

FLEXIBLE EMERGENCY MESSAGING PLATFORM

USER MANUAL

DASDEC™ II & One-Net™ SE

Version 4.0

Revision 0319



Digital Alert Systems, Inc. / Monroe Electronics (DBA)

100 Housel Ave • Lyndonville, NY 14098

www.digitalalertsystems.com

www.monroe-electronics.com

FCC Information

FCC ID: R8VDASDEC-1EN

The DASDEC-1EN and One-Net SE comply with Part 11 (47 CFR 11) of the FCC's rules for EAS encoders and decoders, including a Declaration of Conformity for Common Alerting Protocol (CAP) compliance, and are registered with the FCC under identification number: R8VDASDEC-1EN.

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/her own expense.

Disclaimer

DIGITAL ALERT SYSTEMS, INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Digital Alert Systems shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. The only warranties for Digital Alert Systems products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Digital Alert Systems shall not be liable for technical or editorial errors or omissions contained herein.

Copyright © 2004-2018 Digital Alert Systems, Inc. All rights reserved.

Alert Agent™, DASDEC™, EAS-Net™, MultiPlayer™, MultiStation™, One-Net™, OmniLingual™, PureCAP™, PureCAP™ Plus, TDX™, and Triggered CAP Polling™ are trademarks of Digital Alert Systems, Inc. All other trademarks mentioned in this document or website are the property of their respective owners. While every precaution has been taken in the preparation of this document, Digital Alert Systems assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Safari is a registered trademark of Apple Inc.

CODI is a registered trademark of Chyron Corporation.

Chrome is a registered trademark of Google Inc.

VDS-830, VDS-840, Starmu and Star-8 are trademarks of Keywest Technology, Inc.

Internet Explorer is a registered trademark of Microsoft Corporation

Firefox is a registered trademark of the Mozilla Foundation

SqueezeMax is a trademark of Utah Scientific, Inc.

Contact Information:

Digital Alert Systems, Inc. / Monroe Electronics (DBA)
100 Housel Ave • Lyndonville, NY 14098-9508

Sales & Technical Support:
Office: 585-765-1155

Table of Contents

INTRODUCTION to the DASDEC™ II and One-Net™	i
Icons	i
Highlights	ii
Organization	ii
Conventions	ii
Chapter 1: Hardware Overview	1-1
Introduction	1-1
Front Panel	1-1
Back Panel	1-3
Chapter 2: Hardware Connections	2-1
Installation	2-1
Network Connections	2-1
Radio Antennas	2-2
Audio Wiring	2-2
AES Digital Audio Wiring	2-4
Video Wiring	2-4
General Purpose Input/Output (GPIO)	2-5
Serial Port Wiring	2-6
MPEG Encoder Card Wiring	2-6
Power Connections	2-7
Chapter 3: Initial Setup	3-1
Making First Contact	3-1
Web Interface Login	3-3
Chapter 4: Web Interface and Navigation	4-1
Tabs, Buttons, Hyperlinks, Pull-Downs, Check Boxes and Text Fields	4-1
Web Interface Layout	4-3
Web Interface Navigation	4-7
How To Make Changes and Updates	4-7
Chapter 5: Setup Tab	5-1
Server Setup	5-1
Version 4.0 Specific Upgrade Instructions	5-17
Network Setup	5-29
Time Setup	5-38
Users Setup	5-40
EMail Setup	5-47
Audio Setup	5-52

Video/CG Setup	5-64
Alert Agent™ Setup	5-80
Station Setup	5-101
Demo/Practice Setup	5-113
Net Alerts Setup	5-115
Quick Connect to IPAWS CAP Server	5-129
Quick Connect to NAAD CAP Server (CAP Canada)	5-130
GPIO Setup	5-146
Printer Setup	5-152
Alert Storage Setup	5-154
Chapter 6: Alert Events Tab	6-1
Incoming Alerts	6-4
Incoming/Decoded Alerts	6-4
Forwarded Alerts	6-12
Originated/Forwarded Alerts	6-13
Originated Alerts	6-14
All Alerts	6-14
Backing Up EAS Event Logs	6-15
Chapter 7: Send Alerts Tab	7-1
General Alerts	7-2
One-Button Alert	7-13
Custom Message Pro	7-15
Assigning GPI Triggers to Custom Message Templates	7-25
Chapter 8: System Tab	8-1
Help	8-1
Status	8-2
Logs	8-3
Debug Logs	8-4
Appendix	A-1
Hardware and Software Specifications	A-1
The Emergency Alert System	A-3
Peripherals	A-4
EAS Protocol	A-6
Terms and Definitions	A-11
End User License Agreement	A-15
DASDEC and One-Net Chassis Chart	A-18

This Table of Contents is interactive. Simply click on the chapter or topic heading to navigate directly to the desired page.










INTRODUCTION to the DASDEC™ II and One-Net™

The DASDEC-II and One-Net™ SE Emergency Alert System (EAS) Analog and Digital CAP/Encoder/Decoder platforms are easy to use and relatively easy to learn. Generally, the web-based interface screens (web pages) are self-explanatory. Some users may be able to experiment with features with satisfactory results. However, both platforms offer a large number of features and automated functions, as well as a variety of shortcuts (hyperlinks). Referring to this manual frequently will increase understanding and decrease learning time for successful, customized operation.

This manual combines the features and functions of both the DASDEC-II and the One-Net. Generic language such as EAS device, EAS platform, and device/platform indicate information relevant to both. References to features specific to each platform are called out throughout the manual. See the Icon Guide below.

ICONS

Icons are used in this manual to highlight information.

Type	Icon	Description
Note		Denotes additional topic-specific information.
Attention		Brings attention to a specific topic.
Caution		Discusses possible issues involved with a feature or configuration setting.
Warning		Warns of possible issues when utilizing a feature or configuration setting.
External Link		Provides a link to additional information on an external website, such as the FCC.
Internal Link		Provides a link to additional information on the Digital Alert Systems or Monroe Electronics websites.
New Feature		Highlights new features within this version of software.
One-Net		Denotes Monroe Electronics One-Net SE specific information.
DASDEC-II		Denotes Digital Alert Systems DASDEC-II specific information.



Note

A number of DASDEC-II and One-Net SE features are licensed. Licensing these features enables users to customize the unit to the specific needs of its application. Note that this manual reviews every screen and explains all features and options, regardless of the user's licensing permissions.

HIGHLIGHTS

- The Table of Contents presents chapters in the most efficient way to configure the DASDEC-II and One-Net SE units in a step-by-step tutorial.
- An explanation of how the web interface screens are organized, and how to navigate within the web interface, is included in Chapter 4, Web Interface and Navigation.
- An electronic version of this manual is available on the Digital Alert Systems and Monroe Electronics websites, www.digitalalertsystems.com and www.monroe-electronics.com.
- New features continue to be added to the DASDEC-II and One-Net SE platforms. This manual is updated either in entirety, or by addendum, as new features become available.

ORGANIZATION

The manual describes the platform features, provides step-by-step instructions, and includes sample screen shots for quick reference. Early chapters provide hardware information and configuration details; later chapters detail software features of the software of your DASDEC-II or One-Net SE. Advanced features are included later in the manual, including integrating with other software applications and hardware.

Chapters 2 and 5 pertain to the setup of both hardware and software components. These tasks are presented in the order they should be completed. The order guides a first-time user through basic setup in the most efficient way to configure the EAS device step-by-step.

CONVENTIONS

The following conventions are used throughout this manual.

- The > symbol indicates movement within the web interface, such as clicking on a tab or selecting a radio button. For example, **Setup > Server > Upgrade** means you should select the **Setup** tab, then the **Server** button, and then the **Upgrade** sub-tab.
- Screen names/page titles are presented in **bold**.

Screenshots are provided to show the items visible on the monitor when selections are made or activity is ongoing. The image demonstrates a feature or particular setup. A screenshot is generally the result of following the instructions in the manual for a particular task. Each screenshot is labeled with the name of the screen or web page.

Buttons and links are presented as you would see them on the screen. In many cases, these images will only show a small portion of the complete screenshot, so as to focus on that specific topic.

Features on the interactive web page are typically presented from top to bottom within each section of the page. Many screens are divided into sections by one or more horizontal lines. The lines indicate the grouping of related functions. A feature on the interactive page is typically presented in bold type, followed by a discussion of its use and instructions.

This manual contains numerous [hyperlinks](#) for convenience. These links are distinguished by their blue text. The Table of Contents is interactive as well, allowing the user to click on a chapter or topic headings to be navigated directly to that topic.



Your Comments

Please let us know how we can serve you better. Send questions, comments, and suggestions to at support@digitalalertsystems.com.



Attention

This manual is organized in a sequential fashion to assist first-time users in the step-by-step configuration of the EAS device. For best results, first-time users should follow the instructions in the order in which they are presented.

Chapter 1: Hardware Overview

INTRODUCTION

The DASDEC-II and One-Net SE are 2U rack-mounted EAS devices utilizing standard computer technology in a dedicated chassis with broadcast quality connectors. The PC motherboard uses industry standard connectors for USB, PS/2, serial, VGA, HDMI, networking, and audio. In addition to the standard motherboard connections, the platforms feature broadcast quality video, audio, antenna, contact closure, and power connectors. All external connectors are located in the rear of the unit. An LCD, button, status/alert LEDs, and an internal speaker are located on the front of each unit.

FRONT PANEL



Front Panels of the DASDEC-II and One-Net SE Units

The front panel features a 2 line x 20 character backlit LCD that indicates power-on and real-time device status. Two LEDs (1 green, 1 red) are used for a variety of status indications. A small grill provides audio from an internal speaker. The push-button initiates a simple weekly test.

Front Panel Display

The backlit green LCD shows real-time status. The LCD has numerous purposes indicating system and/or encoding/decoding and active alert along with button action status.

- When the EAS device is powered on, the LCD lights up, indicating power-on state.
- As system software is boot loaded, the LCD displays the following sequence:
 1. DigitalAlertSystems / *DASDEC - 1EN*
 2. ** Startup 3 **
 3. 8x scrolling asterisks on the first line, and the time [HH:MM:SS] and date [DD Month, YY] on the second line
 4. The scrolling asterisks are then replaced by either: OneNet: Starting.. or DASDEC: Starting..
 5. Once the startup sequence is complete, the LCD will enter its normal display state, where the first line of the LCD will display either OneNet: ON or DASDEC: ON, followed by the Server Name and the IP address of the device. The second line continues to display the current clock time and date.



Note
Server Name refers to the individual device's given name. Default names are DASDEC-1F and OneNet-1F EAS, respectively. To change the Server Name, log in to the web browser interface and navigate to **Setup > Server > Main/ License**.

- If the system software is manually stopped or temporarily restarted due to an internal problem, the LCD displays a Server Stopped message until the software restarts to a ready state.
- During the decoding of an incoming alert, the LCD displays information about the source and the stage of the decoding.
- While decoded, forwarded, or originated alerts are active, the top line repeats, displaying pertinent identification for each active alert.
- When a backup configuration is loaded, or when the server software is restarted, the LCD indicates when the server is down or running again.
- During a software upgrade, the LCD display progresses through server down states, and eventually displays Upgrading. When the upgrade is complete, the LCD returns to the normal display state.

Status LEDs

The system's two Light Emitting Diodes (LEDs) are used to display a variety of system status conditions.

System Status	Green LED	Red LED
Initial power on	OFF	OFF
System begins to boot	SLOW FLASH	OFF
System nears a ready state	RAPID FLASH	OFF
System ready	ON	OFF
Decoding an incoming alert	ON	RAPID FLASH w/ PAUSES
Sending an alert	ON	ON
Awaiting manual Forwarding or Acknowledgement	ON	SLOW FLASH
Alert being held for GPI closure	ON	RAPID FLASH
EAS device is non-operational (during restart of upgrade)	FLASH	OFF

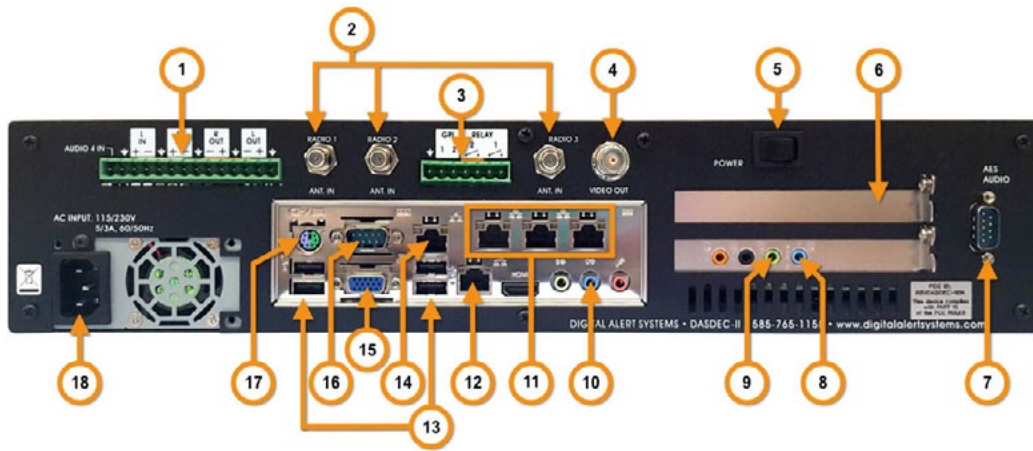
Select Button

The Select button on the front panel is typically used to initiate a Required Weekly Test (RWT), or to acknowledge unforwarded active alerts.

- Press the Select button once to being a manual RWT; the second line of the LCD displays **Press again for RWT**. Press the Select button a second time to begin the RWT alert. (See [Chapter 7 - One Button Alert](#) for more information.)
- When an alert has been decoded and is waiting to be forwarded, press the Select button to acknowledge that alert. The LCD temporarily shows **Acknowledging**.

BACK PANEL

The back panel provides all of the connections necessary for the EAS device.



Back Panel

1	Program Audio / Aux. Audio 4 Terminal Block	10	Main Audio - Line Input 1 & 2
2	Radio Antenna Connectors (Radio 1, 2, & 3)	11	Triple Port Gigabit Ethernet Expansion (optional)
3	General Purpose Input/Output Terminal Block	12	Main Network Interface
4	BNC Video Out (optional)	13	USB Ports
5	Power Switch	14	Second Network Interface
6	Expansion Slot	15	VGA
7	AES Program Audio (optional)	16	Serial Port (COM1)
8	Aux. Audio - Line Input 3 & 4	17	PS/2 Port
9	EAS Audio Out	18	Power Receptacle



Note

The image to the left is a DASDEC-II device (model DASTVR) with the Triple Port Gigabit Ethernet Expansion option installed. Not all DASDEC-II or One-Net devices will contain the same rear connectors. See the [DASDEC and One-Net Chassis Chart](#) for a list different models and back panel configurations.



Note

The device provides software support for the Video Out, Ethernet Expansion, and AES Program Audio as licensed options. Any connections not labeled, such as HDMI, are not supported and are not operational.



Note

The Expansion Slot (6) is typically used for the optional MPEG-2, additional EAS Decoder Audio Inputs (EXP-EAS), or Expanded GPIO Inputs and Outputs (EXP-GPIO) hardware.

Chapter 2: Hardware Connections

INSTALLATION

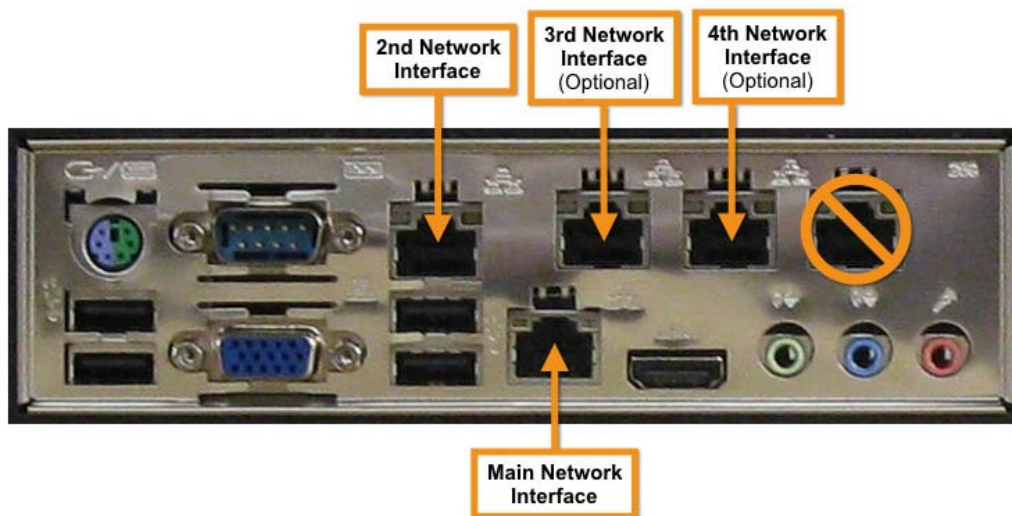
The DASDEC and One-Net frames mount in an EIA-compliant equipment rack by means of four rack screws fastened through the front mounting ears.

For safe, long-term reliability:

- Ensure the ambient air temperature surrounding the EAS device is within the product's specified operating temperature range.
- Maintain adequate ventilation within the rack.
- Ensure that adequate space exists on all sides of the frame for sufficient airflow. It is recommended a 1RU space be maintained between equipment, to avoid the transfer of heat between devices.
- Ensure the location of the EAS device is accessible, dry, and free of dust.

Rack Units	Height	Depth	Width	Weight
2RU	3.50" (8.89 cm)	12.0" (30.48 cm)	19.0" (48.26 cm)	15 lbs (6.8 kg)

NETWORK CONNECTIONS



Network Connections Example (devices may vary)

The current EAS device comes with two network interface ports (Main and 2nd Network Interfaces). These are industry standard RJ45 ports, and support standard networking protocols. The Main Network Interface port is where your initial network connection should be established. By default, this is the only active network interface. The additional network interfaces must be activated via the web interface.

More detailed information about networking can be found in Chapter 5 - Network Setup in this manual.



Caution

The rack and screws should be sufficient to carry the load of the unit, including the weight of accompanying cables. However, it is recommended a horizontal lacer bar be installed behind the back panel to alleviate cable stress, ensure cables stay connected, and provide effective cable management.



Warning

Always install the EAS device behind a firewall or other security measures and restrict network access to trusted hosts and networks only. Never allow direct access to the Internet.



Note

In facilities that require supplementary network connectivity, additional networking hardware may be installed. This optional network expansion will enable the 3rd & 4th Network Interface ports. The 5th network port is non-functional, and is not supported by this device. Navigate to **Setup > Network > Configuration** to configure the network ports via the web interface.

RADIO ANTENNAS

If the EAS device is equipped with internal radio receivers, there will be industry standard F-type connectors for each receiver (up to three total). Review your states' Emergency Alert System Plan for the appropriate monitoring assignments; these assignments will assist in determining the proper antenna for the frequencies that need to be monitored.

The EAS device's internal radios are designed to receive the following frequencies:

Band	Frequencies	Min. Input Level	Max. Input Level
FM	87.9 - 107.9 MHz	30-40 uV(-80 to -77 dBm)	1mV (-48 dBm)
NOAA	162.440 - 162.550 MHz	3-4 uV (-98 to -97 dBm)	<500 uv (-55 dBm)
AM	530 - 1700 KHz	2-3 uV (-102 to -98 dBm)	<500 uv (-55 dBm)

For proper reception, use a good quality, shielded RG6 coaxial cable and connectors. The quality of the incoming audio signal will affect the operation of the audio decoders, and the quality of the forwarded audio messages.

AUDIO WIRING

The DASDEC and One-Net platforms have two types of analog audio: EAS Monitored Audio and Program Audio. EAS Monitored Audio Inputs feed the internal EAS decoders for processing. Only signals with EAS information should be directed to these inputs. EAS Monitored Audio Outputs only send EAS decoded audio. Program Audio connections are used for internal switching of program audio.

Analog EAS Monitored Audio inputs are intended for line-level audio input from external radio receivers and/or other EAS devices. These audio signals are fed to internal decoders for EAS processing. There are numerous ways to configure the number of incoming audio sources for decoding. To establish the best way to wire/connect the audio sources, it is important to first understand the origin of the incoming audio signals.

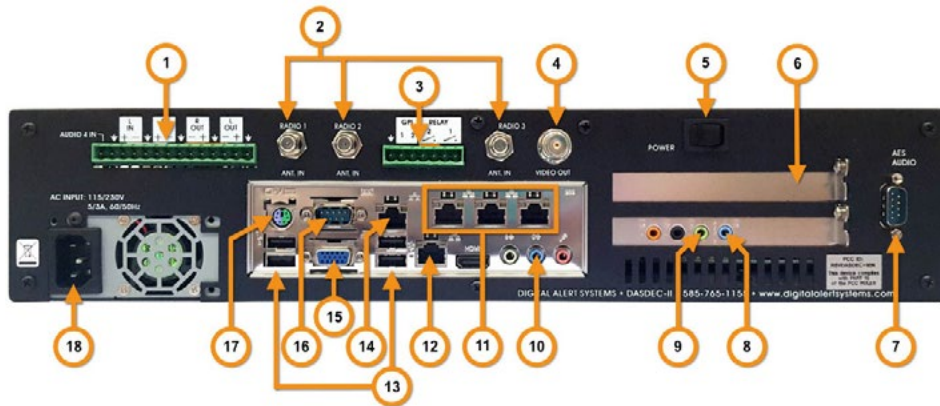
See the back panel graphic on the next page for references to specific components.

- Each audio line connector (3.5mm TRS) supports two EAS decoders. The left side of the input is decoded separately from the right side.
- The Main Audio – Line 1 & 2 inputs **(10)** are disabled if internal radio receivers are being used for Main Audio L1 & L2.
- When Radio 3 is in use, the Auxiliary Audio 4 (terminal block) input **(1)** is utilized for a line-level input (Auxiliary Audio 1 R2).
- For configurations where only two internal radios are being used (Main Audio L1 and R1), utilize the Auxiliary Audio – Line Input 3 & 4 **(8)** for line-level audio.
- The Auxiliary Out **(9)** can be used to monitor radio receivers, selectively play out stored EAS alert messages, and play out active EAS alert messages. This output is intended for audio monitoring, feeding audio to other EAS devices, and feeding audio to the optional MPEG card.



Note

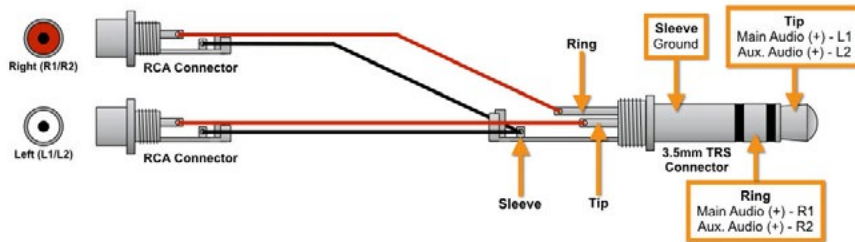
The FCC provides a listing of each state's EAS Plan, along with contact information for individual state emergency communications personnel, at <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/alerting/general/state-eas-plans>.



Back Panel

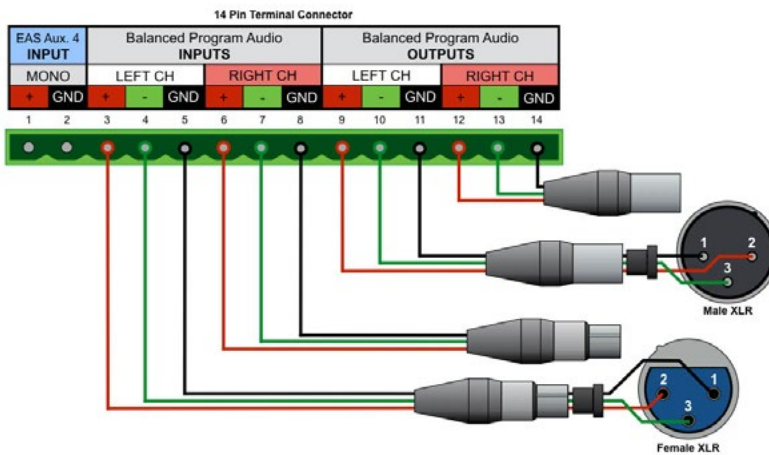
Analog Audio Wiring

The first type of inputs connects to internal EAS decoders (8, 10). These inputs are utilized to process broadcast EAS messages, and are attached to external radio receivers or other EAS equipment. 3.5mm TRS audio jack (mini) connectors are used for these inputs. Each EAS decoder accepts a mono audio signal. This single stereo input jack feeds two separate EAS decoders.



EAS Audio Connectors

The second type of analog audio inputs (1) are connected to the main program audio when internal switching of the audio signal is to be performed within this EAS device. These balanced audio inputs are only utilized for program audio switching, and do not tie to the EAS decoders. A screw type, pluggable terminal connector is used.



Program Audio Connectors



Note
A dual RCA to 3.5 mm jack input adapter can be used to connect two separate mono input signals to an EAS unit line input jack.



Note
This feature is typically used in call-letter broadcast facilities where the main programs' audio signal is bypassed during EAS alerts. Internal switching of a single audio signal is not an effective means of interrupting audio in facilities where multiple programs need to be switched during alerts.

Analog Audio Outputs

There are two types of Analog Audio Outputs: Program and Auxiliary. The Auxiliary Audio output provides EAS decoded audio only. The Program Audio output provides decoded EAS audio. When Program Audio inputs are connected to an incoming audio source, these outputs deliver a switched program signal.


The Auxiliary Audio output jack **(9)** is used to monitor EAS messages, provide an input to other EAS devices, and feed EAS audio to the optional MPEG card. The jack is a 3.5mm TRS (mini) connector that is the same as the Analog Audio Inputs.

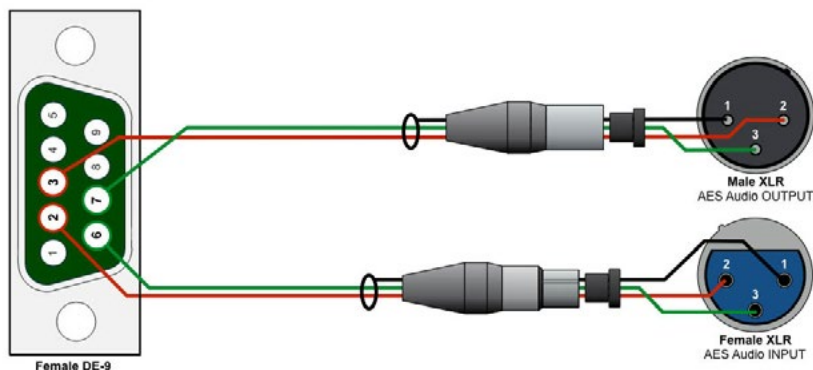
Program Audio outputs **(1)** are adjacent to the Program Audio inputs, found on the same pluggable terminal connector. These balanced audio outputs deliver a continuous audio program stream that switches between the Program Audio inputs and EAS audio during an alert.

When the output audio connections are complete, navigate to **Setup > Audio > Audio Output Levels/Tests** to ensure proper connectivity, and set proper audio levels.

AES DIGITAL AUDIO WIRING

An optional AES audio input/output function is available for the DASDEC platform. This includes the capability for an AES digital audio output, along with a switching AES audio output when an AES audio input is connected. A DE-9 to Male XLR and Female XLR breakout cable is provided. Refer to the diagrams below for cabling of the AES audio inputs and outputs.

 This feature is specific to the DASDEC-II.



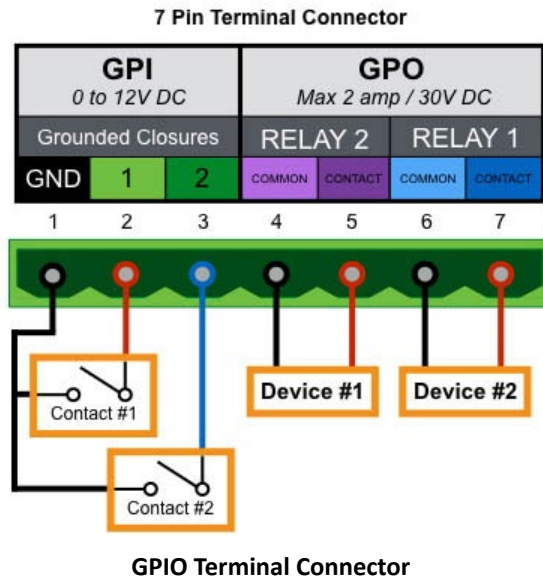
AES Digital Audio Wiring

VIDEO WIRING

Video Output is an optional feature included in some pre-configured devices. When enabled, an NTSC analog composite video signal is available from the BNC jack located on the back panel. This video signal provides visual, full-screen emergency alert details during alert forwarding and/or alert origination.

GENERAL PURPOSE INPUT/OUTPUT (GPIO)

The EAS platform comes standard with two General Purpose Input (GPI) contact closures and two General Purpose Output (GPO) relays. They are located in the upper middle of the back panel (3) via a 7-pin pluggable terminal connector.



GPO relay outputs are programmable. Triggering can be filtered against specific alert FIPS Groups and EAS Group codes. Events that can trigger a GPO relay include:

- Remain closed during EAS audio payout
- Momentarily closed at start of EAS audio payout
- Momentarily closed at start of an alert that has been decoded but not forwarded,
- Remain closed if an alert is held or delayed pending a GPI action.

The EAS device comes with two General Purpose Input (GPI) contact closures. They can be programmed to trigger a variety of actions, such as:

- Issue a Required Weekly test
- Trigger origination of an alert header/attention signal, pausing for voice dub of the audio message, followed by trigger of the EOM audio
- Review of audio portion of an active alert
- Active alert acknowledgment
- Re-enabling of active alert forwarding capability
- Forwarding of a monthly test with original audio

Additional Expansion GPIO Options

For installations that require additional GPIs and GPOs, there are several options available that will expand the standard capabilities. An internal GPIO card may be installed in the PCI expansion slot **(6)** to enable eight additional GPIs and eight additional GPOs. If the PCI expansion slot is not available, there are several network connected GPIO devices, such as the R190a Remote LAN Hub Controller / Net GPIO. The DASDEC and One-Net platforms can mix and match any combination of internal and network connected GPIO devices.



Note
See [Chapter 5 - GPIO Setup](#) for more information and available functions.



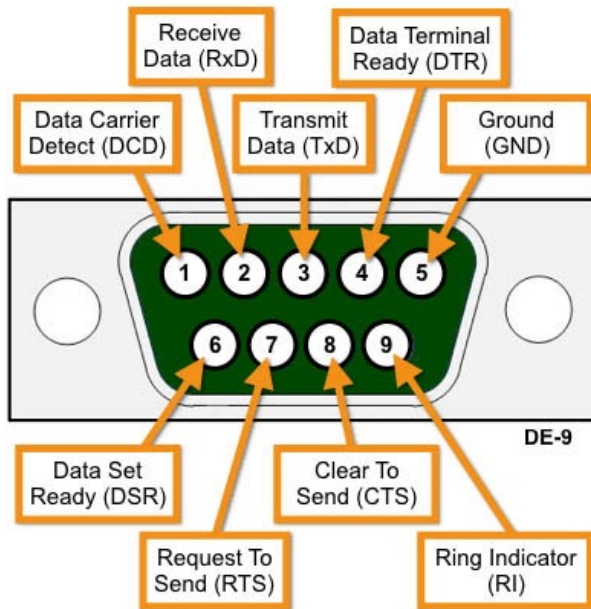
Note
See [Chapter 5 - Net Alerts Setup > Hub Controller/ Net GPIO](#) for more information.

SERIAL PORT WIRING

Each EAS device is equipped with one RS-232 serial port on the back panel. The serial ports connect to and drive a variety of external video character generators and BetaBrite LED signs. The software supports a wide variety of serial protocols, including the most commonly used protocols in legacy EAS equipment, such as TFT Standard and Sage Generic.

An optional USB/serial port expander can provide up to four additional RS-232 serial ports. This option is useful when additional character generators and LED signs are needed.

Each serial port has the same pin-out, as shown below.



Serial Port Connections (Chassis Side)

MPEG ENCODER CARD WIRING

For units equipped with an optional MPEG2 Encoder card, see the image below for wiring the MPEG2. The video output needs to be loop cabled back into the video input of the Encoder card. In addition, one audio output needs to be cabled to the MPEG audio input port.



Optional MPEG2 Encoder Card Audio/Video Connections



Note
For configuration of serial port protocols, see [Chapter 5 - Video/CG](#).



Note
Pins 2, 3, and 5 are the transmit/receive and ground pins, and are the minimum connections needed for a serial interface. Make sure to swap the transmit and receive pins (2 and 3) when making your own cables.

POWER CONNECTIONS

Once all connections are completed, power can then be applied to the device. A panel-mounted IEC compliant AC power receptacle, found in the lower left corner of the device's back panel **(19)**, delivers power to the internal AC power supply. Use only an approved IEC 320 C-13 type line cord rated for a minimum 10A at 250V. A power cord is supplied with your EAS device. Connect the cable's female IEC connector to the power receptacle on the frame, and connect the three-prong male connector to an AC outlet. Press the Power rocker switch **(5)** to initiate the start up sequence. Pressing this button a second time will initiate the shut down sequence.



Warning

The safe operation of this product requires that a protective earth connection be provided. This is provided by the grounding conductor in the equipment's supply cord. To reduce the risk of electrical shock to operators and service personnel, this ground conductor must be connected to an earthed ground.

Chapter 3: Initial Setup

MAKING FIRST CONTACT

The DASDEC and One-Net platforms contain an embedded web server that allows you to effectively communicate with the EAS platform via a standard web browser. Changes to configurations/control settings, initiating EAS alerts, and viewing EAS alerts are all performed through familiar web browsers such as Apple Safari®, Google Chrome®, Microsoft Explorer®, or Mozilla Firefox®. You will connect to the same network as the EAS device, launch a web browser, and input the devices' IP address.

To be on the same network as the EAS device, a customer-supplied laptop or desktop computer must be physically networked to the EAS device.

- This initial contact is necessary to make changes to the network settings within the EAS device so they correspond with your facilities' computer network addressing scheme.
- Once the EAS devices' network address is configured to match those of your facility, the EAS device will be accessible by authorized users within your computer network.
- During this first log in, the system requires you to change the default password.

