duration** – Enter the EAS duration for the message.

- **Upload English/Spanish Audio** – Upload English and Spanish audio files for the message. Press the **Upload English Audio** or **Upload Spanish Audio** button. The **Audio File Upload** window will be displayed. Press the **Browse** (or **Choose File**) button to select an audio file and then press the **Upload** button. A **Preview Audio** link will appear after audio has been uploaded to allow you to listen to the audio from your web browser.

- **Locations** – Click the checkboxes to select the locations that are included in the EAS message.

- **Custom English/Spanish Text** – Enter custom text in English and Spanish for the EAS message. The custom text will be appended to the normal EAS translation text. Do not use characters &, %, or /. Note that the EASyCAP® must be licensed for Custom Messaging before this option can be used.

Press the **Send EAS Message** button to generate the EAS message.

Press the **Close** button to exit the **Generate EAS Messages** window.

Telephone Interface

The EASyCAP® Telephone Interface allows operators or emergency management personnel to activate and abort messages by dialing into an EASyCAP® Encoder/Decoder equipped with a Telephone interface option board. It can be used to generate EAS messages, custom (non-EAS) messages, and to abort messages in progress. Each user is assigned a personal identification number (PIN) by the EASyCAP® administrator. This PIN is required to authenticate telephone users. Each user is also assigned one or more location codes so that messages can be routed to specific areas based on the user that's logged in.

> **NOTE**
>
> ***These instructions provide too much detail to be used during an emergency. The EASyCAP administrator is encouraged to make a short instruction sheet for telephone users to follow. It should contain the telephone number, PIN (if allowed to be documented), and sequence of keys and prompts that will activate the EASyCAP.***

User Prompts

Three tones are used by the EASyCAP® to provide feedback to the telephone user.

- **ACK** – A low to high tone indicating success or an accepted command
- **NACK** – A discordant high to low tone indicating rejection of a command
- **BEEP** – A 1 KHz tone used to prompt the user for a PIN, or to record a message

Command Keys

Command keys may be zero through nine, as well as

The pound key, used to enter a command (or the PIN)

* The asterisk key, used to cancel a command sequence if a mistake is made

Operations

All operations are initiated by using a 2-digit command. The following lists the available operations:

- 00# Hang-up the Telephone
- 01# Abort the message in progress
- 02# Record and save a user audio message
- 10# Activate a custom (non-EAS) message
- 11# - 62#   Activate an EAS message
        The 2-digit command corresponds to an EAS Event, see list below.

Dial-up and Authentication

To use the telephone interface, dial the number for the telephone line connected to the EASyCAP® and wait for the **BEEP** prompt. After the prompt, enter your (4 to 8 digit) PIN number followed by the **#** key.

- Dial the Telephone number for the EASyCAP
- Wait until Telephone is answered and a **BEEP** is heard
- Enter your PIN number followed by the **#** key

Once the **#** key is pressed, an **ACK** prompt will indicate a successful login, or a **NACK** prompt will indicate that the PIN is invalid or that user permissions are insufficient. Three attempts to enter the correct PIN are allowed before the EASyCAP® hangs up.

Hang-up Telephone

Always issue the hang-up command before hanging up the Telephone to guarantee that the EASyCAP's Telephone line is on-hook and it is ready to accept a new call.

To command the EASyCAP to hang-up the Telephone, enter **00** followed by the **#** key. The EASyCAP will play an **ACK** prompt and then hang up the Telephone.

- Enter **00** followed by the **#** key
- Wait until the **ACK** prompt is heard and the Telephone is hung up

Abort Message in Progress

To abort a message that's in progress, enter **01** followed by the **#** key.

- Enter **01** followed by the **#** key
- Wait until the **ACK** or **NACK** prompt is heard

An **ACK** prompt indicates that the message in progress was successfully aborted. A **NACK** prompt indicates that the message was not aborted. This is normally caused by the user account not having permission to abort messages from the Telephone.

Record User Audio Message

One default user audio message can be saved for each user. It is saved into permanent storage so that it can be quickly loaded and used for message activations. The audio message has a maximum duration of two minutes. Note that this is the same default audio message used by the Web Interface for custom messaging.

To record the user audio message, enter **02** followed by the **#** key.

- Enter **02** followed by the **#** key
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
  - If a **NACK** prompt is heard, the operation failed (normally because a message is in progress)
- Speak into the Telephone, a maximum of 2 minutes can be recorded
- Press the **#** key to stop recording audio
  - Press the ***** key to cancel the recording and delete the audio message
- Wait until the **ACK** prompt is heard

Activate a Custom (Non-EAS) Message

Custom (non-EAS) messages can be activated from the Telephone interface. The Web Interface provides the ability to save one default audio and one default text message for each user account. The default audio and text messages can be programmed and saved from the Web Interface's **Custom Messaging** page (go to the **Operations** folder and select the **Custom Messaging** link). This allows the operator to preload an audio and text message which can be activated later from the Telephone. If a default custom text message has not been saved, the text message displayed when a Custom Message is activated from the Telephone will be as follows: "A community access message is in progress. Listen to the audio on this channel for detailed information."

To activate a custom (non-EAS) message that uses audio recorded from the Telephone, enter **10** followed by the **#** key.

- Enter **10** followed by the **#** key
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
  - A **NACK** prompt is heard if the operation failed (because a message is in progress)
- Record the audio message by speaking into the Telephone (2 minutes maximum)
- Press the **#** key to stop recording audio
  - Press the ***** key to cancel the message activation and delete the audio
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

The command to activate a custom (non-EAS) message can optionally include an additional parameter to setup the type of audio used.

Audio Option (third digit of the command)

The user can optionally specify what type of audio is used for the message by entering a third digit in the command. This parameter is optional. If it's not included the message will default to using audio recorded from the Telephone.

- 0 Use audio recorded from the Telephone
     This is the default and is used if the audio option is not specified

- 1 Use the pre-recorded default user audio message

- 2 Use text-to-speech
     Note that this option only functions if the EASyCAP text-to-speech is enabled

- 3 No audio (text only)

To activate a custom (non-EAS) message that uses the pre-recorded default audio message, enter **101** followed by the **#** key.

- Enter **101** followed by the **#** key

- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

To activate a custom message that uses text-to-speech, enter **102** followed by the **#** key.

- Enter **102** followed by the **#** key

- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

To activate a text-only custom message that does not include audio, enter **103** followed by the **#** key.

- Enter **103** followed by the **#** key

- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Activate EAS Message

EAS messages can be activated from the Telephone interface. A two-digit command is provided for each EAS Event code (see list below). Two additional digits can be optionally included to select the audio type and message duration. The user's configured locations determine which FIPS codes are included in the EAS message.

EAS Message Commands (first two digits of the command)

- 11 Required Monthly Test
- 12 Required Weekly Test
- 13 Administrative Message
- 14 Avalanche Watch
- 15 Avalanche Warning
- 16 Blue Alert
- 17 Blizzard Warning
- 18 Child Abduction Emergency
- 19 Civil Danger Warning
- 20 Civil Emergency Message
- 21 Coastal Flood Watch
- 22 Coastal Flood Warning
- 23 Practice/Demo Warning
- 24 Dust Storm Warning
- 25 Earthquake Warning
- 26 Evacuation Immediate
- 27 Extreme Wind Warning
- 28 Flash Flood Statement
- 29 Flash Flood Watch
- 30 Flash Flood Warning
- 31 Flood Statement
- 32 Flood Watch
- 33 Flood Warning
- 34 Fire Warning
- 35 Hazardous Materials Warning
- 36 Hurricane Statement
- 37 Hurricane Watch
- 38 Hurricane Warning