Physical connections to the EAS device can be done in two ways:

1. A direct connection
2. By means of a network hub or switch

In both scenarios, the EAS device and customer-supplied computer are linked via their associated network interface ports by standard CAT-5/5e or CAT-6 cables with RJ45 (8P8C) connectors. Below are examples of what these physical connections look like, and a description on how to network these two devices.

Once the EAS device is correctly wired:

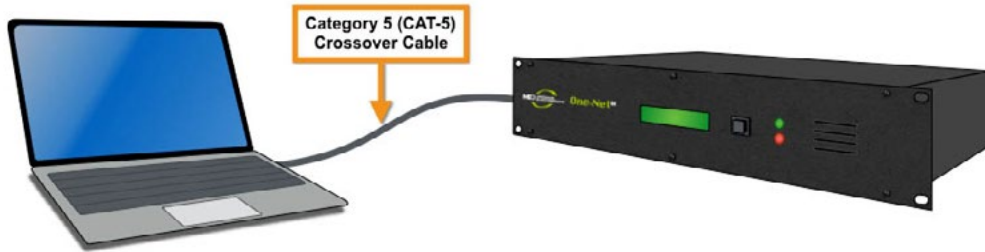
1. Turn on the EAS device by pressing and releasing the power switch **(5)** on the upper right side of the back panel.
2. The LCD screen will light during the power on.
3. Allow the device time to boot. (See the [Front Panel Display](#) section for complete startup sequence.)
4. On the front panel, a solid green System Status LED indicates when the system is completely booted and ready.
5. The first line of the LCD screen should display `OneNet: ON` or `DASDEC:ON`, followed by the devices' IP address.
6. The IP address of each new EAS device is set to 192.168.0.200.



Note

The EAS device is shipped with a CAT-5 crossover cable that is intended for the direct connection scenario.

Direct Connection



Direct Connection

1. Connect one end of the factory supplied CAT-5 network crossover cable to the Main Network Interface port (**12**) at the back of the EAS device, and the other end to the network interface port of a standalone PC or laptop computer. Once the EAS platform is powered up and completely booted, it can be accessed via a web browser launched from the directly connected, customer-supplied standalone computer.
2. Configure the standalone computer to use the static IP address 192.168.0.100 with a subnet mask of 255.255.0.0. The standalone computer and the EAS device should now be able to communicate.
3. Launch a web browser and type `http://192.168.0.200/` into the address bar. If a log-in screen similar to the one shown below appears, communication with the EAS device has been achieved. Skip to the [Web Interface Login section](#) of this chapter for instructions on logging into the device.

ME MONROE ELECTRONICS

OneNet-1F EAS
Serial: 5823
Platform ID: 8S9ES22BH5XKVTP/B81Z0

Username

Password

Sign me in

Copyright © 2018 Digital Alert Systems, Inc.
NOTICE: Access to this system is restricted to authorized users only. Unauthorized access or use of this system may constitute a violation of federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

Web Interface Login Screen

4. Once the EAS devices' IP address and subnet mask have been configured to correspond with your facilities' computer network addressing scheme, it will no longer be accessible from the standalone computer.
5. Reset the standalone computers' network configuration back to its original settings, remove the network crossover cable from both devices, and plug a house network cable into the EAS device.
6. The EAS device will now be accessible via a web browser running on any remote computer on the local area network.
7. Type the EAS devices' new IP address into the address bar of a web browser to access the login screen.



Note

Write down the current IP address and subnet mask settings of your local computer before making changes. This information will be useful when reconfiguring back to its original settings.



Attention

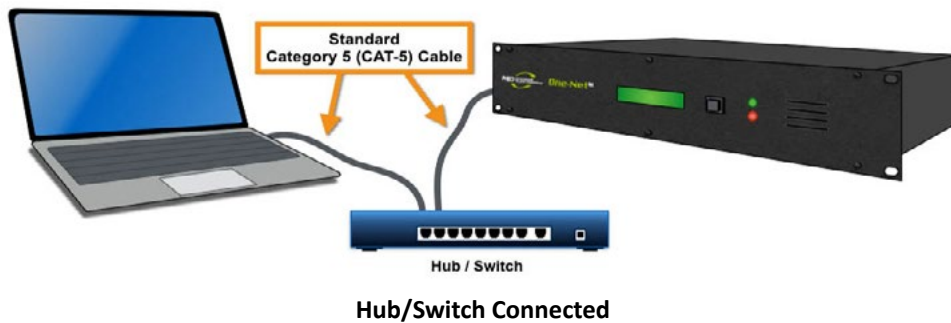
It is advised that you contact a network administrator before starting the following procedure, as a valid IP address and subnet mask settings are required to complete this initial setup. Working knowledge of how to change the network settings of the standalone computer is also necessary.



New Feature

The login page has been updated with a new look along with providing updated security.

Hub/Switch Connection



The primary difference between this type of connection and the direct connection method is the inclusion of additional networking hardware.

1. Connect a standard CAT-5 network cable to the Main Network Interface port **(12)** at the back of the EAS device and the other end into the open port of a routing hub or other network switching device.
2. Once the EAS device is powered up, booted, and operational, it should be accessible via a web browser running on any remote computer on the local area network routed to see the address 192.168.0.200.
3. Configure the remote computer to use the static IP address 192.168.0.100, with a subnet mask of 255.255.0.0. The remote computer and the EAS device should now be able to communicate.
4. Launch a web browser and type `http://192.168.0.200/` into the address bar. If a log-in screen similar to the shown below appears, communication with the EAS device has been achieved. Skip to the EAS Device Login section of this chapter for instructions on logging into the device.
5. Once the EAS devices' IP address and subnet mask have been configured to correspond with your facilities' computer network addressing scheme, it will no longer be accessible from the remote computer.
6. Reset the standalone computers' network configuration back to its original settings.
7. The EAS device will now be accessible via a web browser running on any remote computer on the local area network.
8. Type the EAS devices' new IP address into the address bar of a web browser to access the login screen.

WEB INTERFACE LOGIN

The screenshot shows the login interface for the OneNet-1F EAS device. At the top left is the Monroe Electronics logo. To the right, the device name 'OneNet-1F EAS' is displayed, along with 'Serial: 5823' and 'Platform ID: 859E522B53XKV7P1B8120'. Below this, there are two input fields: 'Username' and 'Password'. A blue 'Sign me in' button is positioned below the password field. At the bottom, there is a small copyright notice: 'Copyright © 2018 Digital Alert Systems, Inc. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the prior written permission of Digital Alert Systems, Inc. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners.'

Web Interface Login Screen



Note

If you are attempting to perform the following procedure, existing network settings within these additional network hardware components may prevent the ability to communicate with the EAS device.



Attention

Consult with a network administrator to ensure the default network address of 192.168.0.200 and 192.168.0.100 will be visible on the network, and will not clash with an existing node. If this method of initially accessing the EAS device is not successful, refer to the [Direct Connection](#) procedure.



Warning

Always install the EAS device behind a firewall or other security measures and restrict network access to trusted hosts and networks only. Never allow direct access to the Internet.

Launch a web browser application from a computer located on the same local area network (LAN) as the DASDEC or One-Net device you intend to reach. Type the EAS devices' IP address in the address bar of the web browser (for example, <http://192.168.0.200>). When the EAS device successfully connects, it will present a screen similar to the one shown above.

If this is the first time logging in, use the following default credentials:

- **Default User Name:** *Admin*
- **Default Password:** *dasdec*

Click the **Login** button.

If the user name or password is incorrect, a *Login failed* message will display next to the **Login** button, indicating the problem.



Note
Multiple login sessions are allowed at the same time.

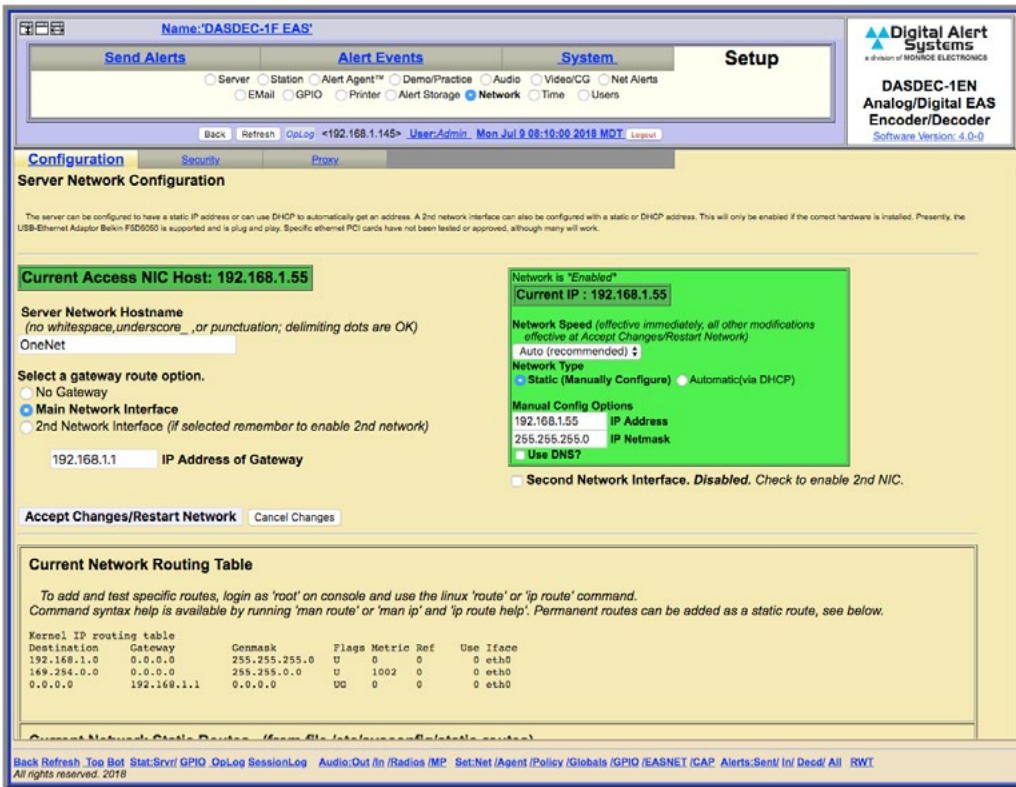
Edit Server User Account Profile Screen

If this is your first time logging in to the system, you will be taken to the **Edit Server User Account Profile** screen, where the default password must be changed.

1. Enter the current default password in the **Enter Current Password** field, and then enter the new password in the next two fields.
2. Pressing the **Submit Changes?** button enters the new login credentials for the Admin user.
3. The user is then directed to the **Setup > Server** screen (below). Near the top of this screen are 14 radio buttons, with the **Server** button highlighted in blue.
4. Click the **Network** radio button. The Server Network Configuration Screen will be displayed (see below). This is the screen where the network settings are modified.

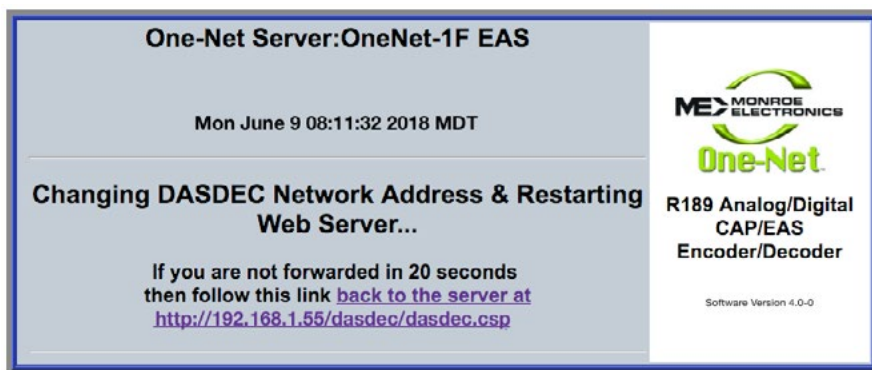


Note
Review the [New Password Policy](#) when creating a new password.



Server Network Configuration Screen

5. Enter the new IP Address and IP Netmask (or subnet mask) in the appropriate fields (located in the large green section on the right side of the screen). If the **IP Address of Gateway** and **DNS** information is available, enter that information as well.
6. Once this information is updated, click the **Accept Changes/Restart Network** button in the lower left.
7. Reset the network adapters to apply the new setting. The following screen will appear:



Network Reset Screen



Note
Before clicking the Login button, bookmark the Login Screen in your web browser. This will make accessing the EAS device easier.

Chapter 4: Web Interface and Navigation

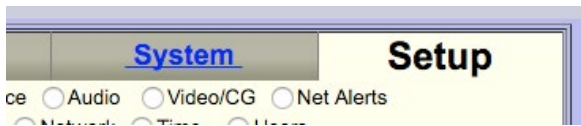
You will communicate with your EAS device by logging into the web interface via a web browser.

Type the IP address of the device and enter the proper credentials (username and password). Click the **Login** button. See the previous chapter ([Web Interface Login](#)) for more detailed login information. Once successfully logged in, the user will see the main web interface for the EAS device.

TABS, BUTTONS, HYPERLINKS, PULL-DOWNS, CHECK BOXES AND TEXT FIELDS

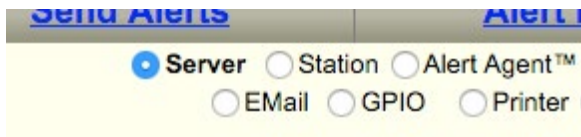
Graphical elements throughout the web interface enable users to navigate the interface and perform operations within the EAS device.

Navigation Tabs



Used to navigate the web interface. Choose the desired section by clicking on the appropriate tab. When active, the tab's background color will be lighter than the other tabs. The interface has both Tabs and Sub Tabs in the Header.

Radio Buttons



Used to navigate the web interface and report the currently selected item. These buttons are used when there are multiple options; only one radio button can be selected at a time. Clicking in the center of the button activates it. Radio buttons are most commonly used for navigation in the Header, but can be found on a handful of interface pages.

Action Buttons



Used to perform specific actions, based on their specified function. Frequently used to submit or cancel configuration changes, along with performing login/logout, initiating tests, and many other functions.

Pull-Down Menus

Add New Server User Account

Enter unused login name

View Only Level Set permission level

View Only Level Enter account comment

EOC Operation Level

Basic Operation Level Account

Operation Level password (space, #, & not allowed)

Operation/Control Level the password

Administration Level

Min 8 characters, with both letters and numbers

Create User

Allow users to select from a list of predefined configuration parameters. Many pull-downs have static selections, but several have selections that change according to modifications made in the EAS unit. Click on the pull-down menu to see a list of selections; move the mouse to the desired item and click on it to select it.

Check Boxes

Global Origination Settings

Weekly Test Settings

Set One-Button Weekly Test Duration

Hours 0 Mins 15

Include qualified forwarded alerts for blocking creation of Random Weekly Tests, instead of just qualified originated alerts. Disabled. Random Weekly Tests (RWT) will be scheduled without regard to Weekly, Monthly, or Emergency alert forwarding. Check to enable.

Automatically Manage random Weekly Test removal upon airing of qualified alerts. Disabled. Random Weekly Tests (RWT) remain scheduled regardless of other alerts that air. Check to enable.

Weekly Test Audio. Disabled. originated Weekly Tests (RWT) do NOT allow encoding an audio message. Check to Enable Weekly Test Audio.

Front Panel Button Weekly Test. Enabled. Uncheck to Disable.

Other Options

Segmented Alert Origination. For sending header separately from audio and EOM. Disabled. check to enable.

Used to select an individual item within the web interface. Unlike radio buttons, check boxes are not tied to any other check box. Check boxes may also display additional information within the web interface, and will not change any configuration settings. Click the center of the check box to activate that function.

Text Fields

Server Network Hostname
(no whitespace, underscore, or punctuation; delimiting dots are OK)

OneNet

Select a gateway route option.

No Gateway

Main Network Interface

2nd Network Interface (if selected remember to enable 2nd network)

192.168.1.1 IP Address of Gateway

White, rectangular boxes used for entering alphanumeric text. Text fields can be used to provide custom names/labels in several areas of the EAS device, input user credentials and configuration settings. Text fields typically allow the entry of any alphanumeric text. In some instances, the text may be limited to just numbers or just letters, or may prohibit specific characters.

Hyperlinks

Event Codes: EAN NF	
FIPS Locations	O
Utah [000000 049000]	A
Play Scheduling	C

Text elements that are highlighted in blue and underlined link to another location within the web interface, or to the World Wide Web. Hyperlinks assist in navigating the many menus found in the web interface. Click on a hyperlink to navigate to the indicated location.

WEB INTERFACE LAYOUT

The screenshot shows the 'Server Name & License Key Configuration' page. The **Header** section includes navigation tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup', along with the One-Net logo and product information. The **Body** section contains the main configuration area, including a table of license keys and their status. The **Footer** section contains a row of commonly used links.

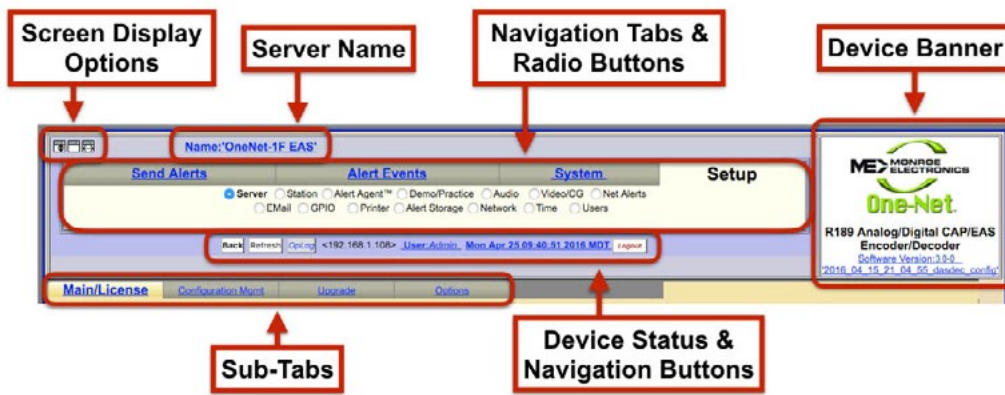
License Key	Status
ADT0d0JguelRuez2JkWRzefW0	CAP Standard - VALID
HCAP Standard Decode granted by Valid CAP Plus key**	
0BhdY0Tgmk4f0EK_willfyq4fy	CAP Plus - VALID
Required package dsddec_server is installed	
Required package dsddec_server is installed	CAP Canada NAAD Decode - NOT VALID
Required package dsddec_server is installed	CAP Caribbean Decode - NOT VALID
EMNet Software is not installed	Comcast EMNet CAP Client - NOT VALID
Skyscraper Software is not installed	Trivest Skyscraper Datacast CAP Receiver - NOT VALID
Required package dsddec_server is installed	CAP IRANS Server Emulation - NOT VALID

Web Interface Sections

This interface is made up of the following three sections:

- The **Header** contains useful information and navigation controls.
- The **Body** is the main portion of the web interface, which allows for configuring settings, sending alerts, viewing alerts, and monitoring system parameters.
- The **Footer** is a row of commonly used links at the bottom of the screen.

Header



Web Interface - Header Section

Located at the top of every screen, the header contains the following information and controls:

- **Screen Display Options:** The three square buttons at the top left of the screen control screen layout by performing the following actions:
 - **Stationary Menu Header:** Locks the header section so it remains at the top of the screen. The remaining portion of the screen may be scrolled up/down. An internal page scroll bar is displayed to the right of the body section of the web interface.
 - **Collapse Menu Header:** Removes the standard top navigation section (tabs and radio buttons) from the header.
 - **Page Width:** Toggles the width of the web interface from 800 pixels to 1000 to 1200 pixels to accommodate monitors and resolutions of differing sizes.
- **Server Name:** The Server Name, located at the top of the header, displays the name of the particular EAS device. This information is useful for facilities with multiple EAS devices, or large organizations with a common network between facilities. To change the server name, follow the hyperlink, or navigate to **Setup > Server > Main/License**.
- **Device Banner:** The Device Banner, located in the upper right-hand corner of the web interface, displays the EAS model, software version, and last loaded configuration file.
 - The DASDEC model have the Digital Alert System logo, followed by DASDEC-1EN Analog/Digital CAP/EAS Encoder/Decoder.
 - One-Net models have a Monroe Electronics logo, followed by One-Net R189 Analog/Digital CAP/EAS Encoder/Decoder.

The installed software version is listed just below as a hyperlink (blue, underlined text); clicking the link will take you to the **System > Help > About** menu, where you can find additional information about the installed software. If the EAS device has recalled a stored configuration file, that configuration file name will be shown just below the software version. This hyperlink will take you to the **Setup > Server > Configuration Management** menu.

- **Navigation Tabs & Radio Buttons:** The web interface contains dozens of unique screens; they are organized with a system of tabs and radio buttons. The main tabs located across the top of the header are: **Setup**, **System**, Alert Events, and **Send Alerts**. Within each tab are subsections organized by radio buttons, located directly below the tabs.
- **Device Status and Navigation Buttons:** Located just under the tab and radio buttons are navigation buttons and device status information in a single line.



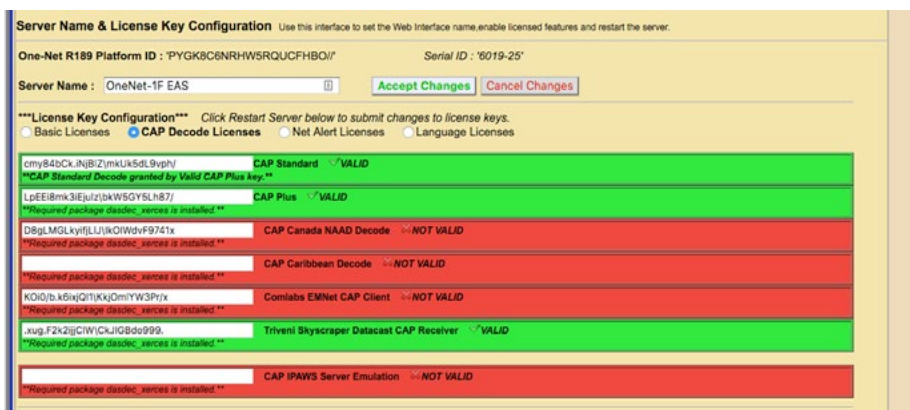
- **Back Button:** The preferred means of navigating back to the previously viewed web interface screen.
- **Refresh Button:** The preferred method to refresh the web interface.
- **OpLog Button:** A quick way to navigate to the **System > Logs > Operation Log** screen.
- **IP Address of the Current User:** To the right of the OpLog button is the IP address of the current user in the EAS device, denoted in standard IPv4 formatting: <xxx.xxx.xxx.xxx>.
- **User ID:** The current user is noted in the hyperlink text to the right of the IP address. In instances where multiple users are logged in to the same device, the User Name will be followed by parentheses. Inside the parentheses will be a single number or multiple numbers.
 - If there is just one number, only one user with that username is currently logged into the device. Example: A (2) means two users are currently logged in.
 - If you see (1:2), the first number (1) is the number of users with the same credentials as the current user, and the second number (2) means two total users are logged in to the device. Clicking the hyperlink navigates the web interface to the **Setup > Users** screen.
- **Date and Time:** Displayed to the left of the logout button, this static display shows when the interface screen was loaded. Clicking the Refresh Button updates the information. Clicking the hyperlink brings you to the **Setup > Time** screen.
- **Logout Button:** Located at the far right, this button logs the user out of the EAS device, and sends the user back to the login screen.



Attention

Using the back/refresh buttons on your web browser can provide misleading/out-of-date server information, and in some cases can result in unintended actions being performed. A good habit is to use the Back and Refresh navigation buttons in the web interface.

Body



Web Interface - Body Section

The body of the web interface is where all configuration, status, and alerting information is displayed and modified. The navigation controls (tabs, radio buttons, and hyperlinks) change the body section. This manual discusses each section in detail.

Footer



Back Refresh Top Bot Status:Server/ GPIO_OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:In/ Decd/ All RWT
All rights reserved. 2016

Web Interface - Footer Section

At the bottom of each web interface page is a row of hyperlinks, broken into the following sections:

Navigation:

- **Back** takes the user to the previous web interface screen
- **Refresh** reloads the current screen
- **Top** takes the user to the top of the current screen
- **Bot** takes the user to the bottom of the current screen

Status:

- **Server** navigates to the **System > Status > Main** screen
- **GPIO** navigates to the **System > Status > GPIO** screen
- **OpLog** navigates to the **System > Logs > Operation Log** screen
- **Session Log** navigates to the **System > Logs > Web Session Log** screen

Audio:

- **Out** navigates to the **Setup > Audio > Audio Output Levels/Tests** screen
- **In** navigates to the **Setup > Audio > Decoder Audio** screen
- **Radios** navigates to the **Setup > Audio > Radio Tuners** screen

Set:

- **Net** navigates to the **Setup > Network > Configuration** screen
- **Agent** navigates to the **Setup > Alert Agent™ > Manage Alert Nodes** screen
- **Policy** navigates to the **Setup > Alert Agent™ > Alert Policies** screen
- **Globals** navigates to the **Setup > Station > Global Options** screen
- **GPIO** navigates to the **Setup > GPIO** screen
- **EASNET** navigates to the **Setup > Net Alerts > EAS NET** screen
- **CAP** navigates to the **Setup > Net Alerts > CAP Decode** screen

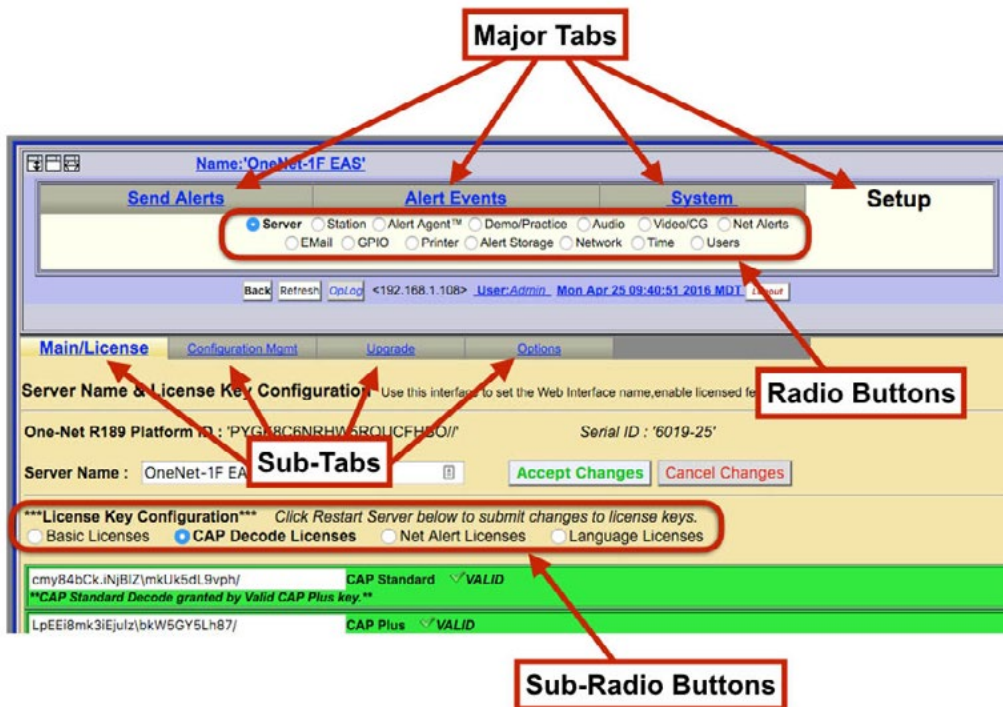
Alerts:

- **In** navigates to the **Alert Events > Incoming Alerts** screen
- **Decd** navigates to the **Alert Events > Incoming/Decoded Alerts** screen
- **All** navigates to the **Alert Events > All Alerts** screen
- **RWT** navigates to the **Send Events > One-Button Alert** screen

WEB INTERFACE NAVIGATION

The web interface is used to set up, control, view status, and monitor all activity. Radio buttons, check boxes, text fields, pull-down menus, and hyperlinks are found throughout.

The web interface uses a hierarchical organizational structure to navigate dozens of screens. The first level is a set of tabs, followed by radio buttons. Under the **Setup** and **System** tabs, you will also find sub-tabs and sub-radio buttons.



Web Interface Navigation

Throughout this manual, you will find references to menu structures, such as **Major Tab > Radio Button > Sub Tab > Sub Radio Button** (for example, **Setup > Server > Main/License > CAP Decode Licenses**).

To navigate:

1. Select one of the major tab menus at the top of the header.
2. Select a radio button.
3. If a level of sub-tabbed pages is shown, choose the desired page.


HOW TO MAKE CHANGES AND UPDATES

Changes can be made on each web interface screen, typically with check boxes, radio buttons, text fields, and action buttons.

Check boxes are labeled with the name of the feature that is enabled or disabled by that particular box. When the feature is enabled, a brief feature description usually follows. Click to disable the feature if it is not wanted. When the feature is disabled, click to enable it.

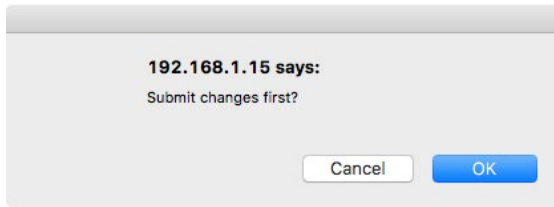


Note
When moving between top-level tabbed menus, such as **Setup** to **System** and **Back** to **Setup**, the last selected **Radio Button > Sub Tab** is remembered for each top-level tab.

<input type="checkbox"/> Left Channel EAS Decoder. DISABLED. Check to enable.
<input checked="" type="checkbox"/> Right Channel EAS Decoder. ENABLED. Uncheck to disable.
None  Autoscale Options.

Pages with an Accept Changes Button

Clicking **Accept Changes** updates the screen information. If the user exits the screen without clicking this button, the web interface prompts the user to “Submit changes first?”, and the user will decide to accept or decline those changes. If the **Accept Changes** button is not clicked, changes may be lost.



On pages with an **Accept Changes** button, there is also a **Cancel Changes** button. Use this button when you have made changes to the screen, have not clicked the **Accept Changes** button, and want to return to the original settings.

Pages without an Accept Changes Button

Pages without an **Accept Changes** button make changes immediately through automatic page submission. Changes made to check boxes, selection boxes, and by clicking buttons are immediate; the screen updates instantly. Screens with options that must change rapidly to be useful are the ones featuring immediate updates. For example, changes on the **Setup > Audio** and **Setup > Server** screens are immediate.

Text Entry Restrictions

There are two types of text entry available within the EAS device. HTML text is used within the web-based user interface - such as the Server Name, Station ID, login credentials, etc. File Name text may also be entered when saving a file to a local hard drive. These types of character restrictions are common and are as follows:

Illegal HTML Characters: **& < > \ " ' `**

Illegal File Name Characters: **< > / \ \ & ` \$ * \ " ' () ^ % @ ! { } [] | ? , ; ; "**



Attention

On pages with an **Accept Changes** button, you must use that button to submit changes.

Chapter 5: Setup Tab

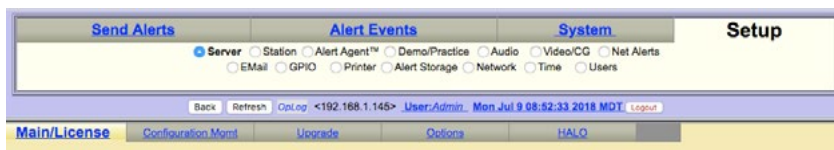


Setup Tab

The majority of all configuration settings are within the Setup tab. There are 14 sub-categories, accessed by clicking their individual radio buttons. These categories are as follows:

Radio Button	Description
Server	License Keys, Saving/Recalling Configuration Settings, Upgrades, and general system options
Station	Global and station origination/forwarding settings
Alert Agent™	Alert Policies & Nodes, Local Access & Custom Message Forwarding, FIPS & EAS Code Groups
Demo/Practice	One-Button Demo/Practice Decode Test
Audio	Encoder & Decoder Audio Adjustments, Audio Output Levels/ Tests, Optional Radio Tuner Settings
Video/CG	Internal CG settings and serial port configuration
Net Alerts	Assorted Network-based communications, including EAS NET, CAP Servers, Networked CGs, Networked Switches, and Networked GPIO devices.
Email	Email setup and various Email Configurations
GPIO	GPI and GPO interface programming
Printer	Printer Configuration
Alert Storage	Alert Storage Management
Network	Network Settings, Security Configuration, and Proxy Server setup
Time	Date/Time and Network Time Protocol (NTP) Configuration
Users	User Account Management

SERVER SETUP



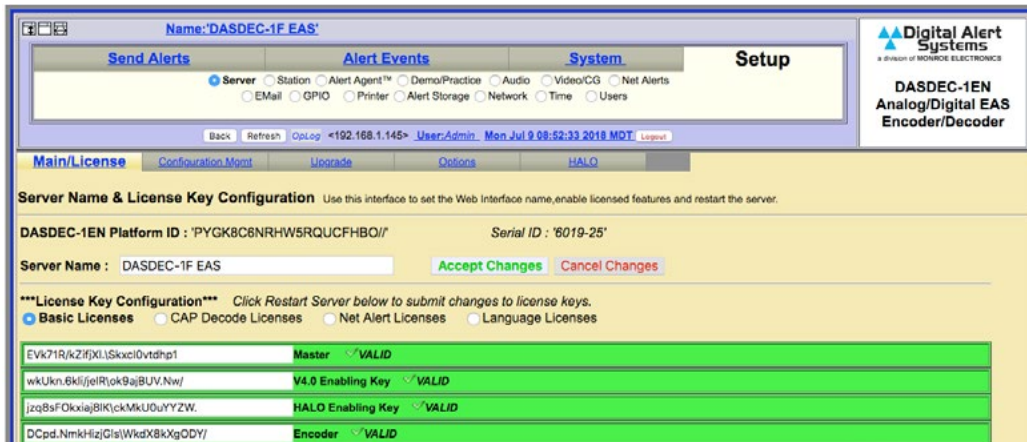
Server Setup Header

The server must be configured before the EAS device is operational. Navigate the web interface to **Setup > Server**. There are four, standard sub-tabbed pages on the **Setup > Server** screen:

- Main/License
- Configuration Mgmt
- Upgrade
- Options

A fifth sub-tab, HALO, is visible if a valid HALO Enabling Key is enabled. During the initial configuration, the principal sub-tab to review is the **Main/License**. The next two sub-tabs, **Configuration Mgmt** and **Upgrade**, support making and installing backups of the Server Configuration and Server Software Upgrade. The fourth sub-tab, **Options**, deals with platform configuration options. The **HALO** sub-tab enables the connection to the HALO server and a handful of HALO-related settings.

Main/License: Server Name & License Key Configuration



Main/License Sub-Tab Screen

There are two main sections on this screen: Platform ID and License Key Configuration. Use this screen to set the Server Name of the device and enable licensed features. There are several crucial action buttons at the bottom of the screen to restart, reboot, and power off the server.

The first task is to check the License Key configuration. The core device software will only run if it has been enabled using a Master license key. Version 4 software is also enabled with a valid license key. Most EAS devices are delivered pre-configured from the factory, so this task already may be complete. If the device is being upgraded to Version 4.0, this is the location for inputting that license key.

DASDEC II-1EN or One-Net R189 Platform ID

This is a unique identifier for the actual EAS device hardware, and cannot be edited. This identification string is needed to generate a license key to enable an unlicensed feature.

Serial ID

Each physical chassis is identified by a unique Serial ID (or Serial Number). This number is used when registering the device and for any service calls to track the device. It cannot be edited. On the top-right corner of the back panel is a small label that will mirror this identifier.

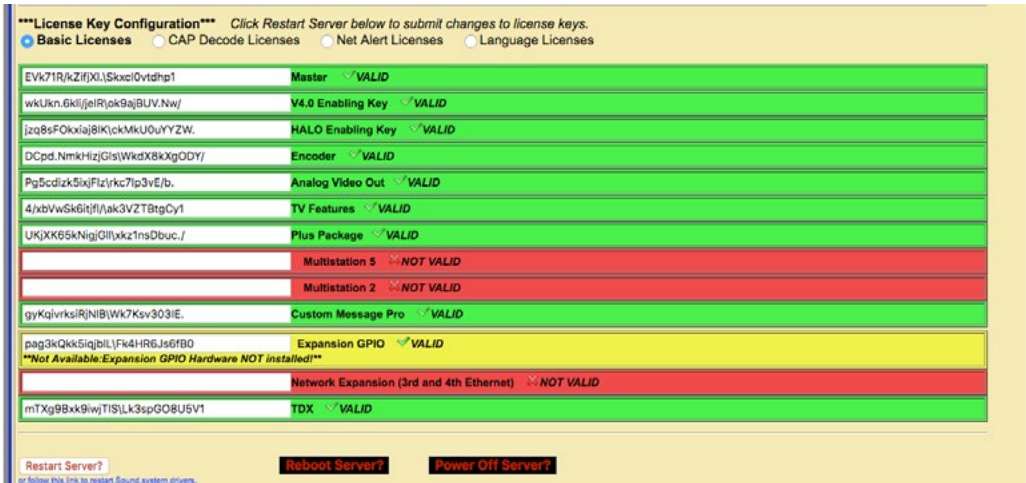
Server Name

The Server Name is the name the EAS device presents through the web interface, is included in EAS logs/reports, and is most useful when multiple EAS devices are located in the same facility or when centrally managed. When edited, it is best to choose a descriptive and unique name for each EAS device, such as *ROC-HE OneNet* or *WMMM DASDEC1*. The Server Name can have spaces and is limited to 70 characters. To change the Server Name, click in the Server Name field highlighting the existing text. Type



Note
Do not confuse the **Server Name** with the **Server Network Hostname** found in the **Setup > Network > Configuration** screen (see below). The Server Network Hostname is how the device is identified across the house network. The Server Name is how the device is labeled within the web interface.

the desired Server Name, up to 70 characters, including spaces. When done, click the **Accept Changes** button. To cancel any entry and revert to the current Server Name, click the **Cancel Changes** button.



License Key Configuration Section

License Key Configuration

Each EAS device has many available features enabled by using a license key interface. These license keys have been organized into four categories, corresponding with sub-radio buttons: Basic, CAP, Net Alert and Language. Description of each license key are in the following tables.

License keys have three different labels:

- **Green license box:** When a feature is correctly licensed with a valid key in the associated key's text field on the left, the license key display is green. The word VALID is shown to the right of the license key name.
- **Yellow license box:** For options that also require specific hardware, the key display is yellow when the license key entry is valid but the hardware is not installed. The word VALID to the right of the license key name indicates the key is OK. A message states what hardware is not yet installed.
- **Red license box:** When the text field is incorrect or blank, the feature's box will be red. The words NOT VALID are to the right of the license key name.

Each license key is unique and specific to a particular EAS device, and consists of character strings including letters, numbers, and punctuation marks. Licenses cannot be copied or shared between devices. To purchase a license key for a feature, contact Digital Alert Systems/Monroe Electronics.

New license keys are typically sent via email, and can be easily copied and pasted into the corresponding license key text field. Once a license key has been entered, the EAS device's software will need to be restarted to activate the key. The quickest way is simply clicking the **Restart Server?** button, located at the bottom of the screen. A confirmation screen will immediately appear with the options to **Yes, Restart Server** or **No, Cancel Server Restart**. Click **Yes, Restart Server** to continue the process; otherwise, click **No, Cancel Server Restart**.

Restarting the software logs all users off the device and shuts down all operations until the software is reloaded. Once reloaded (approximately 45 seconds), users will need to log in to the device. After the restart, it is a good idea to verify that the recently added license key is properly installed by navigating back to the corresponding license key screen and verifying that the license key has a green background and a VALID label.

Restart Server?

Initiates a restart of the EAS device's software. A confirmation screen will immediately appear with the options to **Yes, Restart Server** or **No, Cancel Server Restart**. The system will log out all users, restart, return to fully operational, and wait for users to log in.

Reboot Server?

Is a full system reboot. A confirmation screen will immediately appear with the options to **Yes, Reboot Server** or **No, Cancel Server Reboot**. The entire EAS device will power down and go through a complete hardware reboot process. The system will log out all users, restart, return to fully operational, and wait for any users to log in.

Power Off Server?

Powers down the EAS device. A confirmation screen will immediately appear with the options to **Yes, Power Off Server** or **No, Cancel Server Power Off**. The EAS device will power down completely, and not restart. To restart the EAS device, press and release the power switch on the back of the EAS device.

Or Follow this Link to restart Sound System drivers

At the bottom center of the page is a hyperlink to the **Setup > Audio > Decoder Audio** screen.

Basic Licenses

This grouping of license keys includes core functionality and general software and hardware options. The following list of license keys are included in the Basic License sub-radio buttons.

License Key	Description
Master	The Master license key is pre-configured for each new device. A valid Master license key enables users to operate, configure, and access the permissions allowed by their user credentials. Without a valid Master license key, users can only configure a subset of the basic features: all Setup > Network , > Time , and > User settings, along with all System > Status and Help menus. The Setup > Server menu is limited to the > Main/License sub-tab, where the Server Name , Master License Key , and V4.0 Enabling Key are the only available text fields.
V4.0 Enabling Key	A Version 4.0 Enabling key is necessary to operate the version 4 software, and is preconfigured for each new device. A valid V4.0 Enabling key enables users to operate, configure and access the permissions allowed by their user credentials. Without a valid V4.0 Enabling key, users can only configure a subset of the basic features: all Setup > Network , > Time , and > User settings, along with all System > Status and Help menus. The Setup > Server menu is limited to the > Main/License sub-tab, where the Server Name , Master License Key , and V4.0 Enabling Key are the only available text fields.
HALO Enabling Key	HALO is an enterprise-level EAS management system enabling users to monitor and manage multiple EAS devices within a single user interface. This is a new product from Digital Alert Systems and Monroe Electronics. The HALO Enabling key (or Client License Key / HALO-CLK) is necessary for each EAS device to communicate and exchange files with the central HALO server.



Note

To restart the EAS devices server software, click the **Restart Server?** button at bottom of this page. This is used during license key configuration. It can also be used at any time the EAS device appears to be functioning incorrectly. A confirmation page is displayed before the restart is actually run.



Attention

When restarting the server software, all logged-on users will be forced out of the system, and will be required to log back in. Alert decoding will be temporarily paused during the restart. This is not a system reboot, but nonetheless, use the **Restart Server?** button with care.



Caution

The EAS device's software must be restarted for the license key to take effect. Using the **Accept Changes** button or the **Refresh** button may turn the license key green, but the software will not acknowledge the enhanced features of that key until the software has been reinitialized.



New Feature

Support for HALO is new in version 4.0.



For additional information on HALO visit: <https://www.monroe-electronics.com/HALO/home.html>

License Key	Description
Encoder	<p>A license key for control of the encoder alert origination functionality. A valid Encoder key enables users to configure and use the encoder to run general alert origination. Decoder-only configurations do not need this feature enabled. Decoder only configurations can only issue Weekly tests. The following license keys require a valid Encoder license:</p> <ul style="list-style-type: none"> • Plus Package • Multistation 2/5 • Custom Messaging • TDX • CAP Canada NAAD Decode • CAP Caribbean Decode • All EAS NET options • DVS168 Single Client • DVS644 (SCTE18) • Streaming MPEG 1/2 & 1/2/4
Analog Video Out	<p>Will enable the video output port for displaying emergency message details as composite NTSC on systems with the necessary hardware. Standard on all One-Net models and DASDEC TV packages (DASLPTV, DASLPTVR, DASTV, DASTVR). Consult factory for more information.</p>
TV Features	<p>This option unlocks support for television specific features, including specific serial port protocols, to support a number of external video display devices. Standard on all DASDEC television models.</p>
Plus Package	<p>This option unlocks support for a set of advanced functions. Together with the TV Features license, certain specific broadcast TV options are enabled, including Manual Forward Text review/edit and network control of Chyron Digibox CODI character generators.</p> <ul style="list-style-type: none"> • Support for the USB4R232 4-port serial expander 4x serial ports • Front panel audible announcement of decoded alerts • Custom text modification for ORG codes and CGs • Custom message modification allows both text and audio message editing • Live sequencing of manually forwarded alerts • Adds serial support for Chyron Codi and Net CG support for Cayman Graphics™, Chyron™ Intelligent Interface (ChyTV, and Codi Net CG), Compix™ NewsScroll, and Compix AutoCast character generators • Supports Fox Splicer™ (Cisco DCM™)
Multistation 5 Multistation 2	<p>When the Plus Package license is enabled, two more options are available for licensing the MultiStation modes. MultiStation-2 supports independent control and management of two program streams from a single DASDEC, while MultiStation-5 supports independent control for up to five program streams from a single DASDEC. Each station will be branded with its own individual station IDs and logging. GPIOs can be set for each stream according to Station ID, FIPS, and/or Event Code. Provides sequential or simultaneous station playout and staggered playout with optional MultiPlayer™.</p>



TV Features is **DASDEC** only.



Multistation 5 and Multistation 2 are **DASDEC** only.



More information is available on the Digital Alert Systems website: www.digitalalertsystems.com/pdf/multistation_brochure.pdf

License Key	Description
Custom Messaging Pro	Custom Message Pro software option allows designated individuals secure access to a specific screen where they can create detailed, informative custom audio/video messages for processing by downstream EAS equipment using Administrative (ADR) or Civil Emergency Message (CEM) EAS codes. Entered text is automatically converted to audio using the included Text-to-Voice translation, or a .WAV file may be attached. May be combined with EAS-Net software to propagate custom messages across an entire EAS network. Includes premium voice TTS-David. <i>Not recommended for use with MultiStation feature due to restricted functionality.</i>
Expansion GPIO	Expanded GPIO Inputs and Outputs enable the optional EXP-GPIO board hardware for adding eight (8) additional GP Inputs and GP Outputs, for a total of 10 Inputs and 10 Outputs onboard. Uses internal expansion port; therefore, cannot be combined with MPE2-4 or EXP-EAS options.
Network Expansion	Enables the Triple Port Gigabit Ethernet Expansion hardware option (DASDEC-II/One-Net SE ONLY), creating controls for four unique Ethernet 10/100/1G network links. Please contact the factory regarding upgrading in-field units.
TDX	This option unlocks the EAS Textual Data Exchange (TDX) option, a Digital Alert Systems/Monroe Electronics exclusive protocol for a text transmission technique providing event specific detail in the EAS message without obsoleting existing EAS equipment. TDX adds digital information within EAS alerts for interfacing to a host of newer information technologies and other TDX-enabled devices. Messages that include TDX pass transparently through regular EAS devices, while TDX-enabled devices provide the additional data extraction.



More information on network expansion is available on the Digital Alert Systems and Monroe Electronics websites: www.digitalalertsystems.com/pdf/exp-3nic_datasheet.pdf or www.monroe-electronics.com/EAS_pages/pdf/3-nic_datasheet.pdf.

CAP Decode Licenses

Common Alerting Protocol (CAP) is a consistently disseminated messaging standard used by federal agencies (and others) to communicate emergency information via the internet. This grouping of license keys contains CAP-specific options. The following list of license keys are included in the CAP Decode Licenses sub-radio buttons.

License Key	Description
CAP Standard	CAP software option for directly handling CAP v1.2 messages to ensure compliance with FEMA/IPAWS profile 1.0 requirement for text and audio processing.
CAP Plus	CAP Plus software option for directly handling all currently specified CAP v1.2 messages (text, audio, images, etc.). Includes support for automatic Text-To-Speech translation of alert text, and basic, single-voice, Text-to-Speech license.
CAP Canada NAAD Decode	This features allows users to decode National Alert Aggregation & Dissemination System (NAAD System) alerts in Canada.
CAP Caribbean Decode	Common Alerting Protocol (CAP) - Caribbean Profile Processes CAP messages using profiles for national alerting systems of Anguilla, Montserrat, Sint -Maarten, Aruba (English only).

License Key	Description
Comlabs EMNet CAP Client	Comlab's EMnet client provides Assured Message Delivery of both EAS and IPAWS data directly through a fully integrated embedded application running on DASDEC/One-Net platforms. License keys are available only from Comlabs. Please contact them at +1 (321) 409-9898 or sales@comlabs.com.
Trivini Skyscraper Datacast CAP Receiver	SkyScraper client for fully integrated emergency content reception and management via ATSC or DVB broadcast. Uses exclusive receiver targeting, decryption, and forward error correction to provide data input. (External ATSC or DVB data receiver and antenna required; not included.)
CAP IPAWS Server Emulation	Enables any DASDEC-II or One-Net SE device to emulate an IPAWS server. Contact factory for more details.

Net Alert Licenses

A grouping of network-based communication protocols. These license keys include EAS-NET™, DVS-168, DVS-644, and MPEG streaming options. The following list of license keys are included in the Net Alert License sub-radio buttons.

License Key	Description
EAS NET™ (Includes DVS168)	EAS-Net is Digital Alert Systems exclusive communications protocol software enabling EAS data and audio transmission over a TCP/IP network for up to eight EAS-Net compatible platforms. Also incorporates multi-client DVS-168. <i>Works with Encoder models, or those with DASENCS only.</i>
EAS NET™ CAP Send	This software addition allows origination of CAP alert messages. EAS-Net CAP Send Software option converts EAS messages into CAP v1.2 IPAWS profile and transfers the message file(s) to remote servers using standard EAS-Net communication protocols. Allows EAS origination to activate alert messages on external standardized CAP servers.
EAS NET™ CAP Send to IPAWS Open	This software addition allows facilities to originate/ encode and forward a CAP alert message directly to the FEMA server. Typically used with DASEOC Emergency Messaging Platform.
EAS NET™ Send PureCAP™	EAS-Net CAP/Send PureCAP forwards the received CAP message without modification, so the exact CAP message received is relayed to other downstream devices – in its exact form and format – for further processing.
EAS NET™/CAP Send OmniLingual™ CAP	Adds the ability to send multi language CAP messages between EAS Net devices. Also Requires Valid Multi Language key.
EAS NET™ Mediaroom	Adds EAS-Net support for Microsoft/Ericsson Mediaroom. This license key is a bundle that includes EAS-Net.
EAS NET™ Minerva	This option unlocks EAS alert network forwarding via the Minerva EAS LAN protocol. This license key is a bundle that includes EAS-Net.

License Key	Description
EAS NET™ Automation	EAS NET support for a variety of playout servers, including Wide Orbit RCS Nexgen and Zeta, Harddata, Broadstream Solutions, and many others. This license key is a bundle that includes EAS-Net.
EAS_NET™ AEA	Advanced Emergency Alerts (AEA) are part of the ATSC 3.0 standard. This licensed feature supports the creation of an AEA Table (AEAT) list of AEA messages assembled from the current decoded alert list and embeds them within a proprietary .xml file container which is sent via various EAS-Net protocols to downstream receivers.
DVS168 Single Client	DVS168 Single Client Software interface supports legacy EAS protocol over TCP/FTP IP for EAS Text/WAV audio/control trigger to a single remote DVS168-compatible host. Currently supported products include various Evertz master control, Cisco (S-A) DNCS, and the QMC-2-MG Master Control platform. For more than one DVS-168 host, use EAS-NET. <i>Works with Encoder models, or those with DASENCS only.</i>
DVS644 (SCTE 18)	Digital Video Standard 644 (SCTE-18) communications protocol software enables sending EAS data as an MPEG-2 Transport Stream over a TCP/IP network to up to sixty-four (64) DVS-644(SCTE18) compatible platforms. Works with Encoder models or those with DASENCS only.
MPEG-DASH	Enables a feature set specific to the creation and distribution of MPEG-DASH content.
Stream MPEG 1/2	This license key option unlocks MPEG 1 and 2 streaming video/audio. A license key is provided when special MPEG 2 encoder hardware is purchased.
Stream MPEG 1/2/4	This license key option unlocks MPEG 1, 2, and 4 streaming video/audio. A license key is provided when special MPEG 4 encoder hardware is purchased.



New Feature

Advanced Emergency Alerts (AEA) is new in version 4.0.

Language Licenses

Support for multilingual alerting and premium text-to-speech (TTS) voices are located in this grouping of license keys. The DASDEC/One-Net includes a standard TTS voice, and the ability to add a large number of premium TTS voices for an additional cost. Each premium TTS voice includes the ability to add and edit the lexicons for colloquial pronunciations. The following are just some of license keys available for licensing, with a number of additional premium TTS voices available beyond. Please check with the factory for a list of all available.

License Key	Description
OmniLingual™ Enable Key	OmniLingual module enables automatic alert translation from conventional EAS or CAP sources into one or more languages — including, but not limited to, English, Spanish, French, German, Italian, Hmong, and Somali — for EAS text display and TTS audio conversion and output.
Allison	Premium Text-To-Speech Allison (US English-Female) license key.



Note

OmniLingual™ Enable Key: Requires appropriate Premium TTS module for proper Text-To-Speech conversion. See Premium Text-To-Speech Options below.

License Key	Description
William	Premium Text-To-Speech William (US English-Male) license key.
David	Premium Text-To-Speech David (US English-Male) license key.
Jean-Pierre	Premium Text-To-Speech Jean-Pierre (US French Canadian-Male) license key.

Editing Premium Text-To-Speech Voices

Premium Text-To-Speech Voice License Keys are found within the Language Licenses sub-radio button. When a Premium Voice is purchased and properly licensed, that license key's box will turn green, and an **Edit** action button will appear to the left of the Voice's name. Clicking the **Edit** button will enter the user into that specific voice's Lexicon Editor. From this screen, users can modify the speed (words-per-minute) and pitch factor, and create word definitions for altering phonetic pronunciations of specific words or lexicons of that voice. This screen also facilitates the saving and recalling of lexicon files.

The TTS engine uses a lexicon file for special instructions on how to "speak" a word or phrase in a particular way. For example the word "wind" can be pronounced both as "wīnd" with a long "i" sound, meaning to coil or wrap something, or "w-eh-nd," as in a High Wind Warning. Also, the text abbreviation "T-Storms" may be used as an abbreviation for the word "Thunderstorms." Adjusting the lexicon can greatly improve the way a TTS system understands and voices these types of words. There is a means of sampling text (individual words or phrases), thus allowing a user to very closely refine how the system will speak any text prior to hearing it on-air.

Main/License Configuration Mgmt Upgrade Options

Edit female voice 'Allison' US English; Version 6.2.3

Accept Changes Cancel Changes Apply Changes

The **Lexicon Table** allows override specifications for TTS word pronunciation. Each item consists of 2 fields: WORD | PRONUNCIATION where: WORD is the exact text of the word or abbreviation being defined; and PRONUNCIATION is a list of 'phonemes' which in sequence define the pronunciation of the word. For example, an entry: **t-storm** | **th ah0 n d er1 s t ao1 r m s** will instruct the TTS engine to pronounce the abbreviation t-storm (and T-Storm) as 'thunderstorm'. Literal words are not case sensitive. Individual word definitions can be disabled by toggling the Enable checkbox.

Add New Word Definition

Enable	WORD	PRONUNCIATION (Phoneme List)	
<input checked="" type="checkbox"/>	t-storms	th ah0 n d er1 s t ao1 r m s	Delete
<input type="checkbox"/>	wind	w eh1 n d	Delete
<input checked="" type="checkbox"/>	medina	m ah0 d ay1 n ah0	Delete

Sample Text - Enter text and use the **Make TTS Sample** button to test settings.

The National Weather Service has issued a high wind warning for the city of Medina. T-storms are predicted to continue throughout the day.

160 Words per minute (default is 170)
150 Pitch factor percent(50%-150%, default is 100%)

Make TTS Sample Thu May 5 10:05:29 2016: [Listen to this sample of Allison on the Browser](#)

Thu May 5 11:56:24 2016: [View/Download the current saved lexicon file for Allison.](#)

Upload a Lexicon file at the bottom of this page.

Accept Changes Cancel Changes Apply Changes

Show phoneme rules chart. Check to enable.

Upload a Lexicon text file to One-Net Server.

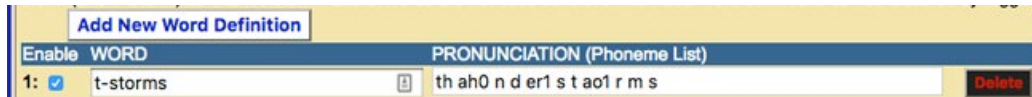
Choose File No file chosen

Upload .txt lexicon file

Edit Voice Screen

At the top of this screen are three action buttons: **Accept Changes**, **Cancel Changes**, and **Apply Changes**. For convenience purposes, they are replicated farther down the screen. The **Apply Changes** button will activate any changes made within the word

definition area, along with the Words per minute and Pitch factor percent text fields. This button allows users to make modifications and test them without leaving this screen. Once the desired modifications are made, the **Accept Changes** button will apply those changes, exit the user from this screen, and return to the **Setup > Main/ Licenses > Language Licenses** screen. This is also the best means to exit this screen. The **Cancel Changes** button voids any changes made prior to clicking the **Accept Changes** or **Apply Changes** buttons, and returns the user to the **Setup > Main/Licenses > Language Licenses** screen.

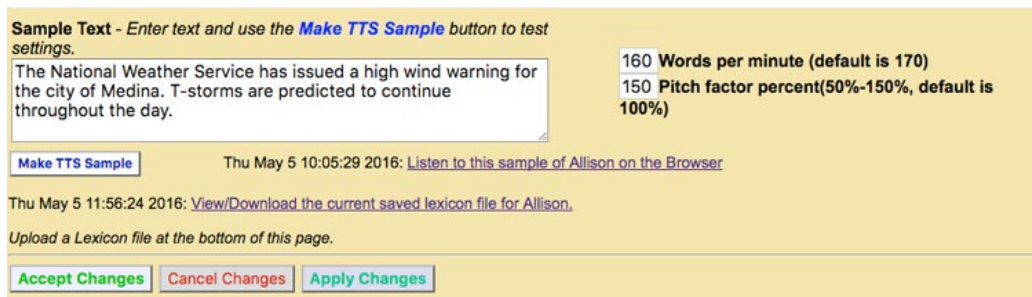


The next section down in this screen is the Word Definition section, or Lexicon Table. This area utilizes the **Add New Word Definition** button to specify a particular word and define its new pronunciation. Clicking this button will insert a new line at the bottom of the word definition list, where users enter the desired word (or string of text) in the **Word text entry field**, and enter the desired **Pronunciation**. Additionally, each Word Definition line includes an **Enable** check box and a **Delete** button. When the **Enable** check box is checked, that word and its corresponding pronunciation will be utilized by the TTS engine. If unchecked, it will be ignored. The **Delete** button will remove the associated word definition from the Lexicon Table.

Pronunciations are based on phonemes, the smallest unit of speech used to make one word. A list of phonemes rules is available by clicking the **Show phoneme rules chart** check box towards the bottom of the screen.



This list of phonemes are the only letter combinations the TTS engine will recognize. Notice all vowel phonemes are immediately followed a number (0 or 1). These numbers are emphasis values, where the 0 de-emphasizes that phoneme, and a 1 emphasizes that phoneme. Every vowel phoneme must contain an emphasis value (0 or 1) for the TTS engine to work properly.



Sample Text Section

Below the Lexicon Table is the Sample Text section. It is in the section where individual words and sentences can be sampled by the TTS engine. This section also includes the speed and pitch settings for this specific voice, along with saving/viewing the lexicon table files.

1. To sample a word, sentence or paragraph, enter the text into the **Sample Text** field. If this field is not large enough to accommodate the text in one view, click and drag the bottom right corner of the field to make it the appropriate size.



Attention

Make sure to click the **Apply Changes** button after making any changes to Word Definitions, Words per minute, and Pitch factor values. This applies to both the **Enable** check box and **Delete** button.



Note

The TTS engine is *not* case sensitive. Word definition fields will not allow upper case letters, and will properly pronounce words that are received with upper case letters, such as proper names.

2. Next, click the **Make TTS Sample** button. This action will create a sample of the text you entered that can then be played within the web browser application.
3. To play the newly created sample, click the hyperlink **Listen to this sample of Allison on the Browser**, and the web browser will play the latest TTS sample. The date found to the left of the hyperlink represents the date and time of the last TTS sample file that will be played.
4. After you have sampled the TTS file, click the **Back** button on the web browser to return to the Edit Voice screen.

The speed of each Premium Voice can be adjusted by entering a new numeric value into the **Words per minute** text field. The default value is 170. Lower numeric values slow down the voice, and higher values increase its speed. The pitch of each voice can be adjusted with the **Pitch factor percent** text field. The default value is 100 (or 100%). The value can range from 50-150; any entered value that is above or below this range will default to the nearest acceptable value. A lower value decreases the pitch, and a higher value increases the pitch.

```

#
# User lexicon entries go here, one per line, in the format
#
# WORD 0 PHONELIST
#
# with any amount of white space allowed.
#
# For example:
# cepstral 0 k eh1 p s t r ah0 l
#
t-storms 0 th ah0 n d er1 s t ao1 r m s
## wind 0 w eh1 n d
medina 0 m ah0 d ay1 n ah0

```

Lexicon Table Text File

Lexicon Tables (or Word Definitions) can be saved for archive purposes. Alternatively, a Lexicon Table may be transferred to another Premium Voice within the same EAS device, or any other EAS device. To view and save a Lexicon Table, click the **View/Download the current saved lexicon file** hyperlink at the bottom of the Sample Text section.

Make TTS Sample
Thu May 5 10:05:29 2016: [Listen to this sample of Allison on the Browser](#)

Thu May 5 11:56:24 2016: [View/Download the current saved lexicon file for Allison.](#)

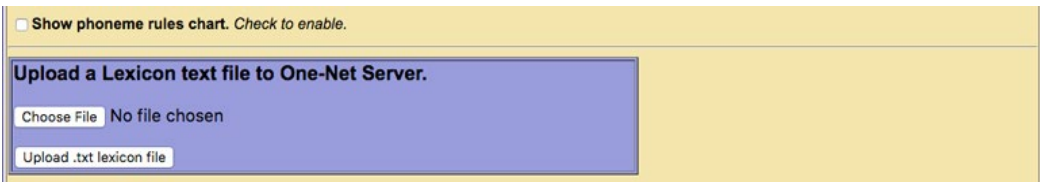
Upload a Lexicon file at the bottom of this page.

You will be presented with a .txt (text) file within the web browser. Use the **Save As...** or **Save Page As...** option found in the File pull-down menu of the web browser to save this file. Save the file to a local hard drive, not on the EAS device. The date to the left of the **View/Download the current lexicon file** hyperlink represents the last time/date the lexicon table was updated.



Caution

When uploading a Lexicon Table text file, it will overwrite the existing Lexicon Table. To retain any existing word definitions and add them to the new Lexicon Table, save the current Lexicon Table and use a standard text editor to combine it with the new table. Once those tables have been combined into one file, upload the file into the appropriate voice.



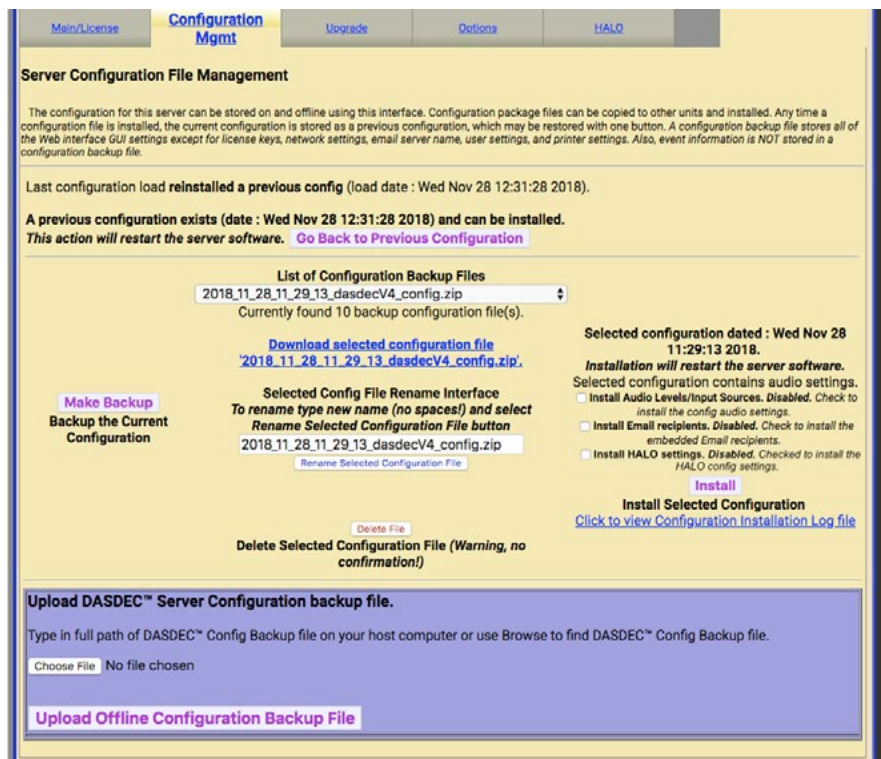
Upload a Lexicon Text File Section

To upload a Lexicon Table text file:

1. Find the purple shaded area at the bottom of the Edit Voice screen entitled **Upload a Lexicon text file...**
2. Click the **Choose File** button.
3. In the local file directory, select/open the appropriate text file.
4. Click the **Upload .txt lexicon file** button, located below the Choose File button.
5. The Lexicon Table text file will be uploaded into this Premium Voice.
6. Once the file has finished uploading, the Lexicon Table will show the new, uploaded Lexicon Table.

Server Configuration File Management

The **Setup > Server > Configuration Mgmt** screen is used to store, manage, and recall configuration backup files. You can create a copy of the current configuration settings and review previously saved configuration files. Each configuration backup is stored in an encrypted ZIP file that contains all settings selected in the setup process. The backup configuration files do not save Network setup, the email server name, user accounts, and license keys. Sound level, email recipients, and HALO settings are stored when a configuration backup file is created, and are optionally restorable.



Server Configuration File Management Screen



Note

In the Lexicon Table Text file, any line starting with a single hashtag (#) denotes a comment line, and is not used in the Lexicon Table. A line starting with two consecutive hashtags denotes a word definition that has not been enabled. This definition will be uploaded into the new table with the **Enable** check box unchecked.



Attention

A recent backup configuration file is **highly recommended**. Backup configuration files serve as a safety precaution. They provide a way to restore your EAS device settings in case of catastrophic disk failure or upgrade error, or to restore the state of former settings when experimenting with new settings. The backup allows you to easily and quickly return to the previous settings if a serious configuration mistake is made. The backup configuration file can also be downloaded to another computer for offline saving. Later, the backup configuration can be uploaded and reinstalled. The same configuration file can also be used to configure another EAS device.

The image above shows the current and previous backup configuration files. Three main areas to review on the Server Configuration File Management screen are the Previous Configuration (top of screen), a list of Configuration Backup Files (middle of screen), and an Upload Server Configuration backup file (purple shaded box at bottom of screen).

When the EAS device is configured for the first time, and before a backup configuration file is made, the page states, **There are no backup configuration files yet**. Remember to return to this page to create a backup configuration file after you have completed setting up the EAS device, or after you make significant changes.

To create the first backup configuration file, click the **Make Backup** button. After the first backup file is made, a pull-down list titled **List of Configuration Backup Files** appears, and the new file name appears in this list. All other standard configuration management options appear, such as a **Download selected configuration file** option, a **Rename Selected Configuration File** text field and action button, a **Delete File** button, and an **Install** button.

A **No previous configuration yet** message is displayed before any backup configuration files have been installed. A previous configuration file is created automatically whenever a backup configuration file is installed. When a previous configuration exists, the date of the file is presented, along with a button for reinstalling this configuration. The previous configuration backup allows you to easily and quickly return to the previous settings before installation of a backup configuration.

Software upgrades result in the creation of a configuration update file. This serves as a precaution in the rare event that an upgrade mangles an existing configuration. It can be used to attempt to restore settings to the pre-update state.

The **Go Back to Previous Configuration** button allows the EAS device to be restored to the state it was in prior to the last configuration file installation. The previous configuration option becomes available after a backup configuration file is first installed. The date of the configuration is listed.

The Configuration Backup Files section (middle) provides all controls needed to manage configuration backup files. Using the controls, you can save the current settings as configuration files, view a list of the stored configurations, rename any configuration, delete a configuration file, download a configuration to a remote computer, and install a configuration.

To create a backup file of the current configuration, click the **Make Backup** button.