- 39 High Wind Watch
- 40 High Wind Warning
- 41 Local Area Emergency
- 42 Law Enforcement Warning
- 43 National Information Center Message
- 44 Network Message Notification

- 45 National Periodic Test
- 46 Nuclear Power Plant Warning
- 47 Radiological Hazard Warning
- 48 Special Marine Warning
- 49 Special Weather Statement
- 50 Shelter in Place Warning
- 51 Storm Surge Watch
- 52 Storm Surge Warning
- 53 Severe Thunderstorm Watch
- 54 Severe Thunderstorm Warning
- 55 Severe Weather Statement
- 56 911 Telephone Outage Emergency
- 57 Tornado Watch
- 58 Tornado Warning
- 59 Tropical Storm Watch
- 60 Tropical Storm Warning
- 61 Tsunami Watch
- 62 Tsunami Warning
- 63 Volcano Warning
- 64 Winter Storm Watch
- 65 Winter Storm Warning

Audio Option (third digit of the command)

You can optionally specify what type of audio is used for the message by entering a third digit in the command. This option defaults to audio recorded from the Telephone.

- 0 Record audio from the Telephone (default, used if audio option is not specified)
- 1 Use the pre-recorded default user audio message
- 2 Use text-to-speech

Duration Option (fourth digit of the command)

You can optionally specify the duration of the EAS message. This parameter is optional. If it's not included the message will default to using a 15 minute duration.

- 0   15 minute duration (Default, used if the duration option is not specified)
- 1-9 the duration in hours (1 sets the duration to 1 hour, 9 sets a 9 hour duration)

Example: Activate RWT with 15 minute duration

To activate a Required Weekly Test message with a 15 minute duration, enter **12** followed by the **#** key.

- Enter **12** followed by the **#** key
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Example: Activate RMT with audio from Telephone and 15 minute duration

To activate a Required Monthly Test message with a 15 minute duration and audio recorded from the Telephone, enter **11** followed by the **#** key.

- Enter **11** followed by the **#** key
    - The first two digits (**11**) activates an RMT message
    - The audio option (third digit) is omitted so the default is used (Telephone audio)
    - The duration option (fourth digit) is omitted so the default is used (15 minutes)
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
    - A **NACK** prompt is heard if the operation failed (because a message is in progress)
- Record the audio message by speaking into the Telephone (2 minutes maximum)
- Press the **#** key to stop recording audio
    - Press the ***** key to cancel the message activation and delete the audio
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Example: Activate Flood Watch with text-to-speech audio and a 1 hour duration

To activate a Flood Watch message with text-to-speech audio and a 1 hour duration, enter **3221** followed by the **#** key.

- Enter **3221** followed by the **#** key
    - The first two digits (**32**) activates a Flood Watch (FLA) message
    - The third digit (**2**) selects text-to-speech audio
    - The fourth digit (**1**) selects a 1 hour duration
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

IPTV Specifications (Series 20)

General Specifications

EAS Encoder/Decoder compliant with all requirements defined in Part 11 of the FCC rules.

Operating Temperature: 0 to +50 C

Max. Operating Humidity: 95%

Supply Voltage: 117 VAC +/- 15%

Current: 600 mA

Weight: 20 pounds

Chassis

2U RU chassis with 3.5" 320x240 color touch-screen LCD and speaker on the Front Panel

Dimensions (H x W x D): 3.5 x 19 x 15.25

Communications

(2) RS-232 serial ports available on male DB-9 connectors

(4) USB ports

(2) 10/100/1000 Ethernet ports available on USB/RJ45 combo jacks

(2) 10/100 BaseT Ethernet ports

(1) Telephone port

Audio

(6) Balanced 600 Ohm audio inputs for EAS monitoring. Each input can be configured for external audio or an optional internal radio receiver

(2) Balanced analog audio outputs, 600 Ohm

(1) Balanced stereo analog audio switch, 600 Ohm

Video

NTSC video character generator

RS-170A color analog video (source only, does not overlay onto video)