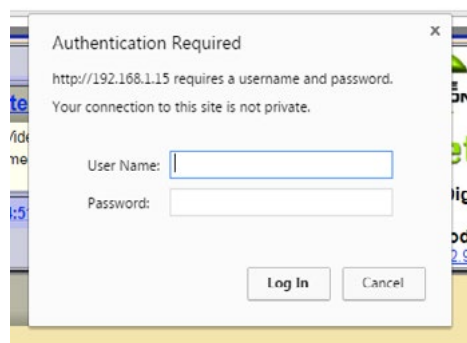
Note
It is recommended that you return to this page and make a new backup file each time significant and satisfactory changes are made to the EAS device configuration.

Configuration Backup File Section

The **List of Configuration Backup Files** pull-down menu displays the most recent backup configuration files. Use the pull-down menu to view and select a file. The selected file will be reflected in a number of other options described below. To add a file from a system, use the **Upload Server Configuration backup file** section found in the purple shaded area at the bottom of this screen.

To download a configuration file to the local host computer (not the EAS device), use the **List of Configuration Backup Files** pull-down menu, and select the appropriate file, which will display as a link. In the screen shot, the file is **2018_11_28_11_29_13_dasdecV4_config.zip**. Each Configuration Backup File will default to a similar name, based on date/time. Selecting the **Download selected configuration file...** hyperlink will allow you to save the file. Make sure to save it on your computer. Do not unzip the file.

The first time you attempt to download a configuration file, a prompt will be presented, requiring authentication. Enter the appropriate credentials; the file will then download to the local host computer.



Authentication Prompt

Many times the default configuration backup file name is not desirable. To rename the configuration file, type a new name in the text field above the **Rename Selected Configuration File** button, and click the **Rename Selected Configuration File** button. Do not use spaces or punctuation characters. Dashes, underscores, and dots are allowed.

The **Install** button installs the currently selected configuration file selected in the **List of Configuration Backup Files** pull-down menu. The date of the selected file is displayed above the button. Installation will restart the server software. Users are prompted with a confirmation screen to ensure the installation of the selected file is intended, and notification that a software restart will occur. Click the **Yes, Install Selected Configuration** button to confirm installation. Otherwise, click **Cancel Configuration Restoration**.

A complete backup file includes all the audio settings, any e-mail recipients and HALO settings.

Audio settings include all configuration settings found within the **Setup > Audio** screens, including:

- **Decoder Audio, Encoder Audio**
- **Audio Output Levels/Tests**
- **Radio Tuners**
- **Decoder Input Selections**



Note
When installing a configuration file and the **Install Email recipients** check box is NOT checked, all of the check boxes within the **Email** radio button screens will be modified to match the incoming configuration.

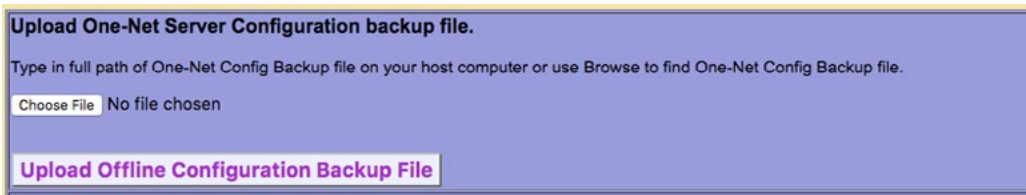
E-mail recipients include (found on the **EMail Server** sub-tab screen):

- any **Email To:** text entry fields
- the **From Name**

HALO settings include all the configuration settings found in the **Setup > Server > HALO** screen.

In some situations, it may not be desirable to recall audio, e-mail, and/or HALO settings. Users are given the option to incorporate these settings separately when utilizing the **Install** button. Prior to clicking the **Install** button, check the **Install Audio Levels**, **Install Email recipients**, and/or **Install HALO settings** check boxes to recall those settings during the Install process.

Users may delete the selected configuration file found in the **List of Configuration Backup Files** by clicking the **Delete File** button. There is NO confirmation opportunity, and the deletion is instantaneous.



Upload Server Configuration Backup File Section

The **Upload Server Configuration backup file** section, located at the bottom of the screen in the purple shaded area, provides an interface to upload a configuration file from a file system accessible to the local web browser host computer. Click the **Choose File** button, and locate and select the desired configuration backup file. Click the **Upload Offline Configuration Backup File** button. Once uploaded, the file appears in the **List of Configuration Backup Files** pull-down menu. Then it can be managed as described above (renamed, installed, deleted, etc.).



Caution

Installing V3 configuration files (created when running version 3.x software) will overwrite the HALO settings. Make sure to NOT check the **Install HALO settings** checkbox if installing a V3 configuration and HALO is licensed.



Caution

When deleting a configuration file from the list of backup files, there is no confirmation opportunity. The deletion is instantaneous.

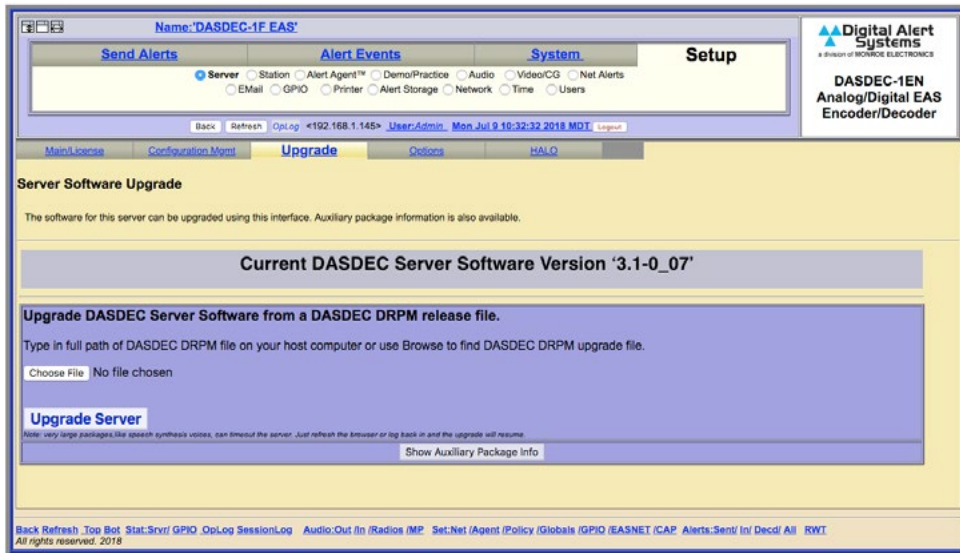


Attention

The process of uploading a server configuration backup file does not make it active within the EAS device. It simply loads that file into the list of available configuration backup files. The uploaded configuration file will then need to be selected in the **List of Configuration Backup Files** pull-down menu and installed (by clicking the **Install** button).

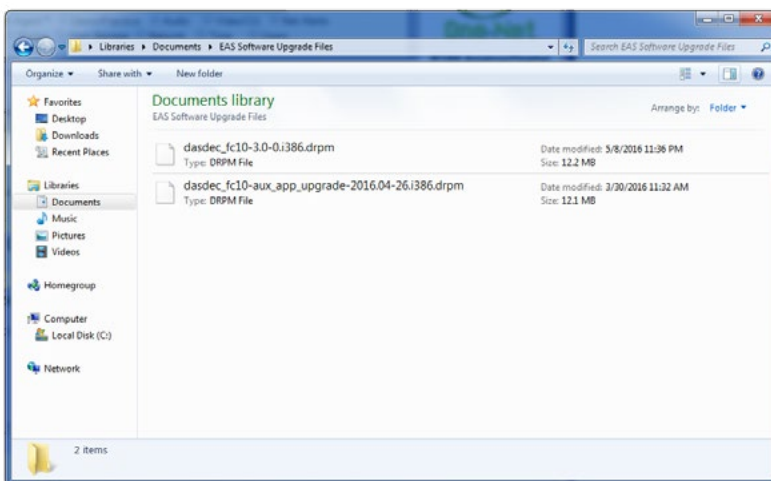
Upgrade: Server Software Upgrade

Software can be quickly and conveniently upgraded by going to the **Setup > Server > Upgrade** screen. This screen displays the current software version, provides the ability to upgrade software packages from a host computer into the EAS device, and provides a **Show Auxiliary Package Info** button to display the auxiliary software packages currently available in the EAS device.



Server Software Upgrade Screen

Software upgrades are performed by installing the upgrade package files. Some upgrades will have multiple software files that need to be installed individually. New software upgrade files are periodically available, and can be obtained from Digital Alert Systems/Monroe Electronics customer service.



Choose File - Windows Explorer

The upgrade software package files (.drpm files) must be available on a local host computer (laptop or desktop computer on the same network as the EAS device).



Note
Only user with **Admin Level** permission may perform software upgrades.



Caution
Always backup the configuration before installing a software update. Go to **Setup > Server > Configuration Mgmt** and click the **Make Backup** button. For safe keeping, download the backup configuration file from the same page to a host computer for safe keeping. See the above section, [Server Configuration File Management](#), for more details.



Caution
DO NOT power off the EAS device during the upgrade process. That may cause significant damage.

To perform a server software upgrade:

1. Click the **Choose File** button to access a file menu where the user can navigate to the desired software file.
2. Select the appropriate file and click **OK**, or double-click to accept.
3. Click the **Upgrade Server** button.
4. After a few moments, a confirmation screen will appear, asking to: **Yes, Upgrade Server** or **No, Cancel Server Upgrade**. Click the **Yes, Upgrade Server** button to proceed. If the file is acceptable, the upgrade will proceed and all users will be logged off the EAS device. The user will be presented with an *Upgrading...* screen, followed by the login screen, after a short period. The upgrade should take about a minute to complete.

In cases where multiple software files are provided as part of a software upgrade, the server software upgrade process will need to be performed for all software files.

Version 4.0 Specific Upgrade Instructions

When upgrading from version 3.x software to version 4.0, users will need to purchase a V4.0 software license key. Once purchased, Digital Alert Systems/Monroe Electronics will provide the user with a V4.0 Enabling Key, a link to download the V4.0 software, and credentials to access the software download via e-mail.

The Version 4.0 software upgrade is significantly different than previous upgrades, therefore it is important to become familiar with these steps and the requirements prior to starting this process.

In preparation for the V4.0 upgrade:

- Confirm the EAS device is 2nd generation hardware — DASDEC-II or One-Net SE
- Verify the EAS device is running V3.x software or higher (*if not, contact customer support*)
- Obtain a valid V4.0 Enabling Key for the specific device
- Download the file ***DAS_Updater.drpm*** from the Digital Alert Systems/Monroe Electronics website — using the link and password included in the V4.0 Enabling Key e-mail.
- The EAS device must have an active Internet connection to the secure upgrade server.
- If an active Internet connection is not available please contact our support team for additional instructions.
- It is **STRONGLY** advised to create backups of both the current configuration and EAS log files.

1. Load the initial DRPM File

To begin, load the **DRPM file *DAS_Updater.drpm*** into the EAS device. The file must be available on a local host computer (laptop or desktop computer on the same network as the EAS device.)

- 1.1. Log into the EAS device and navigate to the **Setup > Server > Upgrade** screen.



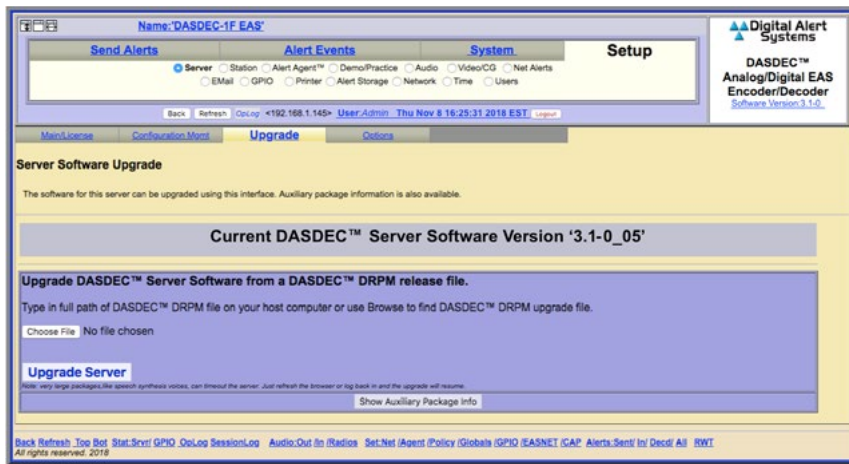
Warning

The **Version 4.0 Specific Upgrade Instructions** are to be used **ONLY** when upgrading from version 3.x software to version 4.0 software. Refer to the [Upgrade: Server Software Upgrade](#) instructions OR the upgrade instructions provided with the software release.



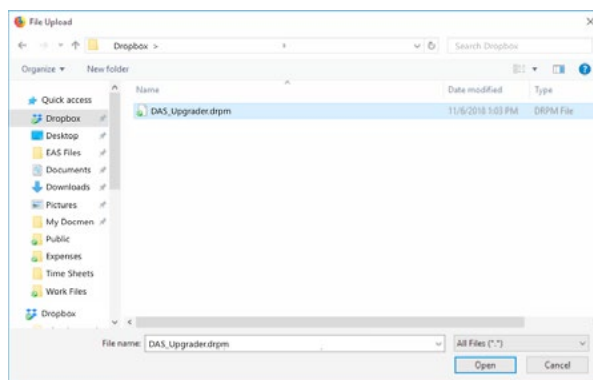
Attention

Version 4.0 can be installed on any 2nd generation hardware system currently running V3.0 or higher. If your system is running a software version below V3.0 or if your EAS device is not a DASDEC-II or One-Net SE, please contact customer service at support@monroe-electronics.com or support@digitalalertsistemas.com for further instructions. Be sure to include your serial number for verification.



Server Software Upgrade Screen (DASDEC version example)

- 1.2. Click the Choose File button and navigate to the desired DRPM software file.



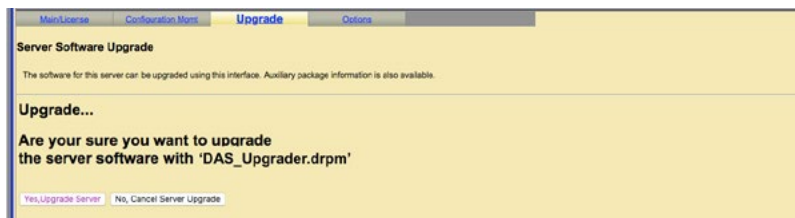
Choose File - Windows Explorer

- 1.3. Select the **DAS_Upgrader.drpm** file and click **Open**, or double-click to accept. The system returns to the **Setup > Server > Upgrade** screen and the selected DRPM file name is displayed next to the **Choose File** button.



Server Software Upgrade Screen with proper file selected

- 1.4. Click the **Upgrade Server** button. After a few moments, a confirmation screen will appear, asking to: **Yes, Upgrade Server** or **No, Cancel Server Upgrade**.



Upgrade - Confirmation Screen



Attention

Completely review the Version 4.0 Specific Instructions before proceeding with the upgrade. Failure to follow these instructions could render the device inoperable.



Note

Instructions to backup the current configuration settings are found in the [Server Configuration Management](#) section. Use the [Backing Up EAS Event Log](#) instructions in Section 6 of this manual.



Note

All existing log files, audio files, and backup configuration files will remain on the EAS device after the upgrade is complete.

- Click the **Yes, Upgrade Server** button to proceed. If the file is accepted as a valid upgrade file, all other users will be logged off and the upgrade will display the initial “*Upgrading ...*” screen.



Initial Upgrading... Screen

Following this screen, the device will display one of the following screens:

IF THE EAS DEVICE DOES NOT HAVE AN ACTIVE INTERNET CONNECTION; the user will see the **Upgrade Retry Screen**. Ensure the EAS device is able to reach the Internet and click the Retry button to proceed.



Upgrade Retry Screen

When the device validates its connection to the Upgrade Server the **Welcome to the 4.0 Software Upgrade** screen will appear.

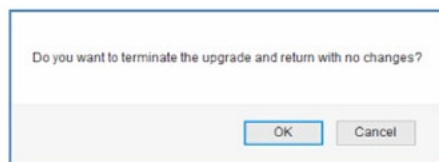


Welcome to the 4.0 Software Upgrade Screen

Proceed to [Step 2](#).

TO TERMINATE THE UPGRADE:

Clicking the **Cancel** button from either the **Upgrade Retry** or the **Welcome to the 4.0 Software Upgrade** screens will halt the upgrade with cancel confirmation dialog box:



Cancel Confirmation Dialog Box

- Clicking **OK** on this dialog box will terminate the upgrade and display an **Upgrade Canceled** page. Refreshing that screen returns to original v3.x login screen.
- Clicking **Cancel** returns to the **Welcome to the 4.0 Software Upgrade** screen.

2. Upgrade the DASDEC/One-Net Device

The **Welcome to the 4.0 Software Upgrade** screen shown above contains a single text box labeled ‘Enter 4.x Upgrade Key here’ along with a **Cancel** and **Start** buttons.

If you are unsure, please click on 'Cancel' and you will be returned to the current system with no changes made. To continue, enter your 4.x Upgrade Key below and click on 'Start'

Enter 4.x Upgrade Key here

Cancel Start

'Enter 4.x Upgrade Key here' Text Box

- 2.1. Locate the V4.0 Enabling Key for the EAS device and enter it into the text box. Note: it's typically easiest to cut & paste the key from the email. Be sure to include all characters. If the key is improperly entered it can be corrected in the verification steps after installation is completed.
- 2.2. Click the **Start** button to proceed and the upgrade confirmation dialog box will appear on the screen.

Once started, the upgrade cannot be undone.
Are you sure you want to upgrade?

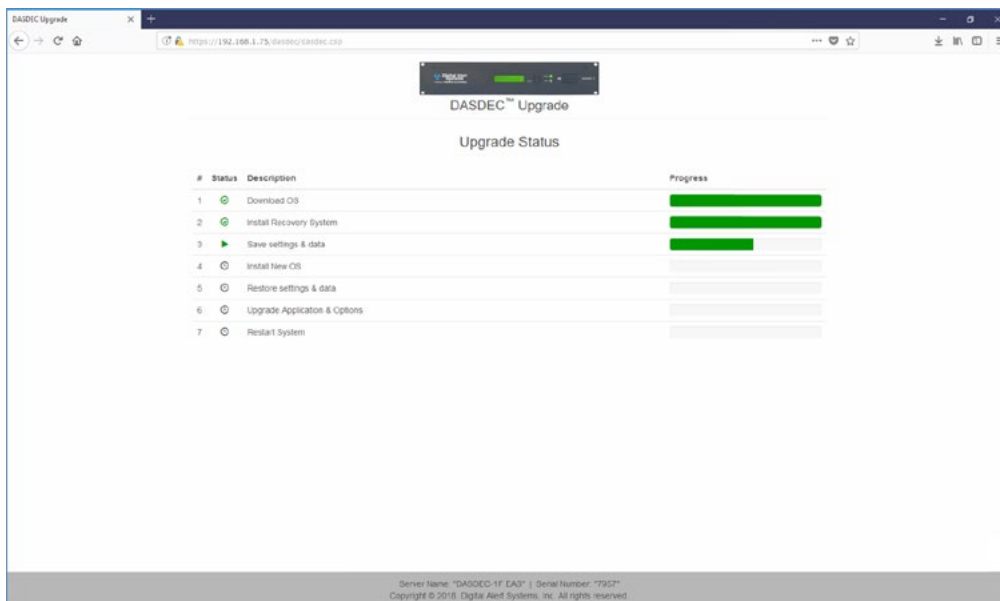
OK Cancel

Upgrade Confirmation Dialog Box

- 2.3. Click the **OK** button found on the upgrade confirmation dialog box to continue the upgrade process. Clicking the **Cancel** button returns the user to the Welcome to the 4.0 Software Upgrade screen

If communication with the secure upgrade server is successful the Upgrade Status screen will appear – displaying the upgrade's sequential progress. Recognize some steps may take longer than others. It is important to **be patient and not interrupt the upgrade process.**

There is no user interaction on this screen. Simply monitor the progress bars as the installer completes each section of the upgrade.



V4.0 Upgrade Status Screen



Note

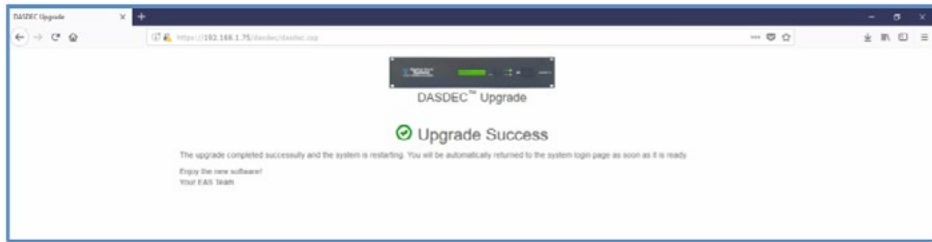
The V4.0 Enabling Key is unique for each EAS device and is automatically added to the **Setup > Server > Main/License** page without verification. If the key is entered incorrectly, the user will be able to verify and correct it during the verification of the upgrade process.



Attention

The time required to complete the upgrade depends on several variables such as internet connection speed, size and number of existing logs and files, and processor speed. Please understand the entire process may take from 15 minutes to several hours to complete.

Once the upgrade is complete, the EAS device will display the Upgrade Success screen and automatically restart.



Upgrade Success Screen

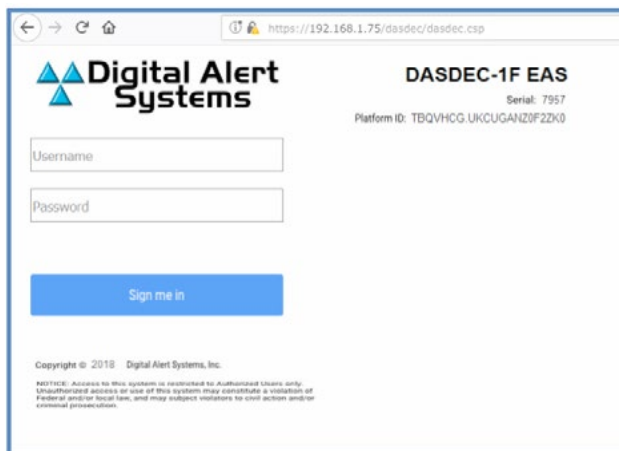
2.4. The display should automatically refresh and present the user with **Resend Information** dialog box, however, depending on the browser, it may be necessary to refresh the web browser manually. Give the unit a few minutes to restart prior to manually refreshing.



Resend Information Dialog Box

2.5. Within the Resend Information dialog box, click the **Resend** button to proceed.

Upon completion, the EAS device will display the new V4.0 login screen.

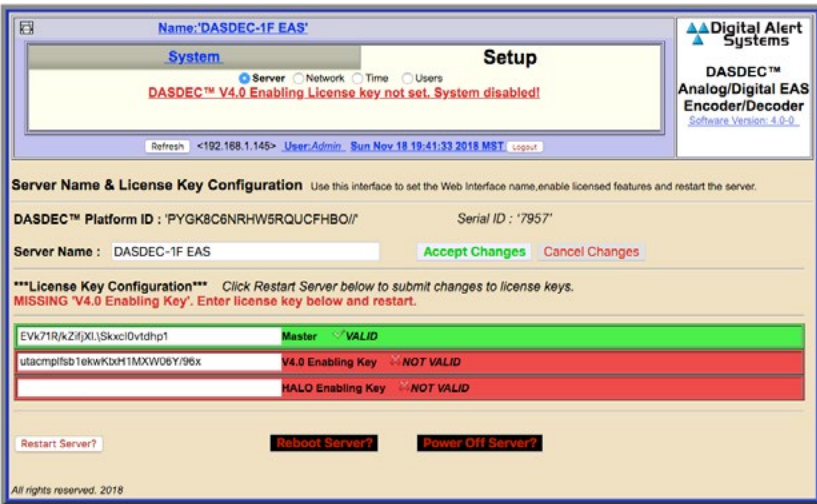


V4.0 Login Screen

3. Verify the V4.0 Enabling Key license key is valid.

3.1. Log into the EAS device as usual.

If, during Step 2.1, an invalid V4.0 Enabling Key was entered in the **Welcome to the 4.0 Software Upgrade** screen, the EAS device will automatically open to the **Setup > Server > Main/License** screen and request a valid key be entered.



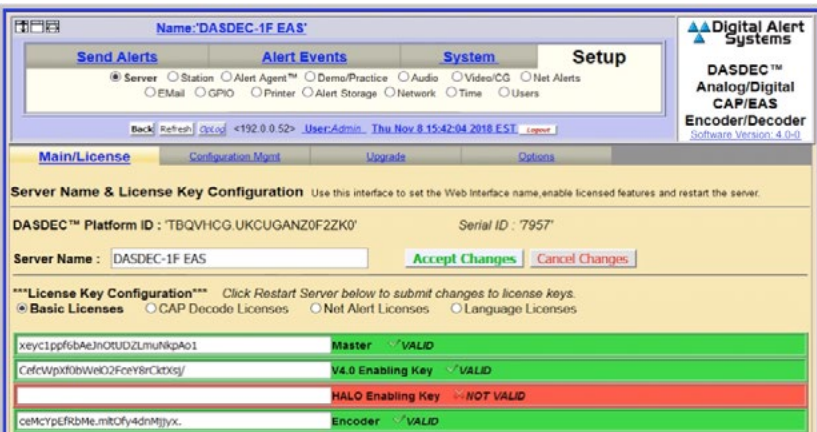
Setup > Server > Main/License screen with example of an invalid V4.0 Enabling

3.2. Enter the proper V4.0 Enabling Key from the provided e-mail – ensuring the license key:

- Corresponds to the serial ID of the device
- Contains all characters between the quotes - including punctuation characters such as periods, dashes, slashes, etc.

3.3. Click the **Restart Server?** button. A Server Software Restart confirmation screen will then appear. Click the **Yes, Restart Server** button to complete the restart procedure.

To reconfirm the validity of the V4.0 Enabling Key, log back into the EAS device and check the text to the right of the **V4.0 Enabling Key** field reads **VALID** and the background is colored green. This indicates the proper license key has been entered and the unit is fully operational.



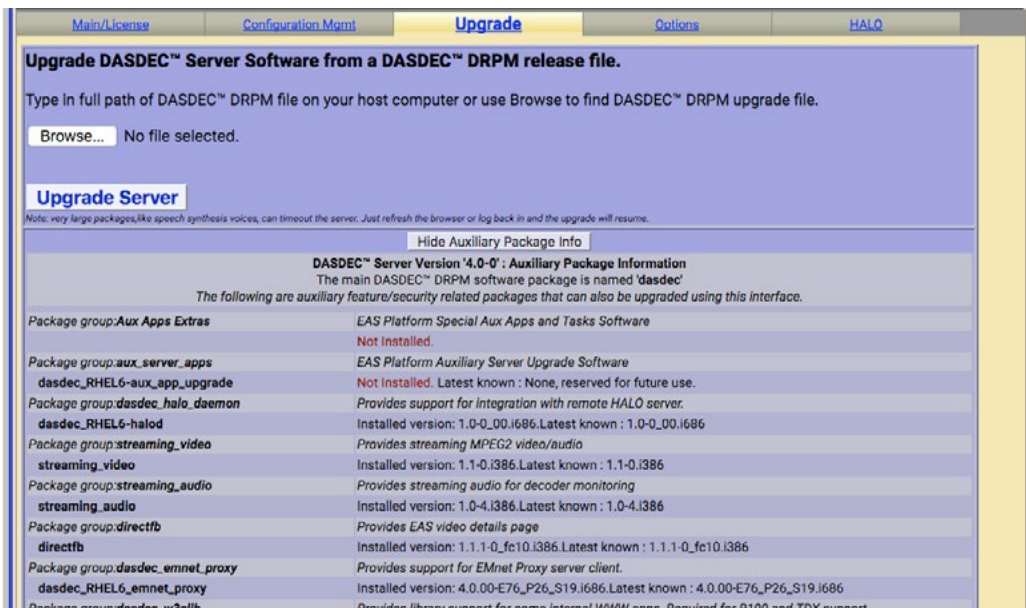
Setup > Server > Main/License screen example showing a valid V4.0 Enabling Key

This completes the DASDEC/One-Net Version 4 upgrade! The user now has complete control of the EAS device. For more detailed information regarding License Keys, refer to the [Main/License: Server Name & License Key Configuration](#) section of this manual.

It is recommended to go to **Setup > Server > Configuration Mgmt** and click the **Make Backup** button to make a V4.0 version backup. See the [Server Configuration File Management](#) section of this manual for additional information.

A **Show Auxiliary Package Info** button at the bottom of the screen displays the currently installed auxiliary files. Clicking this button expands the upgrade screen to display auxiliary feature/security related packages that can also be upgraded using the upgrade interface. Each Auxiliary Package is displayed, along with an explanation of its function, the currently installed version, and the latest known version (as known to the currently installed package). This information is useful when determining if the EAS device has the most current versions of auxiliary software.

Auxiliary Package files are installed in the same fashion Server Software Upgrade files are installed. Locate and select the desired software file by clicking the **Choose File** button. Then click **Upgrade Server** followed by the **Yes, Upgrade Server** button on the confirmation screen to complete the process. The EAS device will log out all users to perform the software restart, and present a login screen once the software restart is complete.



Auxiliary Package Info Session

This expanded view also includes a special **Rebuild RPM Package Database** button for repairing the internal package database. Use this button to repair the RPM package database in case of package installation failure due to RPM database corruption. This command should rarely, if ever, be needed, and should only be used under the direct request of a customer service representative.

Clicking the **Hide Auxiliary Package Info** button at the top of the Auxiliary Package list will collapse the list and set the page back to the simple upgrade interface screen.

Options: Platform Configurations Options

The **Setup > Server > Options** screen is designed to interface with various platform options. These include enabling debug logging, USB port speed, text encoding, CAP output encoding, and Monroe Electronics Model 988 Clock Sync support.



Warning

Do not click the Rebuild RPM Package Database button unless instructed by a Digital Alert Systems/ Monroe Electronics customer service representative.



Platform Configuration Options Screen

The **Server Debug Log Interface** check box enables or disables the Debug Logs. These logs allow customer service engineers to gain a better view of what might be happening with an EAS device. When this option is enabled, a **Debuglogs** radio button is added to the **System** main tab, adding the following sub-tabs: **Decoder**, **Main Server**, **Serial**, **Audio**, **Video**, **Network**, and **Web Server**. For each of these sub-tab categories, a pull-down menu enables users to set either Basic or Extra Debug Log Detail Level or None at all. These pull-down menus allow users to turn on specific debug logs for any of the above sub-tab categories. For example, if the system is experiencing issues communicating via the serial interface with an external character generator (CG), Basic or Extra Debug Log Detail may be selected from a pull-down found in the Serial sub-tab. Data being sent and received between the EAS device and the CG will be documented in the Serial Port Server Log, found on this screen. When the **Server Debug Log Interface** is enabled, those changes are immediate and a hyperlink titled **Link to Debug pages** is made visible, and navigates them to the **System > Debuglogs** screen. When debugging is no longer needed, make sure to uncheck the **Server Debug Log Interface** check box.

The **Select USB Port Speed Option** check box allows users to change the speed at which data is transferred via USB in the EAS device. This feature is important for some USB to Serial applications, where the USB to Serial device may only support USB 1.1 and not USB 2.0. USB 1.1 Serial Adaptors need to run with USB 1.1 speed.

Select Text Encoding Option radio buttons determine whether Windows-1252 or UTF-8 text encoding is used. Windows 1252 is the default setting; however, in situations where non-English languages are required, UTF-8 would be the preferred method. This will provide a more extensive set of characters that include foreign characters.



Note
The Server Debug Log Interface feature is typically used by and under the direction of a qualified customer service engineer. Do not turn this feature on unless directed by a Digital Alert Systems/ Monroe Electronics customer service engineer.

For CAP communications, UTF-8 is the standard text encoding method. Single byte UTF-8 is the default setting, because it is more universally adapted. The **Force Single Byte UTF-8 encoding for CAP and EAS NET** check box should normally be checked. When exclusively communicating with Digital Alert Systems/Monroe Electronics EAS equipment, this setting can be left unchecked.

The Monroe Electronics Model 988 is an interface enabling local authorities secure access via telephone lines to activate the attached EAS device for preselected areas with alarm messages and allows the caller to record an emergency voice message to be played during the alert. The Model 988 embedded clock can be synchronized with the EAS device by connecting a USB cable (supplied with the 988) between it and the DASDEC/One-Net. Check the **Monroe 988 Clock Sync Support** check box and restart the server software to enable the clock sync support. A hyperlink labeled **Link to page with restart button** will direct the web interface to the **Setup > Server > Main/License** screen where a **Restart Server?** button is available towards the bottom of the screen. Click the **Yes, Restart Server** button on the confirmation screen to complete the server restart process. Separate configuration of the 988 will be required.

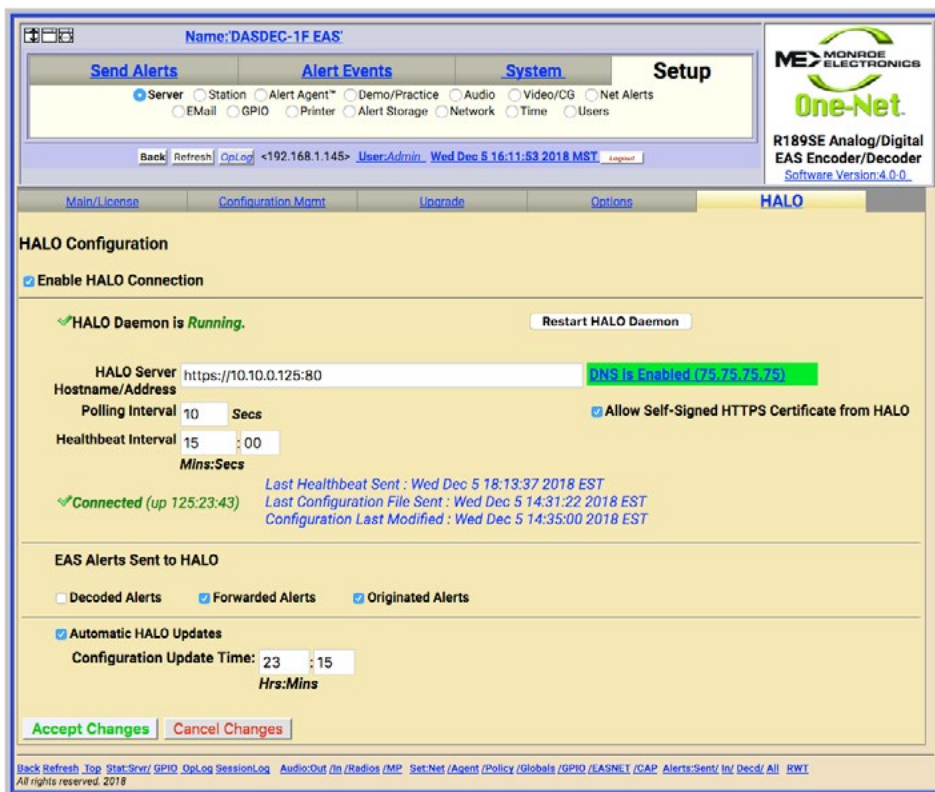
HALO Configuration

HALO is an enterprise-level EAS management system developed by Digital Alert Systems/Monroe Electronics to consolidate the monitoring and management of multiple EAS devices into single user interface. The system enables multiple users individualized access to monitor the status of all connected DASDEC/One-Net EAS devices, automatically store back up configuration files, centralize the collection of EAS alerts, and much more.