Analog video switch with video bypass for fail-safe operation

General Purpose Inputs and Outputs

(6) General purpose outputs: isolated relay, maximum rating 1A @ 30 VDC

(2) TTL outputs: each TTL output can drive 2 TTL loads

(4) General purpose inputs: optically isolated dry contact closure inputs

Radio Receivers

(6) Radio receivers, each can be configured as AM, FM, or NOAA

Minimum RF Input:	AM 31 dBμV, FM 31 dBμV, NOAA 25 dBμV
Maximum RF Input:	60 dBμV
Frequency Range:	AM 520 to 1720 kHz, FM 87.5 to 108 MHz, NOAA 162.4 to 162.55 MHz

* Due to ambient noise and interference, signal strength greater than the minimum may be required for good reception.

Certifications

• FCC Part 11 EAS Encoder/Decoder (FCC ID: P4V-EASYCAP-1)

• FCC Part 15

• NEBS Level 1

IPTV Specifications (Series 30)

General Specifications

EAS Encoder/Decoder compliant with all requirements defined in Part 11 of the FCC rules.

Operating Temperature: 0 to +50 C

Max. Operating Humidity: 95%

Supply Voltage: 117 VAC +/- 15%

Current: 200 mA

Weight: 8.5 pounds

Chassis

2U RU chassis with 3.5" 320x240 color touch-screen LCD and speaker on the Front Panel

Dimensions (H x W x D): 3.5 x 19 x 11

Communications

(2) RS-232 serial ports available on male DB-9 connectors

(4) USB ports

(2) 10/100/1000 Ethernet ports available on USB/RJ45 combo jacks

(2) 10/100 BaseT Ethernet ports

(1) Telephone port

Audio

(4) Balanced 600 Ohm audio inputs for EAS monitoring. Each input can be configured for external audio or an optional internal radio receiver

(2) Balanced analog audio outputs, 600 Ohm

(1) Balanced stereo analog audio switch, 600 Ohm

Video

NTSC video character generator

RS-170A color analog video (source only, does not overlay onto video)

General Purpose Inputs and Outputs

(4) General purpose outputs: isolated relay, maximum rating of 1A @ 30 VDC

(1) TTL output: can drive 2 TTL loads

(2) General purpose inputs

Radio Receivers

(6) Radio receivers, each can be configured as AM, FM, or NOAA

Minimum RF Input:	AM 31 dBµV, FM 31 dBµV, NOAA 25 dBµV
Maximum RF Input:	60 dBµV
Frequency Range:	AM 520 to 1720 kHz, FM 87.5 to 108 MHz, NOAA 162.4 to 162.55 MHz

* Due to ambient noise and interference, signal strength greater than the minimum may be required for good reception.

Certifications

- FCC Part 11 EAS Encoder/Decoder (FCC ID: P4V-EASYCAP-1)

- FCC Part 15

- NEBS Level 1 and Level 3 (depending on the model)

Specifications (Series 20)

General Specifications

EAS Encoder/Decoder compliant with all requirements defined in Part 11 of the FCC rules.

Operating Temperature: 0 to +50 C

Max. Operating Humidity: 95%

Supply Voltage: 117 VAC +/- 15%

Current: 600 mA

Weight: 20 pounds

Chassis

2U RU chassis with 3.5" 320x240 color touch-screen LCD and speaker on the Front Panel

Dimensions (H x W x D): 3.5 x 19 x 15.25

Communications

(2) RS-232 serial ports available on male DB-9 connectors

(4) USB ports

(2) 10/100/1000 Ethernet ports available on USB/RJ45 combo jacks

Audio

(6) Balanced 600 Ohm audio inputs for EAS monitoring. Each input can be configured for external audio or an optional internal radio receiver

(2) Balanced analog audio outputs, 600 Ohm

(1) Balanced stereo analog audio switch, 600 Ohm

Video

NTSC video character generator

RS-170A color analog video (source only, does not overlay onto video)

Analog video switch with video bypass for fail-safe operation

General Purpose Inputs and Outputs

(6) General purpose outputs: isolated relay, maximum rating of 1A @ 30 VDC

(2) TTL outputs: each TTL output can drive 2 TTL loads

(4) General purpose inputs: optically isolated dry contact closure inputs

Radio Receivers

(2) Radio receiver boards can be installed into the EASyCAP®

(3) Radio receivers are installed per board, each can be configured as AM, FM, or NOAA

Minimum RF Input:	AM 31 dBµV, FM 31 dBµV, NOAA 25 dBµV
Maximum RF Input:	60 dBµV
Frequency Range:	AM 520 to 1720 kHz, FM 87.5 to 108 MHz, NOAA 162.4 to 162.55 MHz

* Due to ambient noise and interference, signal strength greater than the minimum may be required for good reception.

Specifications (Series 30)

General Specifications

EAS Encoder/Decoder compliant with all requirements defined in Part 11 of the FCC rules.

Operating Temperature: 0 to +50 C

Max. Operating Humidity: 95%

Supply Voltage: 117 VAC +/- 15%

Current: 200 mA

Weight: 8.5 pounds

Chassis

2U RU chassis with 3.5" 320x240 color touch-screen LCD and speaker on the Front Panel

Dimensions (H x W x D): 3.5 x 19 x 11

Communications

(2) RS-232 serial ports available on male DB-9 connectors

(4) USB ports

(2) 10/100/1000 Ethernet ports available on USB/RJ45 combo jacks

Audio

(4) Balanced 600 Ohm audio inputs for EAS monitoring. Each input can be configured for external audio or an optional internal radio receiver

(2) Balanced analog audio outputs, 600 Ohm

(1) Balanced stereo analog audio switch, 600 Ohm

Video

NTSC video character generator

RS-170A color analog video (source only, does not overlay onto video)

General Purpose Inputs and Outputs

(4) General purpose outputs: isolated relay, maximum rating of 1A @ 30 VDC

(1) TTL output: can drive 2 TTL loads

(2) General purpose inputs

Radio Receivers

(2) Radio receiver boards can be installed into the EASyCAP®

(3) Radio receivers are installed per board, each can be configured as AM, FM, or NOAA

Minimum RF Input:	AM 31 dBµV, FM 31 dBµV, NOAA 25 dBµV
Maximum RF Input:	60 dBµV
Frequency Range:	AM 520 to 1720 kHz, FM 87.5 to 108 MHz, NOAA 162.4 to 162.55 MHz

* Due to ambient noise and interference, signal strength greater than the minimum may be required for good reception.

Specifications for Optional Expansion Boards

AES-EBU Digital Audio Board

(2) AES-EBU digital audio switches: each switch provides a pair of channels, 110 Ohm XLR

Alert audio automatically locks to the incoming bit rate and sample rate (up to 192 KHz)

PCI-Express Expansion

(1) PCI-Express card can be installed to provide additional capabilities such as SDI video, MPEG-2, MPEG-4, audio, video, or other capabilities.

Supported PCI-Express cards must be purchased from VIAVI.

SDI Video Output Board

* Note that the SDI Video Output board is only available for Series 30 Hardware.

(1) SDI Video Output supports 480i, 720p, and 1080i display modes at 59.94 or 60Hz.

(8) channels of embedded audio are supported for 720p and 1080i display modes.

(2) channels of embedded audio are supported for 480i display mode.

Limited Warranty

For the latest warranty information, visit

https://www.viavisolutions.com/literature/viavi-solutions-inc-general-terms-en.pdf

https://www.viavisolutions.com/en-us/literature/viavi-manufacturer-warranty-nse-products-en.pdf

VIAVI

Rev. 20.12, Jan 2021
English