New Feature

Version 4.0 introduces support for HALO - the industries first Enterprise-Level EAS Management System. Additional information on HALO is found at the [Digital Alert Systems](#) and [Monroe Electronics](#) websites.



HALO Configuration Screen

The HALO sub-tab is available when a valid **HALO Enabling Key** is entered into the system. The settings found on this screen enable the connection between this device and the HALO server. These settings also establish when back up configuration files are sent to HALO and the types of EAS alerts sent to HALO. The HALO Configuration screen has three main sections: HALO Connection, EAS Alerts, and Automatic HALO Updates.

HALO Connection Section

This top-most section of the screen is focused on settings necessary to connect this device to the HALO server.



Attention

Contact your system administrator or data center IT professional to obtain the Hostname or IP Address of the installed HALO server within your network prior to configuring these settings.

HALO Configuration

Enable HALO Connection

✓ HALO Daemon is **Running**. Restart HALO Daemon

HALO Server Hostname/Address: DNS is Enabled (75.75.75.75)

Polling Interval: Secs Allow Self-Signed HTTPS Certificate from HALO

Healthbeat Interval: : Mins:Secs

✓ Connected (up 125:23:43)

Last Healthbeat Sent : Wed Dec 5 18:13:37 2018 EST
Last Configuration File Sent : Wed Dec 5 14:31:22 2018 EST
Configuration Last Modified : Wed Dec 5 14:35:00 2018 EST

HALO Sub-Tab - HALO Connection Section

Enable HALO Connection check box

This check box will either enable or disable any and all communication between the EAS device and the HALO server. Check (enable) this check box to configure these settings and enable communication with the HALO server. When unchecked (disabled), none of the HALO configuration setting may be configured.

The Admin user account may choose to display or not display this check box to all users. Navigate to the **Setup > Users** screen and select the Admin user from the pull down menu within the Edit Server User Account Profile (top left) of this interface. There are several display options visible including **Display HALO Daemon disable/enable on Setup->Server->HALO page**. Checking (enable) this check box will display the check box on the Setup > Server > HALO screen for all users. Unchecking (disable) this check box will not display this same check box.

HALO Daemon Status

The HALO Daemon is an Auxiliary Package charged with the task of managing the connection to the HALO server. This package must be in a **Running** state to maintain a this connection.

Restart HALO Daemon

In situations when the HALO Daemon is not in the **Running** state, the Restart HALO Daemon button can be pressed.

HALO Server Hostname / Address

This setting is where the user enters either an IP address or hostname of the HALO server. This interface supports both secure (HTTPS) and non-secure (HTTP) schemes in an IPv4 URL format.

A properly formatted IPv4 URL must be entered into this field. It is important to enter the full address including 'http://' or 'https://', followed by the IP address of the HALO server. Most likely a network port will be assigned to the communications between the EAS device and the HALO server. A port number may be added directly following the

IP address by entering a colon ':' and the port number. Using the example found in the above screen capture, the URL is 'https://10.10.0.125:80' - where the 'https://' denotes a secure connection, '10.10.0.125' is the IP address of the HALO server and ':80' is the port number assigned to EAS device communications with the HALO server.

When using a hostname, the name will need to be registered with a local DNS server so it can be resolved to the HALO server.

Allow Self-Signed HTTPS Certificate from HALO

In order to establish secure network communications a certificate is utilized. The HALO server comes with a self-signed certificate. For the EAS device to use this certificate or any other self-signed certificate, the user must check (enable) this check box. When using a certificate authority (CA) or non-secure communications (HTTP), this check box should remain unchecked.

Polling Interval


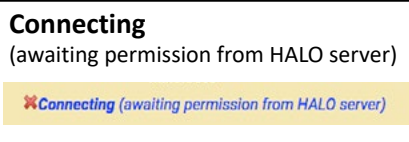
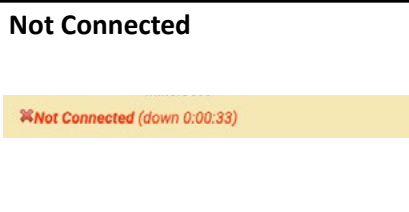
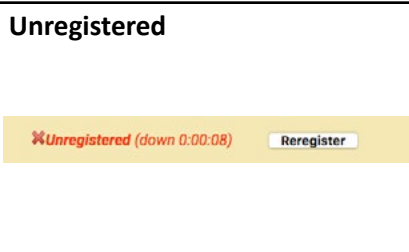
Each EAS device reaches out to the HALO server using the frequency set by this Polling Interval. This value can range from 2 to 120 seconds. The default value is 10 seconds.

Healthbeat Interval

HALO Healthbeats are regular, information-rich communications each EAS device sends to the HALO server. Status information regarding the analog (radios), CAP and EAS-Net monitoring inputs are sent to the HALO server on these regular intervals.

Connection Status

The status of the connection between the EAS device and the HALO server is displayed just below the Healthbeat Interval settings. This section will display one of four statuses: Connected, Connecting, Down, and Unregistered.

Connection Status	Description
<p>Connected</p> 	<p>This status will display a check mark, status text and the 'up' time for this connection in a green color. To the right of this status are three date/time values for the following:</p> <ul style="list-style-type: none"> Last Healthbeat Sent Last Configuration File Sent Configuration Last Modified
<p>Connecting (awaiting permission from HALO server)</p> 	<p>The EAS device has successfully made contact with the HALO server and is awaiting permission to be added to HALO. This device will show up in the HALO interface in the left pane - Queued tab.</p>
<p>Not Connected</p> 	<p>This status is displayed for one of two reasons: no connection has been established to the HALO server OR the established connection has been broken. When a connection has been broken there will be additional text displaying the amount of time the connection has been lost.</p>
<p>Unregistered</p> 	<p>The EAS device has been removed from HALO by an authorized user. The amount of time the device has been unregistered is displayed to the right of the status. The device is no longer communicating with HALO. To reregister the device with HALO, click the Reregister button. The device will again be available in the Queued tab of HALO.</p>

EAS Alerts Section

The EAS device has the ability to send EAS alerts to the HALO server so they may be consolidated, filtered, sorted, and searched within a central user interface. The types of EAS alerts sent to HALO is decided in this section of the screen.



EAS Alerts Sent to HALO

Decoded Alerts Forwarded Alerts Originated Alerts

HALO Sub-Tab - EAS Alerts Section

There are three check boxes allowing users to either enable or disable each of these EAS event types of alerts sent to HALO:

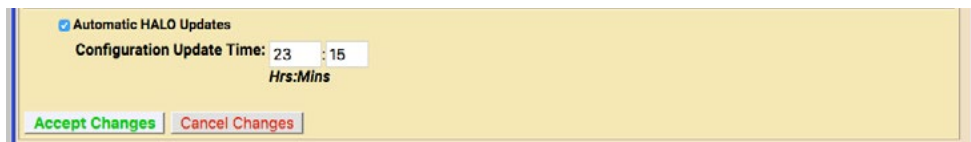
- Decoded Alerts
- Forwarded Alerts
- Originated Alerts

Check the boxes corresponding with event types desired to send to the HALO server. Uncheck the boxes for those event types not desired to send to HALO.

Automatic HALO Updates Section

HALO offers the ability to automatically create backup configuration files and send them to the HALO server for storage and management. Backup configuration files may be automatically generated:

- Once every 24 hours - at the time set by the user (Configuration Update Time)
- ONLY if changes have been made to the configuration settings within the last 24 hours



Automatic HALO Updates

Configuration Update Time: 23 : 15
Hrs: Mins

Accept Changes Cancel Changes

HALO Sub-Tab - Automatic HALO Updates Section

Automatic HALO Updates check box

This check box allows the user to enable (check) or disable (uncheck) the automatic generation of backup configuration files sent to HALO. When checked, the Configuration Update Time settings become available to the user.

Configuration Update Time

These two numeric text boxes allow the user to enter a time of day in a 24-hour clock format. The left box represents hours (0-23) and the right represents minutes (0-59).

Once the desired updates have been made to the HALO screen, click the **Accept Changes** button to input these settings. The **Cancel Changes** button is used to cancel any updates and refresh the screen.

Note

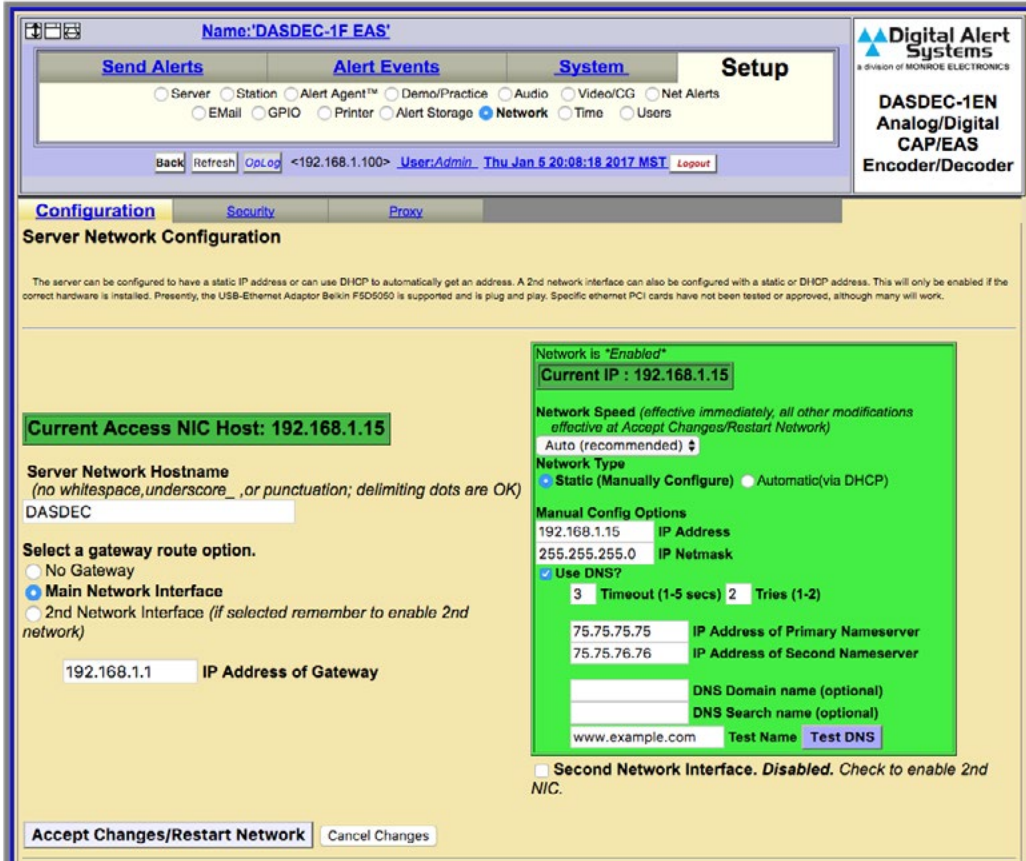
Selecting both Decoded and Forwarded EAS alert event types will send duplicate alerts to HALO since many alerts are decoded and then forwarded. It may be desirable to see all decoded alerts along with the forwarded alerts. It is important to understand by doing this, there will be duplicates.



NETWORK SETUP

There are three sub-tab categories within the **Setup > Network** screen: Configuration, Security, and Proxy. Users will use these categories to configure the EAS device to operate one or multiple networks. HTTPS and SSH security protocols may be enabled and configured. Optional proxy servers may be employed as well.

Configuration: Server Network Configuration



Server Network Configuration Screen (top half)

This screen displays the current network state, and provides controls to configure Server Network Hostname, Network Ethernet IP Addresses, Gateway, and Static Routes. It also displays extensive network configuration information such as Network Routing Table, Static Routes, Network Configuration Settings, DNS Configurations, Network Host, and Network Device Settings.

Recent EAS device models include two network interfaces (or NIC). Each NIC can be configured with individual IP addresses, either by manually entering a static IP address (recommended) or by selecting DHCP to automatically assign network addresses.

The current IP address is displayed just above the entry field for the Server Network Hostname. Other important network configuration info is displayed on the bottom half of the page. See subsequent chapters for more information.

Server Network Hostname

The **Server Network Hostname** field is used to identify this individual EAS device on an IP network. Create a unique name, so as to clearly differentiate this device from other network devices and other EAS devices within the same facility/network. This



Warning

Always install the EAS device behind a firewall or other security measures and restrict network access to trusted hosts and networks only. Never allow direct access to the Internet.



Attention

It is advised that you contact a network administrator or IT professional before modifying any network settings. A working knowledge of your facility's network settings and topology will be helpful when establishing and/or modifying these configuration settings.



Note

An optional Gigabit Ethernet Expansion kit (factory installed) will increase the overall NIC count to four. Each NIC may be enabled by checking the associated **Network Interface** check box.



Note

The **Server Network Hostname** is different from the **Server Name** found in the **Setup > Server > Main/License** screen.

name can also be very important for correct functioning of e-mail. Some e-mail systems require a fully qualified network hostname (e.g., dasdec.mysystem.com). If the EAS device has been given a network name by a system administrator, this name must be entered here.

Enter a unique **Server Network Hostname** into this text field. This must be a continuous string of characters (no spaces), and must not contain an underscore or any type of punctuation except for delimiting dots. Click the **Accept Changes/Restart Network** button to enable this change.

To save any changes to the network interface (except for **Network Speed**), click the **Accept Changes/Restart Network** button.

Gateway Configuration

A gateway is needed to enable direct access to the Internet, or to other networks within a LAN, or if the EAS device will be multicast streaming either MPEG Audio/Video or SCTE-18.

Three radio buttons are provided to select a gateway route option:

- No Gateway
- Main Interface
- 2nd Network Interface

If a gateway is required:

- Select one of the available Network Interfaces by clicking the desired radio button. Any network interface can determine the gateway address range, but there can only be one gateway, and it must be within one of the defined networks.

If a gateway option is selected:

- Enter the IP Address of Gateway within the chosen network. The common value for a gateway address ends in 1 (###.###. ###. 1).

Network Interface Configuration

To configure a network interface, first locate the desired Network Interface configuration box (shown in green above) and determine the appropriate **Network Type**. The **Network Speed** pull-down menu is used to select a fixed network speed for that NIC, or select Auto (recommended), and the NIC will automatically select the appropriate speed.

For Static IP Addresses:

1. Select the **Static (Manually Configure)** radio button.
2. Enter the desired IP address into the **IP Address** text field (including the dots).
3. Enter the desired **IP Netmask** (or subnet mask) in the same way.



Caution

You must be careful when configuring a static IP address. If an inaccessible address is configured into the EAS device, users will not be able to log back in until the remote host's IP address is within the same IP address range as the EAS device.

Configuration Security Proxy

Server Network Configuration

The server can be configured to have a static IP address or can use DHCP to automatically get an address. A 2nd network interface can also be configured with a static or DHCP address. This will only be enabled if the correct hardware is installed. Presently, the USB-Ethernet Adaptor Belkin F5D0500 is supported and is plug and play. Specific ethernet PCI cards have not been tested or approved, although many will work.

Current Access NIC Host: 192.168.1.15

Server Network Hostname
(no whitespace, underscore, or punctuation; delimiting dots are OK)
DASDEC

Select a gateway route option.

No Gateway

Main Network Interface

2nd Network Interface (if selected remember to enable 2nd network)

Use Static Gateway IP Address for DHCP device

Gateway for DHCP device 'eth0' not yet ready.

Network is "Enabled"
Current IP : 192.168.1.15

Network Speed (effective immediately, all other modifications effective at Accept Changes/Restart Network)
Auto (recommended)

Network Type

Static (Manually Configure) **Automatic (via DHCP)**
Proposed change to DHCP

DHCP Values && optional 2nd Nameserver config

3 Timeout (1-5 secs) 2 Tries (1-2)

75.75.75.75 IP Address of Primary Nameserver

75.75.76.76 IP Address of Second Nameserver

DNS Domain name (optional)

DNS Search name (optional)

www.example.com Test Name **Test DNS**

Second Network Interface. Disabled. Check to enable 2nd NIC.

Accept Changes/Restart Network Cancel Changes

Server Network Configuration Screen (unaccepted changes)

For DHCP:

1. Select the **Automatic (via DHCP)** radio button.
2. Check the **Use Static Gateway IP Address for DHCP** check box.
3. Enter the address of the gateway server into the **IP Address of Gateway** text field.
4. Enter the address of the **Primary** and **Secondary Nameserver**.

The **Use DNS** check box must be selected, and the DNS (Dynamic Name Server) configured when communicating on the Internet. This is necessary to interface with FEMA IPAWS and PELMOREX CAP servers along with email services.

To enable DNS:

1. Check the **Use DNS?** check box at the bottom of the NIC configuration box.
2. Additional configuration text fields will appear.
3. Enter the desired IP address into the **IP Address of Primary Nameserver**.
4. Enter the desired IP address into the **IP Address of Secondary Nameserver**.
5. If available, enter the **DNS Domain name (optional)**.
6. If available, enter the **DNS Search name (optional)**.

Timeout

This is the maximum amount of time the system will take to make contact with the configured DNS/Nameserver before reporting a negative result of the DNS query. A positive result will immediately be reported. A value between 1 to 5 seconds may be entered.

Tries

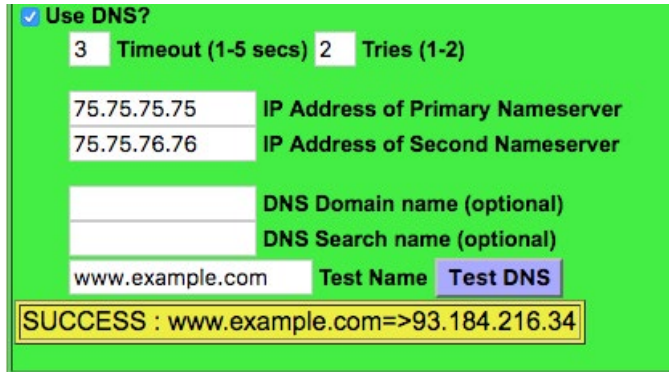
The EAS device will attempt to make contact with the configured DNS/Nameserver the number of tries entered in this field. Either a 1 or 2 value may be entered in this field.

Test Name

This text entry field enables users to test the configured DNS/Nameserver settings (above) by entering a web address (such as www.example.com). Once a good web address is entered, press the Test DNS button.

Test DNS

By clicking the Test DNS button, the system will initiate a search of the given Test Name using the DNS/Nameserver information provided above.



The screenshot shows a green-themed interface for testing DNS settings. At the top, there is a checked checkbox labeled "Use DNS?". Below it are two input fields: "Timeout (1-5 secs)" with the value "3" and "Tries (1-2)" with the value "2". There are two more input fields for "IP Address of Primary Nameserver" (75.75.75.75) and "IP Address of Second Nameserver" (75.75.76.76). Below these are two more input fields for "DNS Domain name (optional)" and "DNS Search name (optional)". At the bottom, there is a "Test Name" input field containing "www.example.com" and a "Test DNS" button. A yellow box at the bottom of the interface displays the result: "SUCCESS : www.example.com=>93.184.216.34".

Successful DNS Test

A second network interface may be enabled by checking the Second Network Interface check box, found just below the Main Network Interface. Follow the above procedure for configuring the second NIC.

The Network Interface box has three different color status:

- **Green:** Valid settings and operational. The box is labeled *Network is *Enabled** in the top-left corner.
- **Brown:** Proposed changes have been made, but not accepted. The NIC is still using the previous settings. Click the **Accept Changes/Restart Network** button to activate the proposed changes.
- **Yellow** (same color as background): The network interface is currently disabled. The box is labeled Network is **Disabled** in the top-left corner. Input configuration settings and click Accept Changes/Restart Network button.

Default settings:

- **IP Address:** The primary network interface is factory set to a static IP address of 192.168.0.200. This is a commonly used, non-public IP address for LAN based appliance hardware. This value is meant to be changed.
- **IP Netmask:** The default IP netmask is 255.255.0.0.
- **DNS or Gateway:** No default DNS or gateway is configured.



Note

www.example.com is a domain name reserved by the Internet Assigned Numbers Authority (IANA) for use in documentation. It is an active web address that can be used for this test.



Attention

The network part of the IP address for the second network must be unique compared to the main interface network. Otherwise, either interface will probably not function. For example, if the main network is 10.0.1. #, a separate network would be 192.168.1. #. There is not a separate DNS to configure for the second network.

Network Status Information

Tables at the bottom of the Setup Network Configuration page show:

- Current Network Routing Table
- Current Network Static Routes
- Remote Rsyslog Configuration
- Current Network Configuration
- Current DNS Configuration
- Current Network Hosts
- Network Device Settings (one for each active network interface)

This information reflects the actual state of the network configuration, and is provided to help with network configuration and troubleshooting.

If the network configuration is damaged, it is possible for the information in this table to not match the configured values displayed in the user interface fields. The information in this table is definitive and accurate.

Current Network Routing Table

To add and test specific routes, login as 'root' on console and use the linux 'route' or 'ip route' command. Command syntax help is available by running 'man route' or 'man ip' and 'ip route help'. Permanent routes can be added as a static route, see below.

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.136.0 0.0.0.0 255.255.255.0 U 0 0 0 eth10
10.120.100.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
169.254.0.0 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1
169.254.0.0 0.0.0.0 255.255.0.0 U 1007 0 0 eth10
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 eth0
```

Current Network Static Routes (from file /etc/sysconfig/static-routes)

```
#any net 192.168.0.0 netmask 255.255.0.0 eth0
```

Static Route Configuration

The server can be configured with this interface to build static routes to specified networks. Make changes then submit and restart network with the **Accept Static Route Changes/Restart Network** button.

Static Route 1: Enable IP Address Netmask Gateway

Device

To manually add specific routes at network restart from the console, login as 'root' on console and manually edit /etc/sysconfig/static-routes. Route entries can be conveniently disabled by placing the '#' as the first character on a line (this turns the line into a comment). Then either run '/etc/init.d/network restart' or 'reboot'.

Remote Rsyslog Config (from file /etc/rsyslog.conf)

Enable Host Name/IP Port

Current Network Configuration

```
eth0 Link encap:Ethernet HWaddr 00:30:18:C5:6E:D6
inet addr:192.168.1.15 Bcast:192.168.1.255 Mask:255.255.255.0
```

Server Network Configuration Screen (Network Status Information)

Static Route Configuration

This simple interface allows statically defined network routes to be configured, enabled/disabled and added/deleted at network startup.

To configure a static route:

1. Click the **Add Static Route** button within the Static Route Configuration section of the screen. A series of static route configuration settings will appear.
2. Enter the **IP Address**, **Netmask** (or subnet mask), and **Gateway** settings into their respective text fields.
3. Select the desired network interface. These settings should be applied from the pull-down menu.
4. Enable the static route by checking the **Enable** check box.
5. Click the **Accept Static Route Changes/Restart** button to apply these settings.

To disable a static route:

1. Uncheck the **Enable** check box.
2. Click the **Accept Static Route Changes/Restart** button.
3. The other static route configuration settings will remain, and the route will remain inactive until enabled again.

Remote Rsyslog Configuration

The Remote Rsyslog support on the EAS device allows users to designate a remote location to send the /etc/rsyslog.conf file. This interface provides the ability to enable/disable the sending of this file via TCP or UDP. All Rsyslog communication is immediately updated to the destination.

To enable the Remote Rsyslog feature:

1. Click the **Enable** check box
2. Select the desired communication protocol (TCP or UDP) from the pull-down menu
3. Enter the desired host name or IP address for the file destination
4. Enter the desired communications port. The default port is set to 514.
5. Click the **Accept Remote Rsyslog Changes** button

To disable the Remote Rsyslog feature:

1. Uncheck the **Enable** check box
2. Click the **Accept Remote Rsyslog Changes** button

Security: Server Network Security Configuration

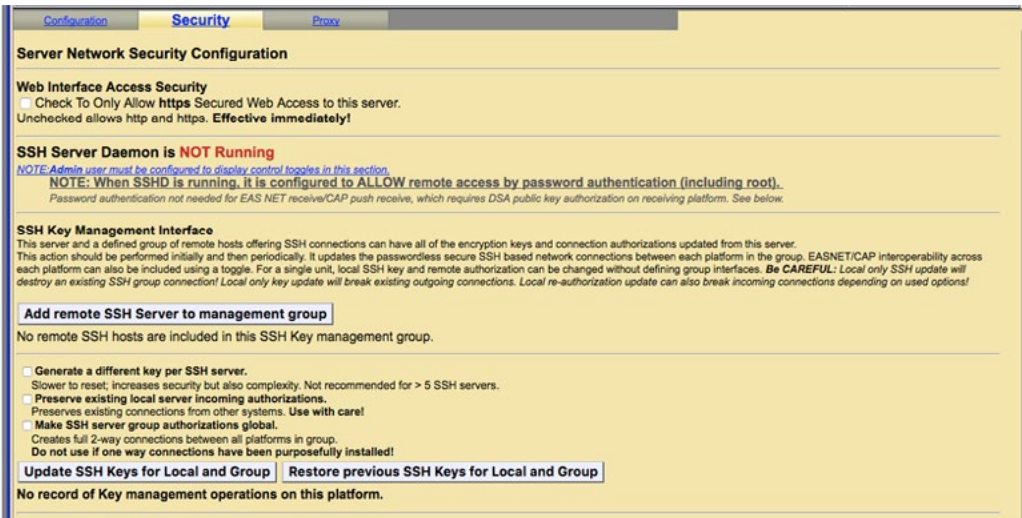
This page provides controls for managing network security. Two features are configurable for network security:

- Switching web access between secure mode (HTTPS) and regular mode (HTTP).
- Managing Secure Shell (SSH) keys across multiple platforms.



Note

A conflicting route can block network connectivity.



Server Network Security Configuration Screen

Web Interface Access Security

Use the **Web Interface Access Security** check box to force HTTPS SSL-based communication to the internal web server. The box is labeled **Check To Only Allow https Secured Web Access to this server**.

If the box is checked:

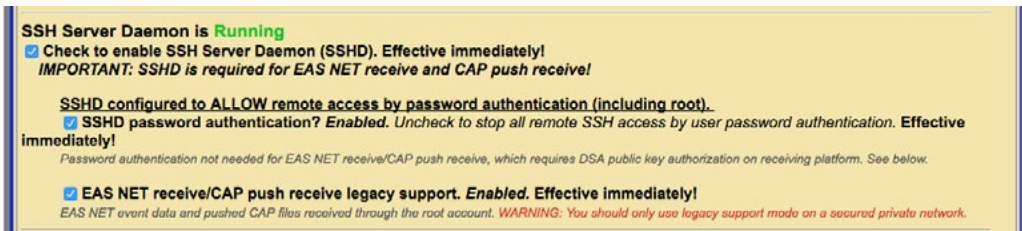
- Browser access is forced to be via HTTPS. The change is immediate.
- All communications to the server will be encrypted.

SSH Server Daemon (Status)

SSH Server Daemon provide secure encrypted communications between two untrusted hosts over an insecure network. These configuration settings are not normally displayed. Only Administration Level users may access these controls, and they must be turned on within the User Account Profile settings.

To enable the SSH Server Daemon:

1. Click the hyperlink labeled **NOTE: Admin user must be configured to display control toggles in this section** or navigate to the **Setup > Users** screen.
2. Select the desired Administration Level access user from the pull-down menu
3. Check the **Display SSH Server disable/enable controls** check box.
4. Follow the **Setup > Network > Security** page hyperlink back to the **Server Network Security Configuration** screen.



Server Network Security Configuration Screen (SSH Server Daemon Section)

The **Check to enable SSH Server Daemon (SSHD)** check box will start the SSH Sever Daemon and will change the status of this feature to **Running** from **NOT Running**, and add two additional check boxes.

The **SSHD password authentication?** check box enables remote access by password authentication. The change of this check box will go into effect immediately.

The **EAS NET receive/CAP push receive legacy support** check box should only be used across a secured private network.

SSH Key Management Interface

Secure Shell is used for EAS-Net network communication/control between an EAS device and other EAS-Net compatible platforms (including other EAS devices). SSH is a secure communications method that relies on public/private key encryption. To communicate with another platform via SSH, the public key from the EAS device public/private key pair must be authorized on the remote platform.

Authorization is usually achieved by copying the public key into a file on the remote host. The EAS device uses the open source package OpenSSH for SSH features stored in a file called *authorized_keys2* under */root/.ssh/*. Authorization allows secure access only from the holder of the public key's corresponding private key.

Even though this method of encryption and secure access is very safe, it is still a good idea to update the public/private keys periodically. To simplify this task, the SSH Key Management Interface allows a group of remote hosts offering SSH connections to have all of the encryption keys updated from the current EAS device location. This updates and maintains secure SSH-based network interoperability for EAS NET across each platform with a single operation.

To add a Remote SSH Host, click the **Add remote SSH Server to management group** button. When a descriptor is added, there is no need to confirm the addition. The screen shot below shows a single remote client descriptor. Add as many descriptors as needed. EAS NET allows up to 8 connections.



Warning

DO NOT MODIFY an SSH Keys without consulting with Digital Alert Systems/ Monroe Electronics.

SSH Key Management Interface
This server and a defined group of remote hosts offering SSH connections can have all of the encryption keys and connection authorizations updated from this server. This action should be performed initially and then periodically. It updates the passwordless secure SSH based network connections between each platform in the group. EASNET/CAP interoperability across each platform can also be included using a toggle. For a single unit, local SSH key and remote authorization can be changed without defining group interfaces. **Be CAREFUL:** Local only SSH update will destroy an existing SSH group connection! Local only key update will break existing outgoing connections. Local re-authorization update can also break incoming connections depending on used options!

Add remote SSH Server to management group

Remote SSH host 1:

Client 1	Interface Name	authorized_keys2	Incoming SSH Authorized Keys File Name
root	SSH Server User Name	id_dsa.pub	SSH DSA Public Key File Name
0.0.0.0	SSH Server Host IP Address	id_dsa	SSH DSA Private Key File Name
/root/.ssh	SSH Config Path	SSH_KEY_UPDATI	SSH Key Mgmt Status File Name

Include EASNET/CAP SSH input user account (for EASNET/CAP receive). Unchecked omits EASNET/CAP SSH input user.
EASNET/CAP SSH User Name : dasdec_netin
/etc/dasdec/netin/dasdec_netin SSH Config Path

Preserve non-group incoming authorizations on this remote server. Preserves existing connections from other systems. Use with care!

Username query: SSH User@IP Connection Test
(select test then click Run Remote Host Test to run test to SSH User@IP; no need to save changes to run test)

Run Remote Host Test

Accept changes to group interfaces

Generate a different key per SSH server.
Slower to reset, increases security but also complexity. Not recommended for > 5 SSH servers.

Preserve existing local server incoming authorizations.
Preserves existing connections from other systems. Use with care!

Make SSH server group authorizations global.
Creates full 2-way connections between all platforms in group.
Do not use if one way connections have been purposefully installed!

Update SSH Keys for Local and Group **Restore previous SSH Keys for Local and Group**

No record of Key management operations on this platform.

SSH Key Management Interface Screen

Once a remote host client descriptor interface is added, it must be configured. Default values for SSH connection to the remote host are provided (except for IP address).

1. Change the following:
 - Interface Name
 - SSH Server User Name
 - SSH Server Host IP Address
 - SSH Configuration Path (directory)
 - Incoming SSH Authorized Keys File Name
 - SSH DSA Public Key File Name
 - SSH DSA Private Key File Name
 - SSH Key Management Status File Name (if needed)
2. Click the **Accept changes to group interfaces** button for changes to effect, or click the **Cancel changes to group interfaces** button to cancel any changes.

To remove a Remote SSH Host description, click the corresponding red **Delete this SSH server interface** button and it will immediately be removed.

A useful feature of this interface is the ability to test network connections to remote SSH hosts. Use the **SSH User@IP Connection Test** pull-down menu to select the type of test. The test options are:

- **Ping Test:** Use a simple network ping to test if the base network route to a remote host exists. To test basic network connectivity, the ping test can be used without regard to the SSH field configuration. Set the IP address (numeric dot.decimal format unless DNS is enabled).
- **Uname query:** This will attempt to get the operating system name from the remote host via SSH.
- **Date query:** This will attempt to get the date and time from the remote host via SSH.
- **SCP test:** This will attempt to copy a test file to the remote host via SSH.
- **Key Mgmt Status:** This will attempt to retrieve the current state of the EAS device key management status from the remote host via SSH.
- **Get Public Key:** This will attempt to retrieve the public key from the remote host via SSH.
- **Get Authorized Public Keys:** This will attempt to retrieve the authorized public key from the remote host via SSH.

Click the **Run Remote Host Test** button and the test results will be displayed in a light green box below the button. These result might take a few seconds.

When you have all of the remote host descriptors entered properly, and you have confirmed SSH connectivity to each remote host, you may safely update the public/private keys for the entire group by clicking the **Update SSH Keys for Local and Group** button. Users may also return to the prior set of keys by clicking the **Restore previous SSH Keys for Local and Group** button.

The status of the last group management operation is printed just below the **Update SSH Keys for Local and Group** button. This gives a date and useful information about the last SSH management operation performed from this EAS device.



Note
The **Update SSH Keys for Local and Group** and **Restore previous SSH Keys for Local and Group** buttons are specific to this SSH Key Management Interface section of this screen.

The section below the SSH Management interface displays the following:

- The current SSH DSA Public Encryption Key and its installation date.
- A printout of the “authorized keys” file, which shows remote hosts authorized for SSH connections to this EAS device.

SSH Server Authorized Key Management section (green section found at the bottom of the Network screen) allows users to enable/disable specific keys, copy key data, and delete keys. This section displays Public Key file data. Each public key is displayed with an Enable check box and red Delete button.

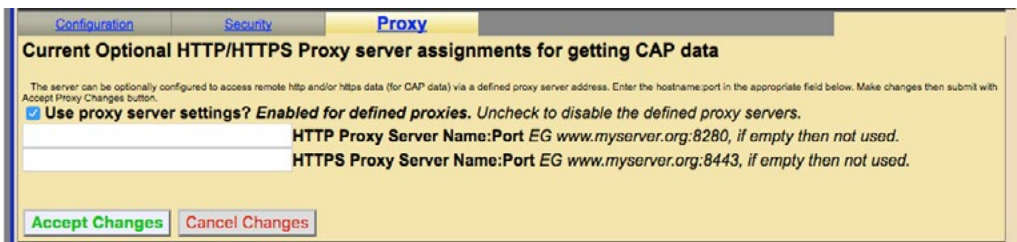
The **Enable** check box is normally checked, which enables this key for use. By unchecking this check box, that key will not be used, and communication with that device or group of devices will be discontinued. Only enabled keys are utilized.

To remove a public key, click the **Delete** button found within that key. This will remove that public key from the screen.

To accept the changes made in the SSH Server Authorized Public Keys Management section (including enabling/disabling and deleting), click the **Accept SSH Authorization** button. To cancel any changes, click the **Cancel Authorization Changes** button.

Proxy: Current Optional HTTP/HTTPS Proxy Server Assignments for Getting CAP Data

The server can be optionally configured to access remote HTTP and/or HTTPS data (for CAP data) via a defined proxy server address. This option would be enabled if defined proxy servers for CAP data acquisition are to be used.



Configuration Security **Proxy**

Current Optional HTTP/HTTPS Proxy server assignments for getting CAP data

The server can be optionally configured to access remote http and/or https data (for CAP data) via a defined proxy server address. Enter the hostname:port in the appropriate field below. Make changes then submit with Accept Proxy Changes button.

Use proxy server settings? Enabled for defined proxies. Uncheck to disable the defined proxy servers.

HTTP Proxy Server Name:Port EG www.myserver.org:8280, if empty then not used.

HTTPS Proxy Server Name:Port EG www.myserver.org:8443, if empty then not used.

Accept Changes Cancel Changes

Proxy Screen

To configure a proxy server with the EAS device:

- Check the **Use proxy server settings?** check box. Two text fields will appear: one for an HTTP proxy server, and the second for an HTTPS proxy server.
- Enter the server name into the appropriate text field. The text should be formatted as *hostname:port*.
- Click **Accept Changes** to confirm and store settings, or **Cancel Changes** to return with no changes.

TIME SETUP

The **Setup > Time** screen allows the hardware clock to be set and synchronized to an external time service. This screen is divided into sections: date and time settings, broadcast specific time settings, and Network Time Protocol Configuration.

Server Date and Time Configuration

Make changes to date and/or time and/or timezone, then press Submit button.

Date and Time **Server Timezone**

Dec 8 2018 Region : US,Canada,Mexico & C America

Mon Day Year Zone : Eastern (UTC-5/-4)

09 :52 :14

Hrs : Mins : Secs

Difference from UTC = -5.00 [Official time link](#) (if your browser has Internet access).

Sunday

Midnight

Network Time Protocol (NTP) Configuration

The OneNet™ clock can be synchronized to a remote clock using NTP. Provide a valid remote NTP server name or IP address accessible from your network. This can be another OneNet™ that has NTP enabled. If the NTP Server name is left blank, and NTP is enabled, this OneNet™ can still be used as an NTP master clock for other systems, but will simply run it's own clock.

IMPORTANT: Make sure UDP port 123 is open in any firewalls between this server and the NTP server.

NTP Server name or IP Address (restart NTP to submit changes): north-america.pool.ntp.org

Verify NTP Server during start/restart as condition for running NTP

Check this toggle to start/restart NTP. Uncheck to stop NTP. Changes are immediately effective!

NTP Server Info

```
server 216.218.254.202, port 123
stratum 1, precision -23, leap 00
refid 'CDMA' delay 0.08742, dispersion 0.00000 offset 0.009165
rootdelay 0.00000, rootdispersion 0.00104, synch dist 0.00104
reference time:   dfb6591a.eb4b562f Sat, Dec 8 2018 9:52:10.919
originate timestamp: dfb6591e.7a9ed1fb Sat, Dec 8 2018 9:52:14.478
transmit timestamp:  dfb6591e.6d131ec0 Sat, Dec 8 2018 9:52:14.426
```

[Public NTP Servers](#) (if your browser has Internet access).

Server Date and Time Configuration Screen

The Date and Time section provides three important functions. It displays the current time, provides a means to manually set the time, and establish the time zone for this EAS device.

To manually set the time:

1. Use the pull-down menus to set the month, day, year, and time zone fields.
2. Enter the desired hour (24 hour format), minute, and seconds into the appropriate text fields.
3. Click the **Submit Date/Time/Timezone Changes** button to enter the time settings.

The **Time** setup screen is static, and will not automatically refresh. The displayed time represents the last time this screen was loaded or refreshed. To update the screen's time, click the **Refresh** button located in the header section of the web interface.

A handy hyperlink is provided to display the current date and time. If the EAS device has access to the internet, click the **Official time link** hyperlink to open a separate browser tab for www.time.gov.

There are two pull-down menus below the Date and Time section that are specific to adjusting the logs to match a specific schedule. These menus are **Select start of broadcast week day** and **Select start of broadcast week hour**. They are intended to align the EAS log output files (from the EAS devices) with a station's broadcast logs. From the pull-down menus, select the desired day of the week (Sunday - Saturday) and hour of the day (Midnight - 11:00pm).

The EAS device supports Network Time protocol (NTP) to synchronize its clock to another clock over a network. This will synchronize the EAS device with an Internet-based atomic clock, another computer running NTP on a LAN, or another EAS device running as an NTP server on a LAN.



New Feature

Version 4.0 improves Time Zone support by adding a complete list of worldwide time zones.



Attention

If time zone is changed, or if the time is set forward far enough, the server software will be restarted. After clicking the **Submit Date/Time/Timezone Changes** button, all users will be logged out of the web interface, the server software will restart, and users will be presented with the login screen.

To enable the NTP feature:

1. Use the **Public NTP Servers** hyperlink (at the bottom of the screen) to find an appropriate remote NTP server.
2. Enter a name or IP address of a remote NTP server that is readily accessible from the EAS device.
3. Check the **Check this to toggle to start/restart NTP** check box.

It is recommended to check the **Verify NTP Server during start/restart as condition for running NTP** check box to ensure the NTP server connection each time the server software is loaded.

The **Check this toggle to start/restart NTP** check box must be checked to start NTP. If no NTP server name is entered and NTP is enabled, the EAS device will become an NTP server that can be pointed at from other EAS devices over the LAN.

NTP Server Info is located in a gray shaded area below the NTP settings. This is an informational display area that provides status about the NTP connection. Use this information to verify the time offset between the EAS device and the remote NTP server.

A **Public NTP Servers** hyperlink is located at the bottom of this screen. Clicking this link will open a separate web browser tab that links to the *support.ntp.org* website. This site provides in-depth information about NTP, along with a list of public NTP servers.

USERS SETUP

The **Setup > Users** screen is used to manage user accounts within the EAS device. Administrative level users have the ability to add/delete user accounts, change account passwords, and set user permission levels along with a few additional features. The Users Setup Screen is divided into two sections: **Edit Server User Account Profile** (left side) and **Add New Server User Account** (right side).

The screenshot shows the 'Users Setup' screen for an 'OneNet-1F EAS' device. The top navigation bar includes 'Send Alerts', 'Alert Events', 'System', and 'Setup'. The 'Setup' section is active, showing options for 'Server', 'Station', 'Alert Agent*', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users' (selected). The main content area is split into two columns. The left column, 'Edit Server User Account Profile', shows the 'Admin' user profile with a dropdown menu, login history, and various system settings like 'Page load indicator', 'Page Scrolling with Stationary (parked) Menu Header', 'Page Width', 'Scroll Height', 'Display decoder status on Login page', 'Display HALO Daemon disable/enable on Setup->Server->HALO page', 'Display reboot and power off buttons on Setup->Server->Main/License page', 'Display SSH Server disable/enable controls on Setup->Network->Security page', and 'Display CAP PUSH INPUT option in CAP Decoder selector on Setup->Net Alerts->CAP Decode page'. The right column, 'Add New Server User Account', has fields for 'Enter unused login name', 'View Only Level', 'Set permission level', 'Enter account comment', 'Set Password for new account', 'Enter a password (space, #, & not allowed)', 'Retype the password', 'Min 8 characters, with both letters and numbers', 'Create User', and 'Show User Permission Levels Help'. At the bottom, there is a 'Change Password' section with fields for 'Enter Current Password', 'Enter New Password (space, #, & not allowed)', and 'Re-enter New Password', along with a 'PASSWORD last modified Tue Dec 4 13:19:29 2018 EST (4 days ago)' and 'Submit Changes?' / 'Cancel Changes' buttons.

Users Setup Screen (Administration Level)



Note

The EAS device uses UDP port 123 for NTP. Check to make sure this port is open in any firewalls.



Note

User account settings within the web interface are separate from the Linux system user accounts. They do NOT control permissions to login to the base Linux system.

Each EAS device comes configured with a single Admin user account. Additional user accounts may be added and it is highly recommended to add separate user accounts for each individual accessing the EAS device with appropriate permission levels. Permission levels have been defined to meet the roles and responsibilities of personnel needing access: for example, a lead/chief engineer or EAS subject matter expert of a facility might have complete Administration Level permissions, while a master control operator might require Basic Operation Level permissions, a user with View Only Level permission would allow EAS alert activity report downloads without the risk of accidental changes to any setup settings. Differing permission levels allow appropriate access to the EAS device based on job function. The six permission levels and corresponding descriptions are found in the table below.

Permission Level	Description
Administration Level	Unlimited permissions
Operation/Control Level	Everything EXCEPT: <ul style="list-style-type: none"> • Upgrades • Software Licensing • Debug Log enable/disable • Web interface user setup/modification • Log deletion • Networked GPIO IP setup • Network setup • Network security setup • Configuration file deletion/rename
Operation Level	Everything Operation/Control can do EXCEPT: <ul style="list-style-type: none"> • Decoder channel enable/disable • Encoder required test setup • Configuration file interface • Time setup • Alert storage management setup • Networked GPIO setup
Basic Operation Level	<ul style="list-style-type: none"> • Can encode and forward alerts and run local access forwarding interface • Can terminate EAN with password re-entry • No Setup operations
EOC Operation Level	Special simplified level for Emergency Operation Centers <ul style="list-style-type: none"> • Can encode alerts • Can terminate EAN with password re-entry • No Setup operations
View Only Level	<ul style="list-style-type: none"> • Decoded, originated and forwarded alerts and status can be viewed • No Setup operations • No alerts can be originated. No manual forwarding. No cancellation



Attention

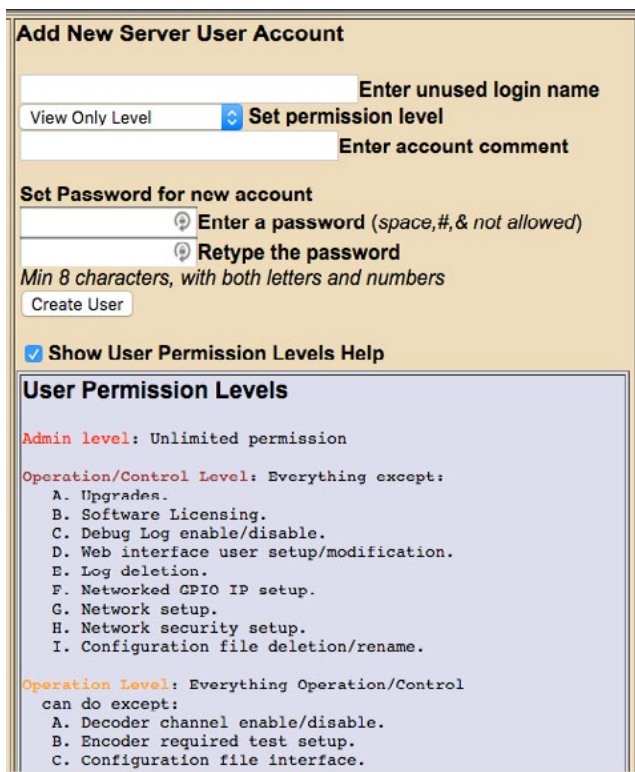
It is recommended to create individual user accounts for each staff member requiring access to the EAS device. User accounts can be configured with the appropriate permission levels for each users' roles and limiting exposure to unintended configuration changes. The EAS device logs user activity and can assist in tracking down issues if they arise.

Password Policy

Version 3.0 introduced an updated password policy for all user accounts. This password policy is designed to make EAS devices more secure and less accessible to unauthorized logins:

- Users are no longer permitted to continue using the default password (*dasdec*) after the initial login.
- Passwords must contain a minimum of 8 characters.
- Passwords must contain both letters and numbers.
- Commonly used (and blacklisted) passwords are not allowed.
 - *password*
 - *12345678*
 - *qwerty*
 - *dasdec*
 - *onenet*
- The EAS device will visually alert users with passwords older than 180 days.

The **Add New Server User Account** section is where new user accounts are created. Only Administration Level users have access to this section of the web interface to add user accounts. The following is a description of each of the settings within this section.



Add New Server User Account

Enter unused login name

View Only Level Set permission level

Enter account comment

Set Password for new account

Enter a password (space, #, & not allowed)

Retype the password

Min 8 characters, with both letters and numbers

Create User

Show User Permission Levels Help

User Permission Levels

Admin level: Unlimited permission

Operation/Control Level: Everything except:

- A. Upgrades.
- B. Software Licensing.
- C. Debug Log enable/disable.
- D. Web interface user setup/modification.
- E. Log deletion.
- F. Networked GPIO IP setup.
- G. Network setup.
- H. Network security setup.
- I. Configuration file deletion/rename.

Operation Level: Everything Operation/Control can do except:

- A. Decoder channel enable/disable.
- B. Encoder required test setup.
- C. Configuration file interface.

Add New Server User Account Section

Enter unused login name

Click in this text field to create and enter an unused (or unique) user login name. The login name may consist of up to 32 characters—including letters, numbers, and punctuation characters. The EAS device will reject attempts to enter a login name that is currently in use.

Set permission level

Click on the pull-down menu to see the six permission levels. Select the desired level by clicking on it.

Enter account comment

A simple text comment field of up to 80 characters to provide a brief description of the user. This text field is the only optional field when creating a new user account.

Set Password for new account

The password for any new account must be entered twice to insure accuracy. Please review the [new password policy](#) (above). Any proposed password not meeting this policy will be rejected (cancelling the creation of the new user account) and a brief description of the issue will be displayed just below the password text fields.

Create User

Click the **Create User** button once all the previous new user account settings have been entered. If the login name is unique and the password meets the password policies, a new user is successfully created and the web interface will display **OK: Created new user** above the **Create User** button. If any issues are found with the proposed user account credentials, the web interface will display the issue above the **Create User** button.

Show User Permission Levels Help

Check/uncheck this box to display/hide the User Permission Levels. This feature is for informational purposes and is available to all users.

The screenshot shows the 'Admin View' of the 'Edit Server User Account Profile' section. At the top, a dropdown menu shows 'Admin'. Below it, a status message indicates that the user 'Admin' is logged on since 'Sun Dec 9 23:24:14 2018' and was previously logged off 'Sun Dec 9 23:23:19 2018'. The main area contains several configuration options, many with 'Enabled' status and 'Effective immediately' notes. These include: 'Page load indicator', 'Page Scrolling with Stationary (parked) Menu Header', 'Page Width' (set to Medium 1000px), 'Scroll Height' (set to Tall 700px), 'Display decoder status on Login page', 'Display HALO Daemon disable/enable on Setup->Server->HALO page', 'Display reboot and power off buttons on Setup->Server->Main/License page', 'Display SSH Server disable/enable controls on Setup->Network->Security page', and 'Display CAP PUSH INPUT option in CAP Decoder selector on Setup->Net Alerts->CAP Decode page'. At the bottom, there is a 'Session Idle Timeout' set to 30 minutes and a 'Change Password' section with three input fields for current, new, and re-entered passwords, and a note that passwords must be at least 8 characters long.

The screenshot shows the 'User View' of the 'Edit Server User Account Profile' section. At the top, a dropdown menu shows 'BillR'. Below it, there is a checkbox for 'Allow user to change password' which is currently disabled. The 'Session Idle Timeout' is set to 'No Timeout'. There is a 'View Only Level' dropdown and a 'Permission Level' dropdown. An 'Account Comment' text field is present. The 'Change Password' section has three input fields for current, new, and re-entered passwords, with a note that passwords must be at least 8 characters long. At the bottom, there are 'Submit Changes?' and 'Cancel Changes' buttons, and a 'Delete this User?' button.



Note

The Admin User view provides more user configuration settings than when viewing other users.

Edit Server User Account Profile Section - Admin View (Left) & User View (Right)

The **Edit Server User Account Profile** section of the screen is where existing User Account profiles are updated such as: changing passwords, permission levels, account comments, session idle timeouts and allowing the user to change their own password. The following is a description of each of the settings within this section.

User Account pull-down menu

Click and select the user account from this pull-down menu. Information about the selected user's current login and last logoff is displayed just below this pull-down menu. This pull-down menu is only available to Administration Levels users.

Allow user to change password

When checked, this setting allows the user to change their own password. If unchecked, the user will need to consult with an Administration Level user to change their password. This check box is only available to Administration Levels users when viewing other users and will have an immediate effect.

Page load indicator

When checked, page load display will appear each time a modification is made to the EAS device. When submitting, applying, or accepting changes a **Loading...** graphic appears in the middle of the screen until that modification has been accepted, allowing users to understand that the EAS device is in the process of performing a function. With this feature unchecked, users will experience a delay immediately after modifications have been submitted. This setting is available to all user levels.

Page Scrolling with Stationary (parked) Menu Header

This check box keeps the header at the top of each screen and scrolls everything below the sub-tabs. This setting is available to all user levels.

Page Width

There are three page width settings for the web interface; Narrow 800 pixels, Medium 1000 pixels, and Wide 1200 pixels. Use the radio buttons to select the desired page width. Users may also make adjustments via the page width icon found in the header. This setting is available to all user levels.

Scroll Height

There are four scroll height setting for the web interface; Short 400 pixels, Medium 500 pixels, Standard 600 pixels, and Tall 700 pixels. These settings represent the height from the bottom of the header to the bottom of the web interface when the **Page Scrolling with Stationary (parked) Menu Header** feature (above) is enabled. Use these radio buttons to select the desired scroll height. This setting is available to all user levels.

Display decoder status on Login page

In some situations, it is advantageous to see the internal radio and audio decoder status along with the CAP decoder status without logging into the EAS device. This check box will display that information on the login screen. This setting is only available for Administration Level users and will apply to all login screens.

The screenshot shows the login interface for a OneNet-1F EAS device. At the top left is the Monroe Electronics logo. The main title is "OneNet-1F EAS" with "Serial: 6185" and "Platform ID: CNWD.R3HXDOTGVEJNQFMS1" below it. On the left, there are input fields for "Username" and "Password", and a blue "Sign me in" button. To the right of the login fields is a "Decoder Status" section divided into "Analog" and "Digital".

Analog	Digital
KSL 1160 AM 96% OK	PUSH INPUT Connected
NOAA 162.55 82% OK	EMNET Not enabled
KNRS 570 AM 42% OK	SKYSCRAPER Not enabled
	IPAWS CAP Connected

Copyright © 2018 Digital Alert Systems, Inc.
NOTICE: Access to this system is restricted to Authorized Users only. Unauthorized access or use of this system may constitute a violation of Federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

Login Screen with Decoder Status Display

Display HALO Daemon disable/enable

Within the Setup > Server > HALO screen there is a **Enable HALO Connection** check box. This check box enables an Administration Level user to remove this button for all users. This setting is only available for Administration Level users.

Display reboot and power off buttons

Within the Setup > Server > Main/License screen there are **Reboot Server?** and **Power Off Server?** buttons. This check box enables an Administration Level user to remove those buttons for all users. This setting is only available for Administration Level users.

Display SSH Server disable/enable controls

The SSH Server settings, located in Setup > Network > Security, are visible only after this check box is checked. This feature has no direct effect on the SSH server status. It only enables and disables the control settings for SSH. This setting is only available for Administration Level users.

Display CAP PUSH INPUT Option

Within the Setup > Net Alerts > CAP Decoder screen there is a **CAP PUSH INPUT** option in the **Select CAP Input Client** pull-down menu. This check box enables an Administration Level user to remove this selection from the menu and remove CAP PUSH INPUT decoder status from the Login page. This setting is only available for Administration Level users.

Session Idle Timeout

This pull-down menu allows users to select how much time will pass before the system auto-log offs. Be careful selecting this value. An open web interface without an operator allows anyone access. This setting is available to all user levels.

Change Password

Enter the current password, then enter the new password twice in the fields provided. Only the Admin user can change the Admin password. The Admin user and users with Administration Level permissions can change their own password and the password of other users. Users without Administration Level permissions may be allowed to change their own passwords (see **Allow users to change password** above). Information about the modification date for the password is displayed just above the Submit Changes button. After 180 days, the EAS device will recommend changing the password through a visual warning.

Submit Changes?

When clicked, this button will submit any changes. It is not necessary to use this button after selecting any of the above check boxes for their changes are immediate.

Cancel Changes

To cancel any proposed changes and refresh the screen, click the **Cancel Changes** button.

Delete this User?

This button is only shown when an Administration Level account is editing other users. Clicking this button will immediately remove the selected user account.



New Feature

Support for HALO is new in version 4.0.



New Feature

The ability to enable/disable the CAP PUSH INPUT is new in version 4.0.

Edit Server User Account Profile

BillIR

User 'BillIR' was previously logged on 'Fri Oct 28 09:55:56 2016'
 User 'BillIR' was previously logged off 'Fri Oct 28 10:06:07 2016'

Allow user to change password. Enabled. Uncheck to disable. Effective immediately.

10 Minutes **Session Idle Timeout**

Operation/Control Level **Permission Level**
 Bill Op/Control Access **Account Comment**

Override Station
 Station 1
 Station 2
 Station 3
 Station 4 **Visible Stations**

Change Password

Enter Current Password
 Enter **New Password** (space,#,& not allowed)
 Re-enter **New Password**

Min 8 characters, with both letters and numbers
 PASSWORD last modified 'Fri Oct 28 09:43:01 2016 MDT' (70 days ago)

Submit Changes? **Cancel Changes**

Edit Server User Account Profile - MultiStation Mode

MultiStation User Access

With a valid MultiStation license key, Administration level users can designate the stations a non-admin user can access. Simply login as an Admin, select the desired user account and a list of **Visible Stations** will be displayed. Click on the station(s) in the list that can be accessed by that user. Multiple stations may be selected by using either the SHIFT or ALT modifier keys while clicking the desired stations.

To create a new user account:

1. Make sure an Administration Level User is selected in the User Account pull-down menu.
2. Enter a unique name in the **Enter unused login name** field
3. Select the appropriate level from the **Set permission level** pull-down menu
4. Add any comment to the **Enter account comment** field
5. Type the desired password information into both the **Enter a password** and **Retype the password** fields
6. Click the **Create User** button.

To modify a user account:

1. Select the desired user in the **User Account** pull-down menu.
2. Make changes to any of the following:
 - **Allow user to change password** check box
 - **Session Idle Timeout** pull-down
 - **Permission level** pull-down
 - **Account Comment** text field
 - **Visible Stations** (for MultiStation users)
 - **Change Password** text fields
3. Click the **Submit Changes?** button.

To delete a user account:

1. Select the desired user in the **User Account** pull-down menu.
2. Click the **Delete this User?** button.

Notes about multiple active user sessions:

- The same user or different users can be logged in more than once and at the same time.
- A count of the number of active sessions is provided in the page header display on the right side of the User:'account name' text display. For instance, if Admin is logged on twice, the header displays User:Admin(2).



- The total number of active sessions is displayed if that number is greater than the current user sessions. For instance, if Admin is logged on twice and another user is logged on once, the header will display User:Admin(2)(3).



- Because each active session is managed separately, the page location within the Web interface can be different for the same user logged in twice.



Caution

Keep in mind that most controls and settings apply globally. If two users with edit permissions are changing the same control (for example, tuning the radio), the last one to set the value “wins.” Refreshing the displayed page will display any changes made by other logged on users.

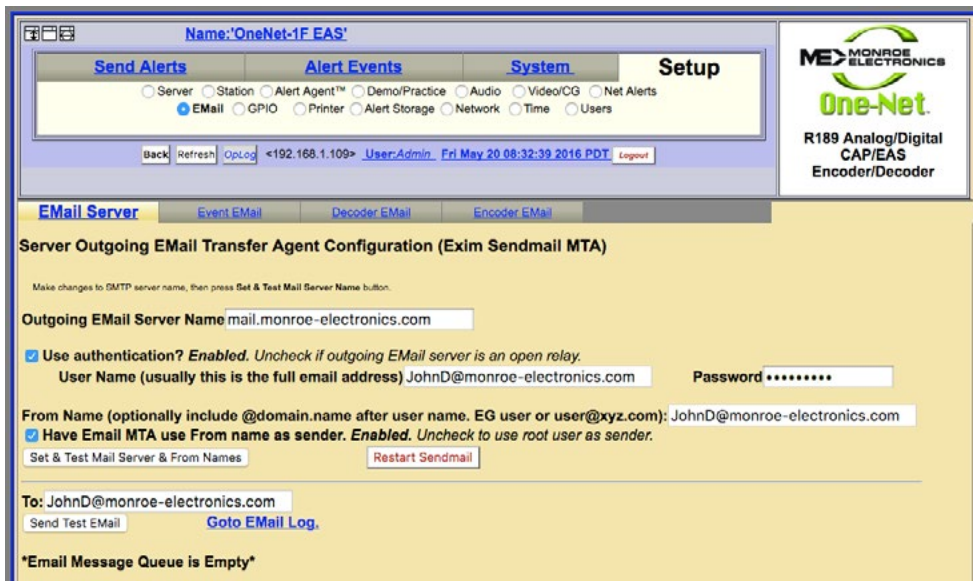
EMAIL SETUP

The EAS device can be configured to send email upon alert decoding, origination, and forwarding. Go to the **Setup > EMail** page to configure an outgoing email server and to configure the send options. There are four sub-tabs within the EMail setup section:

Sub-Tab	Description
EMail Server	Configure and test the outgoing mail settings.
Event EMail	Select which types of event and server access reports are delivered.
Decoder EMail	Select alert decoding and/or alert forwarding emails.
Encoder EMail	Select alert origination emails.

EMail Server

This sub-tab is where the outgoing mail settings are configured. Users can utilize existing e-mail account settings, or create an EAS specific account.



EMail Server Tab

To configure the outgoing email server name without using authentication (port 25):

1. Go to **Setup > EMail > EMail Server**.
2. Enter the name of outgoing mail server in the **Outgoing Email Server** text field.
3. Click the **Set & Test Mail Server & From Names** button.
4. The EAS device will attempt to contact (via a ping) this Email server.
5. If it succeeds, the message **OK:Contacted Email Server (port 25)** will display under the Outgoing EMail Server Name.

To configure the outgoing email server name using authentication (port 587):

1. Go to **Setup > EMail > EMail Server**.
2. Enter the name of outgoing mail server in the **Outgoing Email Server** text field.
3. Check the **Use authentication?** check box – the **User Name** and **Password** text fields will appear.
4. Enter the appropriate user name in the **User Name** text field – this is usually the full e-mail address.
5. Enter the appropriate password in the **Password** text field.
6. Click the **Set & Test Mail Server & From Names** button.
7. The EAS device will attempt to contact (via a ping) this Email server.
8. If it succeeds, the message **OK:Contacted Email Server (port 587)** will display under the Outgoing EMail Server Name.

Many e-mail services require a valid e-mail address in order to send e-mails. In these cases, enter the appropriate e-mail address into the **From Name** text field and check the **Have Email MTA use From name as sender** check box.

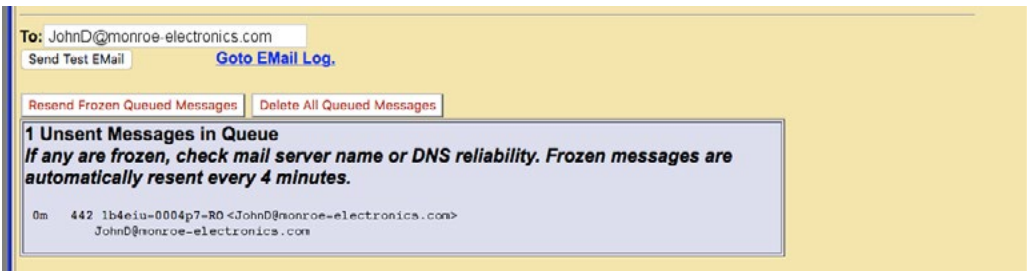
The **Restart Sendmail** button will restart the internal mail client process. It should be used if users are experiencing issues with the e-mail service on this device.



Note
Many e-mail services (such as Gmail, Yahoo, etc.) have increased their security settings. Using one of these services may require additional configuration within the settings of these services.



Note
The **Set & Test Mail Server & From Names** button does a simple ping test to make contact with the outgoing mail server. It does not verify the authentication credentials.

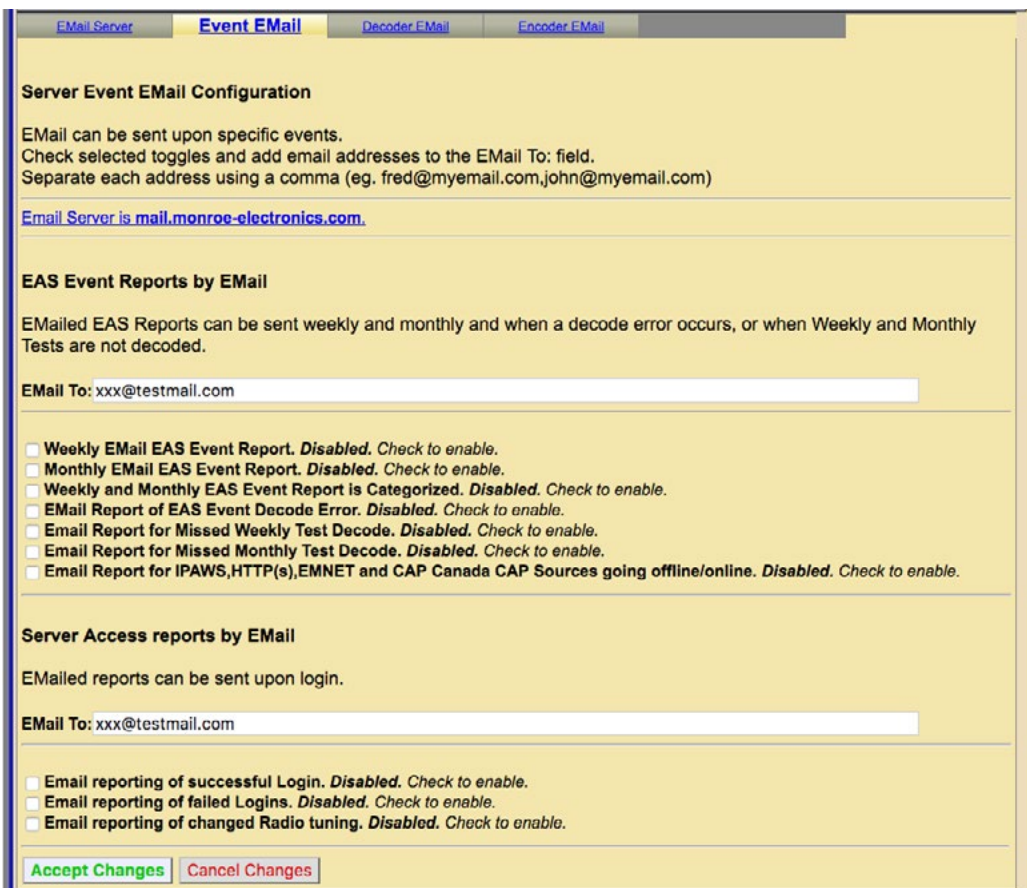


Sent Test EMail Section

To test this e-mail client is configured correctly via the chosen EMail server, type a valid Email address in the **To:** text field and click **Send Test Email**. An e-mail titled *Test Email from DASDEC* will be sent to the entered addressee. Confirmation of proper configuration is established when this e-mail is received. If the message is not received it is likely the message is frozen in the EAS device. All frozen messages are displayed below the **Send Test EMail** button. The system will attempt to resend the message every four minutes.

When there are frozen messages in the queue, two buttons will appear: **Resend Frozen Queued Messages** and **Delete All Queued Messages**. The first button will attempt to resend the frozen message, and the second will delete the messages in the frozen queue.

Event EMail



Server Event EMail Configuration Screen

The Event EMail sub-tab is broken into two functional sections: **EAS Event Reports** and **Server Access Reports**. Each of these sections begins with an **Email To:** text field. A single or multiple e-mail addresses (separated by a comma and no spaces) may be entered into these fields. Weekly e-mails are sent at the beginning of the broadcast week. Refer to the **Select start of broadcast week day** setting in the **Setup > Time** screen. Monthly e-mails are sent of the first day of each month.

EAS Event Reports by EMail

Check any of the check boxes to disable or enable e-mailing of the following weekly or monthly reports:

- Weekly EMail EAS Event Report
- Monthly EMail EAS Event Report
- Weekly and Monthly EAS Event Report is Categorized
- EMail Report of EAS Event Decode Error
- EMail Report of Missed Weekly Test Decode
- EMail Report of Missed Monthly Test Decode
- Email Report for IPAWS, HTTP(s), EMNET and CAP Canada Sources going offline/online.

Server Access Reports by EMail

Check any of the check boxes to disable or enable the immediate e-mailing of the following server access reports:

- Email reporting of successful Login
- Email reporting of failed Logins
- Email reporting of changed Radio tuning

Once the desired updates have been made to the Event EMail screen, click the **Accept Changes** button to input these settings. The **Cancel Changes** button is used to cancel any updates and refresh the screen.

Decoder EMail

To set up the outgoing email for decoder events, select **Setup > Email > Decoder EMail**.

- E-mails can be sent upon alert decoding.
- E-mails can be sent upon alert forwarding.

Check the appropriate check box and add the desired recipients' email addresses in the **EMail To:** text field. Multiple e-mail addresses may be entered by placing a comma between the addresses.

Decoder EMail Configuration.

EMail can be sent upon alert decoding and/or forwarding.
Check the appropriate toggle and add email addresses to the EMail To: field.
Separate each address using a comma (eg. fred@myemail.com,john@myemail.com)

Email Server is mail.monroe-electronics.com.

EMail upon Alert Decoding. Enabled. Uncheck to Disable EMail upon Alert Decoding.
EMail To: JohnD@monroe-electronics.com,JennyS@monroe-electronics.com,KevinR@monroe-electronics.com,SteveW@

EMail upon Alert Forwarding. Enabled. Uncheck to Disable EMail upon Alert Forwarding.
EMail To: JohnD@monroe-electronics.com,JennyS@monroe-electronics.com,KevinR@monroe-electronics.com,SteveW@

Accept Changes **Cancel Changes**

Decoder Email Configuration Screen

Once the desired updates have been made to the Decoder EMail screen, click the **Accept Changes** button to input these settings. The **Cancel Changes** button is used to cancel any updates and refresh the screen.

Encoder Email

To configure the outgoing email upon alert origination, select **Setup > Email > Encoder EMail**.



Encoder Email Configuration Screen

Check the **EMail upon Alert Origination** check box and the **EMail To:** text field will appear. Enter the desired e-mail address. Multiple e-mail addresses may be entered by placing a comma between the addresses.

Once the desired updates have been made to the Encoder EMail screen, click the **Accept Changes** button to input these settings. The **Cancel Changes** button is used to cancel any updates and refresh the screen.

AUDIO SETUP

Audio is at the heart of an EAS system. Because the EAS devices is configured ready for average field situations, the Emergency Alert System requirements in your specific area could require some special tuning:

- At a minimum, users will need to use the Setup > Audio screens to tune the Radio stations used for EAS monitoring.
- You may need to adjust the decoder input levels for the selected stations, since every station will vary in its signal strength.
- Audio output levels may need adjustment to fit with your broadcast parameters.

The following are the tabbed sub-pages on the **Setup > Audio** page:

- Decoder Audio
- Encoder Audio
- Audio Output Levels/Tests
- Radio Tuners
- Multiplayer (*with a valid MultiStation license*)

Audio Output Levels/Tests

The Direct Audio Output Levels and Tests screen is used to configure:

- Audio Output levels for device ports
- Audio Output sample rate and the audio preview devices group
 - Each audio output device results in an audio configuration interface on this page
 - Audio WAV and MP3 files can be uploaded into the EAS device from this page

All standard EAS devices come from the factory with:

- Front Panel speaker
- Main audio output device
- One auxiliary audio output device.

A labeled configuration table is provided for each one of these output devices with:

- Controls for setting output levels from 0 to 100% and for running audio tests
- Indications of whether alert origination and forwarding will use the specific audio output
- A main audio toggle control for enabling or disabling the analog audio pass-through option

Testing and Calibrating Levels

Audio tones can be played through each available audio output to test audio connections and calibrate levels using audio test equipment:

- Configure the levels by entering numbers from 0 to 100 for any specific port.
- Output level values near 70 are a good starting point.
- Each audio device displays the same style of table for the control interface.
- The table allows:
 - Mono Audio Output Level control
 - Tests (Audio)
 - > Tone Test Duration
 - > Test Audio File
 - Forwarding/Encoder Output Enable



Attention

Due to the need for immediate feedback when tuning audio, the **Setup > Audio** screens do NOT have an **Accept Changes** button. Changes to check boxes, selection boxes, and clicking buttons on these pages are immediate.



Note

Some browsers will not accept the text edit change to an audio level until the mouse is clicked outside of the field entry box. Other browsers simply will accept the change when the Enter key is touched.



Note

Setup > Audio web interface pages for Decoder and Encoder Audio display and reference audio output levels for certain features. There are numerous hyperlinks throughout and should be used to make and monitor changes to various audio settings.

Decoder Audio Encoder Audio **Audio Output Levels/Tests** Radio Tuners

Direct Audio Output Levels and Tests

This server provides audio output on an internal speaker and on sound card speaker output ports. This page allows direct setting of any output level indexed by audio device. It also provides tests of audio playback. It also provides links for resetting forwarding and encoding audio output associations. All changes effective immediately. On some browsers, hitting enter after setting the level will not result in the change being submitted. However, clicking any other button or the background will submit the changed level.

32000 Sample/sec **Audio Output Sample Rate** (Get as small as possible for your system.
All associated sound files should be set to this rate. Note: Multiplayer requires 16000. Digigram AES PCI Audio out requires 32000 or more samples/sec)

Normalize decoded EAS audio message.

80 **EAS Header/Tone/EOM Amplitude percent (25-100, dflt=80. If changed remember to rerun Init Multiplayer.)**

Front Panel Audio Output
 Main Audio Output
 Aux1 Audio Output

Audio Preview Devices

Front Panel Speaker

(Linux audio mixer device '/dev/mixer0')

Mono Audio Output Level (1..100)	Tests	Forwarding/Encoder Output Enable (Click link to edit)
70 Click Here After Level Edit	5 Tone Test Duration (1..180 Sec) <input type="button" value="Test 960 Hz Tone"/> <input type="button" value="Test 853 Hz Tone"/> <input type="button" value="Test Attention Signal"/> Test Audio File Amber_intro.wav <small>Duration: 2.064 secs Rate:32000 samples/sec Mono</small> <input type="button" value="Play"/> Listen on Browser <input type="button" value="Delete"/> <input type="button" value="Resample"/>	<input type="checkbox"/> Alert Forwarding on Front Panel Speaker Always ENABLED. <input type="checkbox"/> Alert Origination on Front Panel Speaker Always ENABLED. <input type="checkbox"/> Mute Front Panel during alert origination/forwarding.

Main Audio

(Linux audio mixer device '/dev/mixer0')

Mono Audio Output Level (1..100)	Tests	Forwarding/Encoder Output Enable (Click link to edit)
70 Click Here After Level Edit L Out (& R Out on Rev C) on	5 Tone Test Duration (1..180 Sec) <input type="button" value="Test 960 Hz Tone"/> <input type="button" value="Test 853 Hz Tone"/> <input type="button" value="Test Attention Signal"/>	<input checked="" type="checkbox"/> Main Audio Passthrough. Enabled. Internal audio output only during EAS alerts. <small>Uncheck to disable passthrough and enable full time internal audio. Effective immediately.</small>



Note
 The same **Audio Output Sample Rate** control is presented within the **Setup > Audio > Decoder Audio** (Alert Forwarding Audio Configuration section) and within the **Setup > Audio > Encoder Audio** (Alert Encoder Audio Configuration section). Changing this setting in one location will change it in all locations. The sample rate applies to audio for both alert Forwarding and Origination. AES Audio requires 32000 or more samples per second.

Direct Audio Output Level and Tests Screen

Audio Output Sample Rate

Controls the sample rate of audio played from the EAS device. The default sample rate is 16000 samples/second.

- For a EAS devices with AES digital audio output, this rate needs to be set at 32000 or higher samples/second.

Normalize decoded EAS audio message

Checking this box will automatically manage the audio output levels. It is recommended to disable this feature when setting and testing levels.

EAS Header/Tone/EOM Amplitude percent

Sets the loudness of the EAS Header, the Attention Tone, and the End of Message Tone. The default value is 80.

Audio Preview Devices

Shows all of the available audio outputs. Select one or more to create the Audio Preview device group. Some EAS device web interface screens support an audio preview button Play > Preview that will run audio file play-out. To select multiple audio outputs, hold the Control key while clicking to select.

Front Panel Speaker

Allows for editing the volume of the front panel speaker as well as playing test tones and WAV files. This speaker is controlled by the Linux audio mixer device '/dev/mixer0'.

Mono Audio Output Level

Sets the volume from 0 (mute) and 100 (full volume). Enter the desired value in the text field. For the setting to become effective, click on the label 'Click Here After Level Edit'

Audio Tests

There are several audio test options:

- Play a standard test tone (960 or 853 Hz tone or the EAS Test Attention Signal) for the time entered the Tone Test Duration (1 to 180 seconds) field
- Play an uploaded audio WAV file from the Test Audio File pull-down menu
 - Selected files display:
 - › Duration of the audio file in seconds (directly under pull-down menu)
 - › Sample rate in sample/sec (directly under pull-down menu)
 - › Mono or stereo audio (directly under the pull-down menu)
 - › A Play button to play on the front panel speaker
 - › A Listen in Browser hyperlink to save and/or play the file on the browser host computer
 - › A Delete button to delete the selected test audio file
 - › A Resample button resamples the uploaded audio files to match the Audio Output Sample Rate at the top of the screen. This will keep a consistent sample rate throughout an EAS alert.

Forwarding/Encoder Output Enable

Both Alert Forwarding and Origination audio are always enabled (played) on the Front Panel Speaker. There is no link to edit in this section for the Front Panel Speaker.

The screenshot displays two audio control panels. The top panel, 'Main Audio', is for the Linux audio mixer device '/dev/mixer0'. It features a 'Mono Audio Output Level' slider set to 70, with a 'Click Here After Level Edit' button. Below this is a 'Tests' section with a 'Tone Test Duration' of 5 seconds and buttons for 'Test 960 Hz Tone', 'Test 853 Hz Tone', and 'Test Attention Signal'. A 'Test Audio File' section shows a dropdown menu with 'Canadian_Alerting_Attention_Signal_(8sec).wav' selected, along with 'Play', 'Listen on Browser', 'Delete', and 'Resample' buttons. On the right, 'Forwarding/Encoder Output Enable' is set to 'ENABLED', with sub-sections for 'Alert Forwarding on Main Audio' and 'Alert Origination on Main Audio', both also 'ENABLED'. The bottom panel, 'Aux 1 Audio', is for the Linux audio mixer device '/dev/mixer2'. It has 'Left' and 'Right' audio output levels both set to 75, with a 'Click Here After Level Edit' button. It shares the same 'Tests' and 'Test Audio File' sections as the Main Audio panel. Its 'Forwarding/Encoder Output Enable' is 'DISABLED', with 'Alert Forwarding on Aux 1 Audio' and 'Alert Origination on Aux 1 Audio' also 'DISABLED'. A 'PCM Limit (70-100)' section is present at the bottom left of the Aux 1 Audio panel, with a value of 90 and a note: 'Larger=>Louder. Recommended value 88-90.'

Direct Audio Output Levels & Tests (Main & Aux 1 Audio Sections)

Main Audio and Aux Audio Tables

The interface tables for Main and Auxiliary (Aux 1 and Aux 2) audio operate like the Front Panel Speaker table described above, with some key differences:

- Auxiliary Audio is optional and thus may not appear
- It is possible to have two auxiliary audio interface tables
- Auxiliary Audio provides stereo output volume level control

Forwarding / Encoder Output Enable & Main Audio / Passthrough Audio

The Main Audio table has a special check box that controls the state of the Main analog audio pass-through circuit. This circuit controls analog audio input/output pass-through on the screw terminal connector on the back of the EAS device. Pass-through audio allows external balanced audio to be passed through the EAS device and interrupted during an EAS audio activation.

- If the Main audio output is to be tested by playing a file or a tone, or if pass-through audio is not needed, the Main Analog Audio Passthrough check box should be disabled. This will enable full time output of internal audio.
- Otherwise, check to enable analog audio pass-through. When Pass-through is Enabled, the only time EAS device generated audio is played on the Main audio output port is during an EAS alert.

Tests:

- To test the Main and/or Auxiliary Audio outputs, attach speakers to the EAS device audio output ports.
- Run the various tone test buttons.

Tests allow the EAS device to play each of the two single tones that comprise the dual-tone EAS Attention Signal.

Alert Forwarding and Alert Origination

The Main and Auxiliary Audio tables display an active hyperlink showing whether the forwarded and originated alert audio is output on the audio device.

To make changes to these states:

- Click the hyperlink to jump to the correct Decoder Audio or Encoder Audio setup page.
- Modify the associated check boxes.



Direct Audio Output Levels & Tests (Upload Audio .WAV Section)

Upload Audio .WAV file

The interface at the bottom of this screen allows .WAV and MP3 files to be uploaded into the EAS device.

- Click the Browse button to locate the file on the computer
- Click the Upload .WAV file button. MP3 files are converted automatically into a WAV files.

Uploaded audio files are available for tests as well as for encoding and manual forwarding.



Note

The EAS Attention signal and WAV files can be played as described above for the front panel speaker interface table.

Radio Tuners

Several EAS device models include internal radio receivers. These radios can be configured, tuned, and monitored using the **Setup > Audio > Radio Tuners** screen.

Each radio is tuned/configured via the web interface to any AM, FM, or NOAA frequency.

The screenshot displays the 'Radio Configuration' screen with three radio tuner settings:

- Radio 1:** FM selected, 104.3 MHz FM (87.9 - 107.9), Level: STRONG (69%).
- Radio 2:** FM selected, 107.9 MHz FM (87.9 - 107.9), Level: MODERATE (61%).
- Radio 3:** FM selected, 107.1 MHz FM (87.9 - 107.9), Level: No Audio Detected (14%).

Each radio configuration includes a frequency tuning interface with 'Accept Typed Frequency Change' and 'Cancel Typed Frequency' buttons, and a list of audio sources: Front Panel Speaker, Main Audio, and Aux 1 Audio. Stream URLs for MP3 and OGG/Vorbis are also provided.

Radio Configuration Screen

For a radio to be utilized by a decoder channel, the decoder must be set to the internal audio source that indicates a radio is available (go to **Setup > Audio > Decoder Audio**).

The chosen radio frequency settings are automatically recalled at boot time following a software restart.

A numeric level indicator displays the strength of reception:

- FM, AM and NOAA band selection occurs immediately.
- NOAA frequency selection occurs immediately upon button selection.
- All AM and FM frequency must be submitted using the **Accept Typed Frequency Change** button.

As a convenience, the decoder channel associated with each radio tuner is displayed in an active hyperlink. This can be clicked to immediately go to the **Setup > Audio > Decoder Audio** page.

After tuning and verifying reception, check the input levels on the **Setup Audio >**



Note

External antennas are usually required for proper radio reception. Antennas are connected to a coax connector on the back of the EAS device. Antennas can be purchased through third party vendors. For recommendations, contact Digital Alert Systems/ Monroe Electronics.



Note

It is important to tune the radios to stations that carry EAS alerts. This is a fundamental part of properly setting up the EAS device. Consult your states' EAS plan for the monitoring assignments in your area.



Caution

Do not leave the monitor on during normal operations. Radio monitoring is intended for configuration purposes and can interfere with EAS specific processes.

Decoder Audio page and make sure they are rated as OK (or occasionally Elevated).

It is IMPORTANT to verify radio reception and decoder input levels after tuning. Radio reception can be monitored using the provided **Listen on:** buttons for each radio. When you select one of the speakers listed, audio from the associated decoder for the radio will play out of the chosen output. To stop the audio play-out, click on the Turn Radio Monitoring Off button that will be displayed above the radio tuning sections. Radio frequencies can be tuned while listening.

Decoder Audio

The Decoder Audio page has three areas to configure:

- Alert Decoding Audio Configuration
- Decoder Audio Monitoring Configuration
- Alert Forwarding Audio Configuration
- ALSA Sound System (Administration Level users only)

Each EAS decoder channel can be independently tuned for input sensitivity and can be enabled and disabled. Decoder input can also be heard using the audio monitoring controls on this page. The audio output devices used during alert forwarding are also configured from this screen.

Main and Auxiliary Audio Decoder Configuration

Each analog sound card (Main, Auxiliary) has its own decoder status and configuration display table.

Soundcard name and associated Linux mixer device

The name of the sound card and its associated Linux mixer device name are shown above the display table.

Audio Input Source: Internal/Radio or Line-In Jack

To the right of the sound card name are radio buttons that indicate the analog audio input source for the sound card: Internal Radio or Line-In Jack. Typically, this will be set to the Internal/Radio setting for the Main Audio device. To connect external radio receivers, use the Line-In Jack setting on the appropriate sound card device.

If Internal/Radio is selected, a link to the **Setup > Audio > Radio Tuners** page is provided in the first column on the display table as a convenience.

Several EAS device models include up to three internal radio receivers.

- Two are connected to the main audio device
- The third is connected through the Audio Input Source “Internal A” connection
- A fourth audio source, from the back panel screw connector terminal, is also routed through this input channel

When a new input source is established, refresh this page a few times to insure a consistent level quality of OK. **This page redisplay more slowly than most other web interface screens, so be patient when you access or refresh this page.**

Soundcard decoder pair display table

Each table provides names and controls for two decoders to be selectively enabled and disabled and for decoder input levels to be set. Typically, all decoders can be enabled. The EAS device supports two EAS decoders per stereo line input channel. This results in each sound card device providing two decoders, one on the left channel and one on



Note

The Decoder Audio Monitoring interface provided on the **Setup > Audio > Decoder Audio** screen may also be used to listen to radios. It is less convenient than using the buttons provided on the Radio Tuners screen. It is necessary to use the Decoder Audio Monitoring interface to listen to the fourth decoder input or to listen to decoders five and six on units that provide two extra decoders.



Note

The AES digital audio card does NOT support EAS decoding. Each table has a radio button selector for the Audio Input Source. Each soundcard supports two (2) decoder channels. Decoders can be selectively enabled/disabled and the input levels can be set. The interface is described below.



Note

The input source selection switch is VERY important since it controls the origin of the audio input stream used as the EAS audio source.

the right channel (L1 and R1). Each decoder is displayed in a separate row in the sound card status table. Each row has four columns to review and configure.

Decoder Audio Encoder Audio Audio Output Levels/Tests Radio Tuners

Alert Decoding Audio Configuration

The One-Net provides two EAS decoders per stereo line input channel. Each soundcard thus provides two decoders, one on the left channel and one on the right channel. This page allows decoders to be selectively enabled and disabled, allows decoder input levels to be set, allows decoder audio buffer snapshots to be saved to disk, and allows audio monitoring of a single decoder input. **Decoding is sensitive to input levels.** The quality of the input level is rated in real time per decoder. With every page refresh the quality is displayed to allow correct level setting. When an input source is established, refresh this page a few times to insure a consistent level quality of OK. Decoder EAS Auto-scale adds automatic boost of input signal when an EAS header is detected. This is only useful when incoming EAS audio is at unacceptably lower levels than program audio. This page also allows selection of the sound card speaker output ports used during alert forwarding. Changes are updated immediately. On some browsers, hitting enter after setting the level will not result in the change being submitted. However, clicking any other button or the background will submit the changed level.

Main Audio (/dev/mixer0) Audio Input Source Internal/Radio Line-In Jack

Decoder Name, Label and Info	Audio Input Level (1..100)	Audio Level Status	Decoder Enable
L1 KSL-AM : Radio 1	Left Level 55	OK Snapshot	<input checked="" type="checkbox"/> Left Channel EAS Decoder. ENABLED. Uncheck to disable. None <input type="button" value="Autoscale Options"/>
R1 NOAA : Radio 2	Right Level 32	LOW Snapshot	<input checked="" type="checkbox"/> Right Channel EAS Decoder. ENABLED. Uncheck to disable. None <input type="button" value="Autoscale Options"/>

KSL-AM(L1) snapshot (Mon Mar 28 11:03:19 2016): [L1_snapshot.wav](#)
 KSL-AM(L1) Last Post Decoded Alert Snapshot (Thu May 19 16:31:38 2016): [L1_post_alert_snapshot.wav](#)
 Prev:1. [Wed May 18 03:09:27 2016](#) 2. [Wed May 18 03:07:07 2016](#) 3. [Fri May 6 15:15:37 2016](#)
 NOAA(R1) snapshot (Fri Jul 11 08:47:03 2014): [R1_snapshot.wav](#)
 NOAA(R1) Last Post Decoded Alert Snapshot (Sat May 14 07:50:10 2016): [R1_post_alert_snapshot.wav](#)
 Prev:1. [Sat May 14 07:47:50 2016](#) 2. [Wed Mar 16 10:08:54 2016](#) 3. [Wed Mar 9 13:51:53 2016](#)

Auxiliary Audio 1 (/dev/mixer2) Audio Input Source Internal A Internal B Line-In Jack

Decoder Name, Label and Info	Audio Input Level (1..100)	Audio Level Status	Decoder Enable
L2 : Radio 3	Left Level 55	N/A	<input type="checkbox"/> Left Channel EAS Decoder. DISABLED. Check to enable.
R2 : Rear Connector	Right Level 75	ZERO Snapshot	<input checked="" type="checkbox"/> Right Channel EAS Decoder. ENABLED. Uncheck to disable. None <input type="button" value="Autoscale Options"/>

L2 snapshot (Fri Jul 11 09:42:33 2014): [L2_snapshot.wav](#)
 L2 Last Post Decoded Alert Snapshot (Mon Jul 14 08:42:06 2014): [L2_post_alert_snapshot.wav](#)
 Prev:1. [Mon Jul 14 08:38:23 2014](#) 2. [Mon Jul 14 08:35:49 2014](#) 3. [Mon Jul 14 08:26:59 2014](#)
 R2 Last Post Decoded Alert Snapshot (Tue Dec 8 09:03:02 2015): [R2_post_alert_snapshot.wav](#)
 Prev:1. [Tue Dec 8 08:39:40 2015](#) 2. [Tue Dec 8 07:39:02 2015](#) 3. [Mon Jul 14 08:42:06 2014](#)

Decoded Alert Auto-Snapshot. **Enabled.** Uncheck to Disable Decoded Alert Auto-Snapshot

Alert Decoding Audio Configuration Screen

The audio soundcard table columns are:

Decoder Name, Label and Info

- The decoder base name, automatically set by the server, provides an identification tag for the decoder
- This input text field provides a description of the decoder channel that will be used throughout the interface.
- If the Audio Input Source is set to Radio, a link to the Setup > Audio > Radio Tuners page is displayed as a convenience.

Audio Input Level (1..100)

- Change the input level as needed until the Audio Level Status is OK (green) or occasionally Elevated (yellow)

Audio Level Status

- EAS decoding is sensitive to audio input levels
- The quality of the input level is constantly being rated in real time per decoder. Input level status is automatically rated by:
 - Zero (red)
 - Low (red)
 - OK (green)

- Elevated (yellow)
- High (red)
- Use the Refresh button in the header of the page to make multiple checks of the Audio Level Status quality. This will assist in setting the correct level setting.

Snapshot

Each decoder is also given a Snapshot button. When clicked, a WAV file of the corresponding decoder audio input buffer is saved, dated, and displayed as a web link accessible via this web page.

- The file is named based on the decoder channel name
- It can be downloaded via the provided web link

In the screen shot, four snapshot files are shown:

- KSL-AM(L1) snapshot (Mon Mar 28 11:03:19 2016): L1_snapshot.wav***
- KSL-AM(L1) Last Post Decoded Alert Snapshot (Thu May 19 17:31:38 2016): L1_post_alert_snapshot.wav***
Prev:1. Wed May 18 18:03:09:27 2016 2. Wed May 18 03:07:07 2016 3. Fri May 6 15:15:37 2016
- NOAA(R1) snapshot (Fri Jul 11 09:47:03 2014): R1_snapshot.wav***
- NOAA(R1) Last Post Decoded Alert Snapshot (Sat May 14 08:50:10 2016): R1_post_alert_snapshot.wav***
Prev:1.Sat May 14 08:47:50 2016 2.Wed Mar 16 11:08:54 2016 3.Wed Mar 9 14:51:53 2016

Items a & c were generated by the **Snapshot** button and items b & d were Post Decoded Alert Snapshots and were generated automatically after decoding finished. See the **Decoded Alert Auto-Snapshot** check box below.

Decoder Enable

- A check box to enable/disable a decoder
- An Autoscale Options pull-down menu

Autoscale Options

An EAS Autoscale is a method to automatically increase the input gain level when EAS alert data is detected. This can result in decoding alerts that have low audio levels from the source. The following are options in this pull-down menu:

- None
- FFT Filter
- Amplification

Decoded Alert Auto-Snapshot

This check box enables/disables the Decoded Alert Auto-Snapshot. The default value is enabled (checked) and should usually remain this way. This feature allows for:

- A snapshot WAV file being generated after an alert is decoded or after a decode error is detected
- Detailed troubleshooting in the case where an incoming EAS audio has resulted in decoder errors.

Careful analysis of the post-alert snapshot audio can pinpoint the nature and source of upstream EAS errors.



Attention

A decoder must be enabled to decode incoming EAS alert audio.

Decoder Audio Monitoring Configuration

Two interfaces in this section for users to select the desired audio source and select the appropriate monitor output to hear the audio from.

- The **Select Decoder Audio to Monitor** list shows all the available decoder audio channels
- The **Decoder Audio Monitor Output** list allows a specific output port to be selected

Decoder Audio Monitoring Configuration

You can listen to any one of the server decoder input channels. Choose a decoder channel to monitor, and then choose an output device. The selection is effective immediately. **DO NOT LEAVE THE MONITOR ON DURING NORMAL OPERATION.** [Audio monitoring can also be controlled from the Radio Tuners page.](#)

Select Decoder Audio to Monitor	Decoder Audio Monitor Output
None	Main Audio
KSL-AM(L1)-Main, Radio 1	Aux 1 Audio
NOAA(R1)-Main, Radio 2	MP3 Stream http://192.168.1.15:8000/dasdec_mon.mp3
R2-Aux 1, Rear Connector	OGG/Vorbis Stream http://192.168.1.15:8000/dasdec_mon.ogg
	None

Front Panel Speaker Audible Decode. Disabled. Check to Enable Audible Decoding on Front Panel Speaker

Decoder Audio Monitoring Configuration Section

To operate:

- Select a decoder channel to monitor
- Select one of the following monitor outputs:
 - Front Panel Speaker
 - Main Audio output
 - Aux1 Audio output
 - MP3 Stream (for monitoring from web interface)
 - OGG/Vorbis Stream (for monitoring from web interface)

The MP3 and OGG/Vorbis Stream monitor outputs allow users to monitor the audio as a stream from a local host computer. This is useful for checking the decoder input when the EAS device is monitored in an office apart from the equipment room. The host computer's web browser will need a streaming audio player that can support either OGG/Vorbis audio format or MP3.

Listening to the decoder input is a VERY IMPORTANT part of configuring for EAS reception. Make sure that these tools are used after radio tuning in order to verify audible reception.

Front Panel Speaker Audible Decode

When enabled, audio for an incoming, decoding alert is played on the front speaker. This check box defaults to disabled.



Note

The selections occur immediately and will cause a page refresh. When audio monitoring is enabled, a red ****ON**** label will be displayed to the left side of the interfaces. To disable audio monitoring, select the None decoder option and/or the None output option.



Caution

Do not leave the monitor on during normal operations. Radio monitoring is intended for configuration purposes and can interfere with EAS specific processes.



Note

The radios may alternatively be monitored within the **Setup > Audio > Radio Tuners** screen. See the [Radio Tuners section](#) of this manual for a complete description of the radio monitoring interface.

Alert Forwarding Audio Configuration

This server can be configured to send the audio output during alert forwarding to selected sound card speaker output ports. This page allows enabling/disabling of these output ports as well as links for setting output levels. NOTE: Forwarding and encoding share the same output ports; level changes for one applies to the other. Changes take effect immediately.

32000 Sample/sec **Audio Output Sample Rate** (Set as small as possible for your system.
All associated sound files should be set to this rate. Note: Multiplayer requires 10000. Digigram AES PCI Audio out requires 32000 or more samples/sec)

Normalize decoded EAS audio message.

Main Audio (Linux audio mixer device '/dev/mixer0')

Mono Audio Output Level (1..100) (Click link to edit)	Forwarding Output Enable
70	<input checked="" type="checkbox"/> Decoder Alert Forwarding on Main Audio Output. Enabled. Uncheck to disable.

Main Audio passthrough Enabled. Internal balanced audio output is switched on by EAS alert.

Aux 1 Audio (Linux audio mixer device '/dev/mixer2')

Audio Output Level (1..100) (Click link to edit)	Forwarding Output Enable
Left: 75, Right: 75	<input checked="" type="checkbox"/> Decoder Alert Forwarding on Aux 1 Audio Output. Enabled. Uncheck to disable.

Alert audio delay. Enabled. Alert audio playback is delayed by a specified number of seconds. This allows a time delay after closing the EAS broadcast relay in order to compensate for transmitter latency. Uncheck to disable alert audio playback delay period. Applies to both origination and forwarding. 6 Seconds of Delay
 For Audio Loop control go to Setup->Video/CG->Video Out

ALSA Sound System Active

Alert Forwarding Audio Configuration Section

Alert Forwarding Audio Configuration

Audio Output Sample Rate

This selector controls the sample rate of audio played from the EAS device.

Normalize decoded EAS audio message

Checking this box will automatically manage the audio output levels. It is recommended to disable this feature when setting levels.

Audio Forwarding Tables

After the EAS device decodes an EAS alert, it can be triggered to “Forward” the alert. The audio component of forwarding is the action of playing the alert audio over selected audio outputs.

- The Main Audio device is always present on an EAS device.
- Auxiliary Audio outputs are present if an appropriate sound card has been installed.
 - Most EAS devices have an Aux 1 sound device. Use the check box under the column Forwarding Output Enable to set the Main station audio port forwarding.

Audio Output Level

This displays the current Audio Output Level as set in the **Audio Output Levels/Tests** sub-tab. Clicking on the hyperlinked number provides a shortcut to the **Setup > Audio > Audio Output Levels/Tests** screen to change the output levels.

Forwarding Output Enable

Each audio device has an interface for enabling/disabling **station** audio forwarding on the device. Each table provides a check box to control whether the **Main station** forwarded audio is played using the output device. Typically, these should all be enabled.



Note
 The same **Audio Output Sample Rate** control can also be found in the **Setup > Audio > Audio Output Levels/Tests** (Direct Audio Output Levels and Tests section) and **Setup > Audio > Encoder Audio** (Alert Encoder Audio Configuration section). Changing the setting in one location will change it in all locations. The sample rate applies to audio for both alert Forwarding and Origination. AES Audio requires 32000 or more samples per second.



Attention
 Forwarding and encoding share the same physical output ports; audio level changes for one applies to the other.



Note
 When the EAS devices’ MultiStation Mode is enabled, the audio forwarding configuration for each **station** overrides the settings on these tables! Configure station alert audio forwarding on the proper station interface configuration page under **Setup > Station**.

Alert Audio Delay

Used to control a delay period before the playout of alert audio, after the EAS Audio playout relay is closed. When enabled, a numeric text field is provided for entering a user specified number of seconds of delay.

ALSA Sound System Active

If the EAS device is experiencing issues with the input or output sound, click the **Run/Restart ALSA Sound System?** button. This will restart this process without restarting the EAS device.

Encoder Audio

There are two main configuration options for encoder audio:

- Alert Encoding Audio Configuration
- Alert Audio File Recording.

Alert Encoding Audio Configuration

When the EAS device is used to originate an EAS alert (or encode an alert), the audio associated with the alert must be played from an output port in order for the alert to be transmitted or decoded by another decoder. The audio for the alert must be configured to play over a selected audio output.

This interface allows for:

- Setting audio sample rate
- Enabling/disabling Originating audio on each of the audio output devices
- Setting a play-out delay time

Alert Encoding Audio Configuration

This server can be configured to send the audio output from the encoder to selected sound card speaker output ports. This page allows enabling/disabling of these output ports as well as links for setting output levels. NOTE: Forwarding and encoding share the same output ports; level changes for one applies to the other. This page also provides for selecting the audio device used for audio recording.

All changes on this page take effect immediately. On some browsers, hitting enter after setting the Mic Level will fail; on all browsers you can always click on the provided label next to the Mic level after editing to set the change.

32000 Sample/sec **Audio Output Sample Rate** (Set as small as possible for your system.)
All associated sound files should be set to this rate. Note: Multiplexer requires 16000. Digigram AES PCI Audio out requires 32000 or more samples/sec

Main Audio (Linux audio mixer device '/dev/mixer0')

Mono Audio Output Level (1..100) (Click link to edit)	Encoder Output Enable
70 This output is L Out on the rear panel audio connector block.	Main Audio passthrough Enabled. Internal balanced audio output is switched on by EAS alert. <input checked="" type="checkbox"/> Encoder Alert Origination on Main Audio Output. Enabled. Uncheck to disable.

Aux 1 Audio (Linux audio mixer device '/dev/mixer2')

Audio Output Level (1..100) (Click link to edit)	Encoder Output Enable
Left 75 Right 75	<input checked="" type="checkbox"/> Encoder Alert Origination on Aux 1 Audio Output. Enabled. Uncheck to disable.

Alert audio delay. Disabled. Check to enable alert audio playout delay period. This can compensate for loss of audio due to streamer/transmitter latency. Applies to both origination and forwarding.
For Audio Loop control go to Setup->Video/CG->Video Out

Select audio device for alert audio file recording :

Main Audio (/dev/mixer0) Auxiliary Audio 1 (/dev/mixer2)

Input Source Microphone Input Line Input Left
Record Input Level (click here to activate changed value) 100

Alert Encoding Audio Configuration Screen



Note

This same control is presented within the **Setup > Audio > Encoder Audio** screen. This delay setting applies to both alert Forwarding and Origination.



Note

The same **Audio Output Sample Rate** control is presented within the **Setup > Audio > Audio Output Levels/Tests** (Direct Audio Output Levels and Tests section) and within the **Setup > Audio > Decoder Audio** (Alert Forwarding Audio Configuration section). Changing this setting in one location will change it in all locations. The sample rate applies to audio for both alert Forwarding and Origination. AES Audio requires 32000 or more samples per second.

Audio Output Sample Rate

This selector controls the sample rate of audio played from the EAS device.

Main Audio and Auxiliary Audio Tables

These tables allow for examining audio output status and enabling/disabling playing Main station Originated alert audio on the individual audio output devices.

- The Main Audio device is always present on an EAS device.
- Auxiliary Audio outputs are present if an appropriate sound card has been installed.
 - Most EAS devices have an Aux 1 sound device.

The table has two columns:

- Audio Output Level
- Encoder Output Enable

Audio Output Level

The audio output levels are displayed and provide an active shortcut link to the Audio Output Levels/Tests page for changing the output levels.

Encoder Output Enable

Each table provides a check box for controlling if the Main station originated alert audio is played using the output. Typically, these should be enabled.

Alert Audio Delay

This check box allows for delaying the play-out of alert audio for a user-specified number of seconds after the EAS Audio play-out relay is closed.

Select audio device for alert audio file recording

The EAS devices' encoder provides an interface to record audio into WAV files.

- This interface is available under the Encoder > Send EAS > General EAS web page
- These files can be used for the voice audio portion of an EAS alert
- There are options for selecting which audio device and input source (microphone or line input) is used for the recording

Sound card source

The standard EAS device provides one Auxiliary Audio card in addition to the Main Audio card.

- When more than one sound card device is present, a radio button selection option for the recording sound card will be displayed. Select the card to use as the recording source.

Input Source

Once the source sound card is selected, set the **Input Source** by choosing one of the following:

- Microphone Input
- Line Input Left

The selection is determined by the actual source from which you will record.

Record Input Level

Use the Input Level control to set the level for the recording input gain level. Enter a value from 0 - 100 in the Record Input Level field. After you set the value, you must click on the text '**click here to activate changed value**'.



Attention

Forwarding and encoding share the same physical output ports; audio level changes for one applies to the other.



Note

When the EAS devices' MultiStation Mode is enabled, the audio forwarding configuration for each **station** overrides the settings on these tables! Configure station alert audio forwarding on the proper station interface configuration page under **Setup > Station**.



Note

This same control is presented within the **Setup > Audio > Decoder Audio** screen. This delay setting applies to both alert Forwarding and Origination.



Note

During recording, the decoders on the selected audio card source are disabled.

VIDEO/CG SETUP

Select **Setup > Video/CG** to access the screen for controlling operation of external and internal character generation.

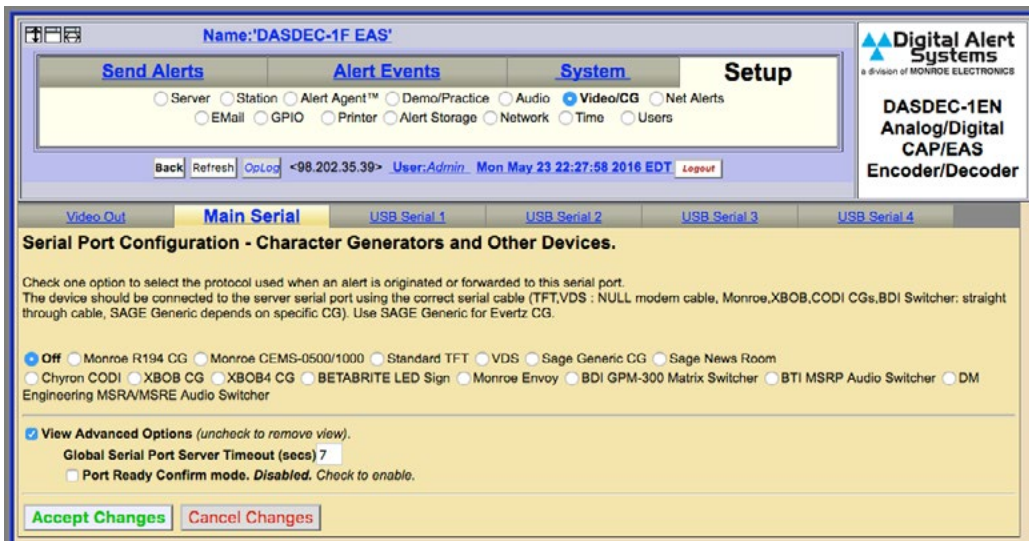
The screenshot shows the 'Setup' page for 'Name: DASDEC-1F EAS'. The 'Video/CG' option is selected under the 'System' tab. The page is divided into three main sections:

- Serial Port Configuration - Character Generators and Other Devices:** This section allows selecting a protocol for alert origination. Options include Off, Monroe R194 CG, Monroe CEMS-0500/1000, Standard TFT, VDS, Sage Generic CG, Sage News Room, XBOB CG, XBOB4 CG, BETABRITE LED Sign, Monroe Envoy, and DM Engineering MSRA/MSRE Audio Switcher. A 'View Advanced Options' checkbox is checked, revealing a 'Global Serial Port Server Timeout (secs)' field set to 7 and a 'Port Ready Confirm mode' checkbox which is disabled.
- Video Output Configuration:** This section describes the internal CG's ability to generate NTSC video output. The 'Internal CG full page video output' checkbox is checked and labeled as 'Enabled'. Below it, there are dropdown menus for 'Video page duration in seconds for multiple page displays' (set to 5), 'Video page color' (set to Red outline around Dark Blue-Violet), 'Video page font size' (set to 26), and 'Video page font name' (set to Luxi Serif Mono Bold). There is also an 'Optional custom text for first line of page' field which is currently empty. A 'Set override alert page title' checkbox is disabled. There are buttons for 'Show Color Bars', 'Show Date/Time', 'Show Character Set', 'Clear', and 'Release Video'. The 'Linux command prompt on video output' checkbox is checked and labeled as 'Enabled'. The 'Serial controlled video duration' checkbox is disabled.
- Video Duration Control:** This section has three radio button options: 'Video Duration=Full Alert Duration' (disabled), 'Video Duration=Alert Audio Duration' (selected), and 'Video Duration=Custom Duration' (disabled). Below this is a 'Mins:Secs' field set to 0:0. A note at the bottom states: 'To setup alert audio repeat loop during video display, set total video duration to at least 1 minute or to full alert duration.'

At the bottom of the page are 'Accept Changes' and 'Cancel Changes' buttons.

Video/CG Configuration Screen

The main Video/CG screen consists of the serial port configuration for an external character generator (CG) and configuration of the internal character generator in support of the video output. The basic settings enable the control of a single serial port (COM1) in addition to the internal CG settings.



Video/CG Configuration Screen (Broadcast Mode)

In Broadcast mode (with a valid Plus Package License Key), there are six sub-tabs within the Video/CG Setup:

- Video Out
- Main Serial
- USB Serial 1 through 4 for up to four expansion USB serial ports

Broadcast mode EAS devices support up to five (5) simultaneous serial ports (one main RS232 port on the back panel (COM1), and 1 to 4 expansion RS232 ports provided via a USB port expander), each running a different character generator protocol.

Main Serial

The **Main Serial** sub-tab screen has three sections:

- Serial Port Character Generator Configuration
- Character Generator Attribute Settings
- FIPS Group and EAS Codes Group filter configuration

Serial Port Character Generator Configuration

The radio selection buttons show the Character Generator (CG) used when a decoded alert is forwarded or encoded (or no CG). Here is a list of supported character generator protocols:

- Monroe R194 CG
- Monroe CEMS-0500/1000
- Standard TFT
- VDS
- Sage Generic CG
- Sage News Room
- Chyron CODI
- Decade Engineering XBOB
- Decade Engineering XBOB-4
- BetaBrite LED sign
- Monroe Envoy
- BDI GPM-300 Matrix Switcher
- BTI MSRP Audio Switcher
- DM Engineering MSRA/MSRE Audio Switcher



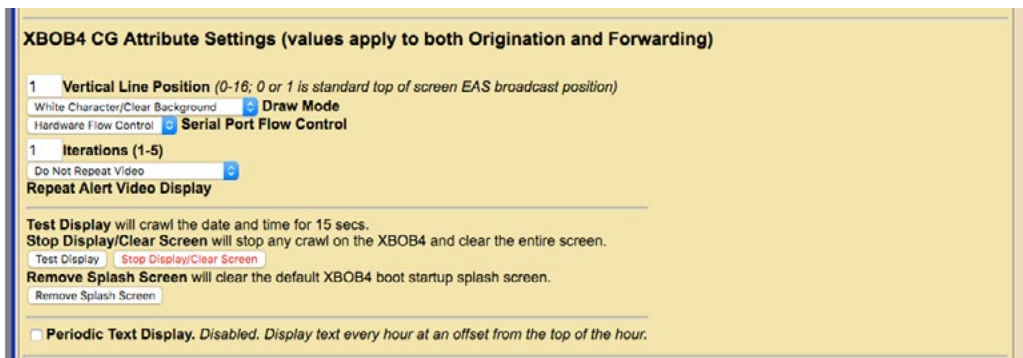
Note
Many EAS device models can also optionally provide native analog NTSC composite video output. Video/CG behavior is configured only on this page and applies to both Decoder Alert Forwarding and Encoder Alert Origination.



Note
The **Accept Changes** button at the bottom of each screen is required to submit any modifications.

Of these, the Monroe CEMS-0500/1000, VDS 840, and Decade Engineering XBOB require a TV Features license key. The Chyron CODI interface requires both a TV Features and a Plus Package license key.

- Choose the appropriate protocol for the connected serial device and check that option.
- The CG should be connected to the server serial port (on the back panel) using the correct serial cable (TFT, CODI, VDS use NULL modem cable, Monroe CGs use straight through cable, SAGE Generic depends on specific CG, usually a straight through cable).
- Use SAGE Generic for Evertz MediaKeyer and Logo Inserters as well as for Miranda Imagestore CGs. Most of the character generator protocols present some further configuration options. Some, like Chyron CODI and VDS840 present direct control of alert repetition, font colors, number of crawl loops, etc.
- Experiment with these settings to get the desired behavior. The CODI protocol also presents options for generating test patterns. Most CG's also can be configured to run repetitions of the video output during an alert.



XBOB-4 CG Attribute Settings Section

CG Attribute Settings

The options displayed here depends on the selected CG protocol.

- The screenshot shows the Decade Engineering XBOB-4 CG is selected. A user would choose the correct settings for:
 - Vertical Line Position
 - Draw Mode
 - Serial Port Flow Control
 - Iterations

There are also **Test Display**, **Stop Display/Clear Screen**, and **Remove Splash Screen** buttons. This interface includes a **Periodic Text Display** check box.

FIPS and EAS Codes properties configuration. Only originated or forwarded alerts with matching FIPS and EAS codes will activate this serial device.

FIPS Group *Erie, NY (036029)* **EAS Group** *AVW : AVALANCHE WARNING*
 Western NY *Genesee, NY (036037)* NY State Codes *BZW : BLIZZARD WARNING*
Livingston, NY *CAE : CHILD ABDUCTION EMERGENCY*
(036051) *CDW : CIVIL DANGER WARNING*
 7 locations 21 codes

Source alert FCC EAS Station IDs Activation criteria string
(only use to screen specific incoming alert station IDs; up to 8 character each, separate each source EAS station ID with a | char; eg. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2). The * character matches all FCC EAS Station IDs.

All EAS Station IDs Activate this port.

Do not use GPI triggers GPI Properties Configuration - Optionally designate GPI inputs/states required to use this interface.

View Advanced Options (unchecked to remove view).
 Global Serial Port Server Timeout (secs) 7
 Port Ready Confirm mode. Disabled. Check to enable.

Accept Changes **Cancel Changes**

FIPS and EAS Codes Properties Configuration Section

FIPS and EAS Codes filter configuration

Use this section to edit activating FIPS Groups and EAS Code Groups.

Select a FIPS Group from the pull-down menu. A gray box will appear to the right of the pull-down menu with a list of all the FIPS Codes within that group. This list represents the geographic areas that will activate this serial port. Follow the FIPS Group hyperlink to the **Setup > Alert Agent™ > FIPS Groups** sub-tab to manage (add, delete, & edit) the FIPS Groups lists.

Select an EAS Group from the pull-down menu. A gray box will appear to the right of the pull-down menu with a list of EAS Codes within that group. This list represents the EAS Codes that will activate this serial port. Follow the EAS Group hyperlink to the **Setup > Alert Agent™ > EAS Code Groups** sub-tab to manage the EAS Code Group lists.

Source alert FCC EAS Station IDs

This is additional filter criteria for activation of this serial port. Enter the desired Station ID or Station ID's (separated by a '|') into this text field. This serial port will not activate without matching this station ID(s). By using the wildcard character '*', all station ID's will activate this serial port.

GPI Properties Configuration

A pull-down menu is provided to select a specific GPI's state (open or closed) during an alert. These input GPI states will help determine the operation of a specific serial port. Once a selection has been made within this pull-down menu, all the available GPIs are listed below the pull-down menu.

View Advanced Options

This check box exposes two additional settings:

- Global Serial Port Server Timeout (sec)
- Port Ready Confirm mode

Remember to click the **Accept Changes** button to apply any changes. Or use the **Cancel Changes** button to cancel and refresh the screen.

USB Serial 1 through 4

The USB Serial sub-tabs have the same organization as the Main Serial port screen and operate in the same way. Each page corresponds to a different physical serial port.



Note

If activating FIPS Groups and/or EAS Groups are configured, then the serial port CG will only be activated during alert origination or forwarding when the alert contains at least one of the FIPS Group codes and matches at least one of the EAS Group codes.



Caution

The criteria entered in the FIPS and EAS Codes section of this web interface establish the operation of a specific serial port. In most cases this filtering is not necessary. Make sure any input to these fields is well thought out.



Note

The creation of and management of FIPS and EAS Code Groups is found in the Alert Agent Setup section of this chapter. Use these links to learn more about [FIPS Groups](#) and [EAS Code Groups](#).

These ports are supported using a USB to 4 Port RS232 Adapter. Other adapters may work, but they must be based on the FTDI chipset.

- Make sure that the proper cable is used for the external CG hardware.

The USB serial ports offer a slightly different list of CG's as compared to the Main serial port.

- Monroe R194 CG
- Monroe CEMS-0500/1000
- Standard TFT
- Sage Generic CG
- Sage News Room
- Chyron CODI
- Decade Engineering XBOB
- Decade Engineering XBOB-4
- VDS
- BetaBrite LED sign
- BDI GPM-300 Matrix Switcher
- BTI MSRP Audio Switcher
- DM Engineering MSRA/MSRE Audio Switcher

As with the Main serial port, a status box is also displayed above the CG radio button selector to indicate the status of the specific USB serial port.

Serial port protocols

The supported protocols and their options are listed below:

1. Monroe R194 CG Attribute Settings

The following attributes are available:

Iterations (1-5)

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once
- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down option, the **Set Alert Video Repetition Period** settings will appear. Input the desired numeric time values - in minutes and seconds. 2 minutes is the minimum value.

Test Display

Click this button to test the interface with the R194 CG. The test consists of crawling the date and time for about 15 seconds.

Stop Display

Click this button to stop the Test Display.

Periodic Text Display

These settings are not directly related to EAS operations and are intended to produce periodic displays with the R194 CG. Station ID's and other static information can be displayed on an hourly basis. The following settings will appear:

Text

Enter the static text to be used during the Periodic Text Display.

Clock Offset

A positive or negative offset before/after the top of the hour with a range of -29 to 30 minutes.

Duration

Enter the duration of the Periodic Text Display. Values from 5 to 45 seconds may be entered.

Test Periodic Text Display

Click the **Test Periodic Text Display** button to test the established settings.

2. Monroe CEMS 500/1000 CG Attribute Settings

Repeat Alert Video Display – Defaults to Do Not Repeat

Select from a set of options for repeating the data write to the remote device after a pause period set from the **Set Alert Video Repetition Period** field. The repeat period has to be at least 2 minutes.

3. Standard TFT Attribute Settings

This is available on all serial ports, however, the first port (starting with Main and ending with USB 4) using TFT standard controls audio play-out.

TFT emulation mode: EAS ORG code is untranslated

When disabled, the ORG code "EAS" is translated in the alert translation text. Enable to emulate the TFT behavior of not translating ORG code "EAS".

TFT Pre-Alert Notification mode

When disabled, EAS Alerts are exclusively played under TFT client control. When enabled, notifies and gives alert command access to TFT client prior to independent alert play-out. If this option is enabled then another check box is presented:

TFT Pre-Alert Notification omit audio play-out

Check to play audio if TFT client requests EAS alert audio play-out. If disabled, the audio requests will be immediately answered without audio play-out.

TFT client relay command emulation

When disabled, the standard EAS Audio relays are used. When enabled, requests by the TFT client for relays will be mapped to the GPIO output relays.

Max Delay before forced play-out – Defaults to 13 minutes

Set this value in minutes: seconds from 2 minutes, 10 seconds up to a maximum of 13 minutes. This is the maximum time that can elapse after a successful EAS ready to play notification to a remote TFT protocol device before the EAS audio will be force played.

Pre/Post Alert Audio extension – Defaults to disabled

When enabled, TFT client audio play commands will use pre and post alert audio if they are defined.

In No-Audio mode, hold EOM for audio duration – *Defaults to disabled*

Option is typically used when using a MultiPlayer or another TFT interface is the master. When enabled, TFT client audio play commands will use pre and post alert audio if they are defined.

Additional EOM hold delay

This option becomes visible when the above **In No-Audio mode** is enabled.

Serial Port Flow Control

Select Hardware or Software or None depending upon the hardware support on the remote device. Available options include:

- No Flow Control
- Software Flow Control
- Hardware Flow Control

4. Sage Generic CG Attribute Settings

Serial Port Baud Rate – *Defaults to 9600*

Select 9600 or 19200 baud depending on the remote device requirements.

Serial Port Flow Control

Select **Hardware**, **Software** or **No Flow Control** depending upon the hardware support on the remote device.

Max text length - *Defaults to 2000*

Maximum number of characters sent to the connected CG. Evertz has a maximum number of 2,047 characters.

Throttle down serial port write speed – *Defaults to disabled*

When Enabled, data is written with pauses between 128 byte blocks. This can be helpful when sending this to devices that cannot do flow control.

Iterations – *Defaults to one. Crawl is done once*

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once
- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down option, the **Set Alert Video Repetition Period** settings will appear. Input the desired numeric time values - in minutes and seconds. 2 minutes is the minimum value.

5. Sage News Room Attribute Settings

Check to run immediate upon matching decoded alert – *Defaults to disabled*

When enabled, data for matching FIPS and EAS filtered alerts is sent to the remote device using the Sage News Room protocol.

Serial Port Baud Rate – *Defaults to 9600.*

Select 9600 or 19200 baud depending on the remote device requirements.

Serial Port Flow Control

Select **Hardware**, **Software** or **No Flow Control** depending upon the hardware support on the remote device.

Max text length - *Defaults to 4000*

Maximum number of characters sent to the connected device.

Throttle down serial port write speed – *Defaults to disabled*

When Enabled, data is written with pauses between 128 byte blocks. This can be helpful when sending this to devices that cannot do flow control.

6. Chyron CODI CG Attribute Settings

Vertical Position

Set from video scanline 10 (top most) to 440 (bottom).

Font - *Defaults to one*

Set from 1 to 8.

Color – *Defaults to white*

- White
- Blue
- Yellow
- Red
- Magenta
- Cyan
- Green
- Black

Crawl Background - *Defaults to no background banner*

- No background banner
- On (method 1: def banner only)
- On (method 2: vid, banner, vid)

Speed

- 120 Pix/Sec NTSC
- 360 Pix/Sec NTSC
- 600 Pix/Sec NTSC
- 840 Pix/Sec NTSC
- 1080 Pix/Sec NTSC
- 240 Pix/Sec NTSC
- 480 Pix/Sec NTSC
- 720 Pix/Sec NTSC
- 900 Pix/Sec NTSC
- 1200 Pix/Sec NTSC

CODI Serial Port Baud Rate – *Defaults to 9600*

Select 9600 or 19200 baud depending on the remote device requirements.

Text over Video Antialiased – *default enabled*

When enabled, the text is anti-aliases over the video background.

Video Blanking control

May be required for backgrounds on Analog CODI.

When Checked, clears CODI screen prior to message crawl

When enabled, the screen is fully cleared of graphics prior to the EAS text crawl.

When checked, delays CODI message crawl until after EAS audio header & attention

When enabled, the crawl is delayed until after the EAS audio header and attention two-tone signal is played.

Iterations – *Defaults to one. Crawl is done once*

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once
- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down option, the **Set Alert Video Repetition Period** settings will appear. Input the desired numeric time values - in minutes and seconds. 2 minutes is the minimum value.

CODI Test Patterns, Screen Clear, and Reset

Set Test Pattern

Select a test pattern by entering a numeric value between 1 and 22

Display Selected Test Pattern

Click the **Display Selected Test Pattern** button to display the (above) selected test pattern.

Clear CODI Display

Clicking the **Clear CODI Display** button will clear the CODI video output. This is useful after displaying a test pattern.

Reset CODI

Clicking this button will reset the CODI CG.

7. XBOB CG Attribute Settings

Vertical position – *Defaults to one*

Sets the vertical location of the crawl on the screen from 0 (topmost) to 16 (bottom)

Solid black background – *Defaults to enabled*

When Enabled, the crawl text is set to display on top of a black banner.

Iterations – *Defaults to one. Crawl is done once*

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once
- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down option, the **Set Alert Video Repetition Period** settings will appear. Input the desired numeric time values - in minutes and seconds. 2 minutes is the minimum value.

8. XBOB4 CG

Vertical Line position – *Defaults to one*

Sets the vertical location of the crawl on the screen from 0 (topmost) to 16 (bottom)

Draw Mode

Controls the appearance of the crawl displayed on the screen. Choose between the following:

- White Character/Clear Background
- White Character / Black Background
- White Character / Half-tone Background
- Black Character / White background.

Serial Point Flow Control

Select Hardware or Software or None depending upon the hardware support on the remote device.

Iterations – *Defaults to one. Crawl is done once*

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display – *Defaults to Do Not Repeat*

Select from a set of options for repeating the data write to the remote device after a pause period set from the **Set Alert Video Repetition Period** field. The repeat period has to be at least 2 minutes.

Test Display

Click this button to test the interface with the XBOB4 CG.

Stop Display/Clear Screen

Click this button to stop the Test Display and clear the video output.

Remove Splash Screen

Will clear the default XBOB4 boot startup splash screen.

Periodic Text Display

These settings are not directly related to EAS operations and are intended produce periodic displays. Station ID's and other static information can be displayed on an hourly basis. The following settings will appear:

Text

Enter the static text to be used during the Periodic Text Display.

Draw Mode

Controls the appearance of the crawl displayed on the screen. Choose one of the four available modes. (see Draw Mode above)

Display Mode

Choose between **Crawl** or **Do Not Crawl**

Clock Offset

A positive or negative offset before/after the top of the hour with a range of -29 to 30 minutes.

Duration

Enter the duration of the Periodic Text Display. Values from 5 to 45 seconds may be entered.

Test Periodic Text Display

Click the **Test Periodic Text Display** button to test the established settings.

9. VDS CG Attribute Settings

Select VDS Mode

- Standard VDS840
- StarMU/Star 8
- Sage VDS840 Emulation
- Sage VDS830 Emulation
- VDS830

Serial Port Bit Config

- 8 data, 1 stop bit
- 8 data, 2 stop bit
- 7 data, StarMU/Star 8

Serial Port Flow

- No Flow Control
- Software Flow Control
- Hardware Flow Control

VDS Serial Port Baud Rate – Defaults to 9600

Select 9600 or 19200 baud depending on the remote device requirements.

Vertical position – Defaults to video 20

Set from 20 (top most) to 208 (bottom).

Speed – Defaults to Med

- Slow
- Medium
- Fast

Crawl Font – Defaults to one

Set from 1 to 4.

Char Color – Defaults to white

- | | |
|-------------------------|------------------|
| - Clear, key over video | - White |
| - Yellow | - Bright Cyan |
| - Bright Green | - Bright Magenta |
| - Bright Red | - Bright Blue |
| - Gray | - Dull Yellow |
| - Cyan | - Green |
| - Magenta | - Red |
| - Blue | - Black |

Set Color Background by EAS Severity? – Defaults to disabled.

When enabled, the text color is determined based on a color selection set for the EAS severity category. Select the desired color for each severity level.

Delay VDS message crawl – Defaults to disabled

When enabled, the crawl is delayed until after the EAS audio header and attention two-tone signal is played.

Iterations – Defaults to one. Crawl is done once

This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once

- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down option, the **Set Alert Video Repetition Period** settings will appear. Input the desired numeric time values - in minutes and seconds. 2 minutes is the minimum value.

10. BetaBrite LED Sign Attribute Settings

Check to display immediately upon matching decoded alert

When enabled, matching FIPS and EAS filtered alerts are crawled on the BetaBrite LED display upon decoding. When disabled, matching FIPS and EAS filtered alerts are displayed upon origination and forwarding play-out. Use this feature as a way to post a visual notification that an alert has been decoded.

Stop decoded alert display upon Acknowledgement event

Becomes visible when the **Check to display immediately matching decoded alert** check box is enabled. Clicking this check box will cause the BetaBrite display to clear after the pending alert message is acknowledged.

Max text length – *Default to 4000*

Controls the maximum number of characters sent to the BetaBright LED Sign.

Display Duration Control

The duration of the BetaBrite crawl is set by selecting one of three Display Duration Control radio button options. The duration can be set to the full alert duration, to the alert audio duration, or to a custom duration. The first two options apply to Originated and Forwarded alerts while the third (Custom Duration) option applies to Decoded alerts.

- Full Alert Duration
- Alert Audio Duration
- Custom Duration (displays duration settings in Minutes and Seconds)

Test Display

Click this button to test the interface with the BetaBright. The test consists of crawling the date and time for about 30 seconds.

Stop Display

Click this button to stop any crawl on the BetaBright.

11. BDI GPM-300 Matrix Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

12. BTI MSRP Audio Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

13. DM Engineering MSRA/MSRE Audio Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

FIPS and EAS Codes properties configuration

Each of the Serial interface screens contain filtering for both FIPS and EAS codes along with Station ID filtering. Functionally, this means these serial devices can be selectively configured to activate during specific EAS alert, locations and/or origination Station ID's. When selecting "All Locations" from the FIPS Group or "All" from the EAS Group pull-down menus, no filtering will take place.

FIPS and EAS Codes filter configuration

Use this section to edit activating FIPS Groups and EAS Code Groups.

Select a FIPS Group from the pull-down menu. A gray box will appear to the right of the pull-down menu with a list of all the FIPS Codes within that group. This list represents the geographic areas that will activate this serial port. Follow the FIPS Group hyperlink to the **Setup > Alert Agent™ > FIPS Groups** sub-tab to manage (add, delete, & edit) the FIPS Groups lists.

Select an EAS Group from the pull-down menu. A gray box will appear to the right of the pull-down menu with a list of EAS Codes within that group. This list represents the EAS Codes that will activate this serial port. Follow the EAS Group hyperlink to the **Setup > Alert Agent™ > EAS Code Groups** sub-tab to manage the EAS Code Group lists.

Source alert FCC EAS Station IDs

This is additional filter criteria for activation of this serial port. Enter the desired Station ID or Station ID's (separated by a '|') into this text field. This serial port will not activate without matching this station ID(s). By using the wildcard character '*', all station ID's will activate this serial port.

GPI Properties Configuration

A pull-down menu is provided to select a specific GPI's state (open or closed) during an alert. These input GPI states will help determine the operation of a specific serial port. Once a selection has been made within this pull-down menu, all the available GPIs are listed below the pull-down menu.

View Advanced Options

This check box exposes two additional settings:

- Global Serial Port Server Timeout (sec)
- Port Ready Confirm mode

Remember to click the **Accept Changes** button to apply any changes. Or use the **Cancel Changes** button to cancel and refresh the screen.

Video Out

The Video Output Configuration sub-tab has three check boxes:

- Internal CG full page video output
- Linux command prompt on video output
- Serial controlled video duration

The EAS device can generate video output for originated and forwarded alerts. When video output is generated, a set of details pages will be played out of the BNC video output port.

Click **Accept Changes** to apply changes to this page.

Video Out Main Serial USB Serial 1 USB Serial 2 USB Serial 3 USB Serial 4

Video Output Configuration.

This DASDEC-1EN servers internal CG can generate NTSC video output for originated and forwarded alerts.

Internal CG full page video output. Enabled. Uncheck to disable.
Page duration for multi-page display is a fixed number of seconds ▾
5 Video page duration in seconds for multiple page displays.
Red outline around Dark Blue-Violet ▾ Video page color
26 ▾ Video page font size
Luxi Serif Mono Bold ▾ Video page font name
Optional custom text for first line of page
 Set override alert page title. Disabled. Check to override the default alert page titles.
Show Color Bars Show Date/Time Show Character Set Clear Release Video

Generate MPEG-DASH alert. Enabled.
manifest.mpd Manifest file name
32 H.264 Compression Quality 0-51 (0:no compression, 51:max compression; default=32)
Main ▾ H.264 Profile Value (default=Main)
31 ▾ H.264 Main Level Value (default=31)
128k Video Bitrate (as 32k to 256k; default=128k)
32k Audio Bitrate (as 16k to 256k; default=32k)
1 Video Representation ID (default=1; must be different from Audio ID)
2 Audio Representation ID (default=2; must be different from Video ID)
8 Segment Duration Seconds (2 to 32 secs; default=8)
30 ▾ Frames per second (default=30)

Linux command prompt on video output. Enabled. Causes four second delay of alert video. Uncheck to disable.
 Serial controlled video duration. Disabled. Alert details video is ended based on the "Video Duration Control" selections below. Check to enable serial control for ending alert video.
Video Duration Control Video Duration=Full Alert Duration Video Duration=Alert Audio Duration Video Duration=Custom Duration

0 : 0 Optional Duration Extension Time (mins:secs). Extends Video Alert Duration up to 1 hr
Mins:Secs
To setup alert audio repeat loop during video display, set total video duration to at least 1 minute or to full alert duration.

Accept Changes Cancel Changes

Video Out Screen

Internal CG full page video output

Use the check box to enable or disable the **Main station** Video Output if licensed and the hardware support is enabled. The EAS device can provide a full screen NTSC analog video display of the current originated or forwarded alert.

Page Duration pull-down

The **Page Duration** has two settings available in this pull-down menu:

- Page duration for multi-page display is a fixed number of second
- Page duration is Video Duration/Number of Pages



Note

In current software, running the NTSC video details generator will slow down the start of every alert by a few seconds as the video system is initialized from a VGA console state to a video output state. Depending on the required timing of your on-air system, this can be objectionable. Only enable NTSC video details output if it is needed.



Note

When MultiStation mode is enabled, the Video Output toggle for each **station** overrides this **Main station** setting check box! Configure per station alert Video Output on the proper station interface configuration page under **Setup > Decoder > Forwarding**.

Video Page Color pull-down

The following color selections are available within this pull-down:

- Red outline around Dark Blue-Violet
- Red
- Dark Red
- Orange
- Blue
- Dark Blue-Violet
- Black

Video page font size pull-down

This pull-down menu sets the font size for the video page output. Available sizes range from 16 to 34.

Video page font name pull-down

This pull-down menu sets the font type for the video page output. There are 14 available fonts with a mix of serif, san serif, bold, italic, and narrow.

Optional custom text for first line of page

The text entered into this field will be displayed as the first line of each page of the alert.

Set override alert page title

Video Display Buttons:

These are a series of five buttons used to test the output of the video card:

Show Color Bars – Displays NTSC color bars

Show Date/Time – Displays the current date and time

Show Character Set – Displays a set of characters based on the configured font, size and color.

Clear – Clears the current video output screen to black. Useful when clearing the screen from the previous test buttons.

Release Video – Releases the VGA output from displaying video and returns the VGA screen to the Linux command prompt.

Video Duration Control

Full Alert Duration

Optional Duration Extension

Generate MPEG-DASH alert

A valid MPEG-DASH license key is required for this feature. When enabled, this feature will create MPEG-DASH content of EAS alerts. The following settings are made visible when this feature is enabled:

Manifest file name

Enter the desired name of the manifest (.mpd) file. Make sure to include the .mpd file extension in the file name.

H.264 Compression Quality – Default to 32

This value determines the amount of compression within the H.264 stream. The value of '0' is no compression and the value of 51 is max compression.

H.264 Profile Value – Default to Main

Choose between **Baseline**, **Main** and **High** profiles from this pull-down menu.

H.264 Main Level Value – Default to 31

Choose between the value of 31 or 40 from this pull-down menu.

Video Bitrate – Default to 128k

Enter a Video Bitrate value between 32k to 256k.

Audio Bitrate – Default to 32k

Enter a Video Bitrate value between 16k to 256k.

Video Representation ID – Default to 1

Enter the Representation ID for the video. Must be different from the Audio Representation ID.

Audio Representation ID – Default to 2

Enter the Representation ID for the audio. Must be different from the Video Representation ID.

Segment Duration Seconds – Default to 8

Input the Segment Duration Seconds in the provide text box. Value should be between 2 and 32.

Frames per Second – Default to 30

Choose between **24**, **29.97** and **30** frames per second from this pull-down menu.

Linux command prompt on video output

Forces the video output to display the command line prompt. Enabling this option will cause a four second delay in the alert video.

Serial controlled video duration

This setting is either enabled or disabled by checking/unchecking the check box.

- When enabled, the screen states, '**Alert details video is ended when serial protocol controlled EOM audio finishes. Uncheck for other video control options.**'
- When disabled, as shown in the above screen shot, the message changes to 'Alert details video is ended based on the '**Video Duration Control selections below.**' and displays the following settings:

Video Duration Control: Select which of the three radio buttons is needed for Video Duration Control:

- Video Duration=Full Alert Duration
- Video Duration=Alert Audio Duration
- Video Duration=Custom Duration

Custom Duration allows for setting the exact video duration in minutes and seconds, up to one extra hour. One use for this option is to provide for a minimum video duration on short Weekly Test alerts.

Optional Duration Extension Time

These text fields allow users to extend the video alert duration up to 1 hour.

ALERT AGENT™ SETUP

Alert Agent™ is a unique and powerful feature for the DASDEC/One-Net - giving users better control and functionality when configuring the EAS device and managing EAS alerts. The Alert Agent™ radio button includes the following sub-tabs:

Sub-Tab	Description
Alert Policies	Configure the decoder alert language, duplicate EAS handling, update policy for active EAS alerts and pending alert acknowledgment.
Manage Alert Nodes	Create, edit, test and delete Alert Nodes.
Local Access Forwarding	Create custom text for Civil Emergency Messages.
Custom Msg Forwarding	Configure custom message forwarding
FIPS Groups	Create, edit, manage, and delete FIPS Location Groups along with encoder FIPS locations.
EAS Code Groups	Create, edit, manage, and delete EAS Code Groups along with encoder EAS codes.

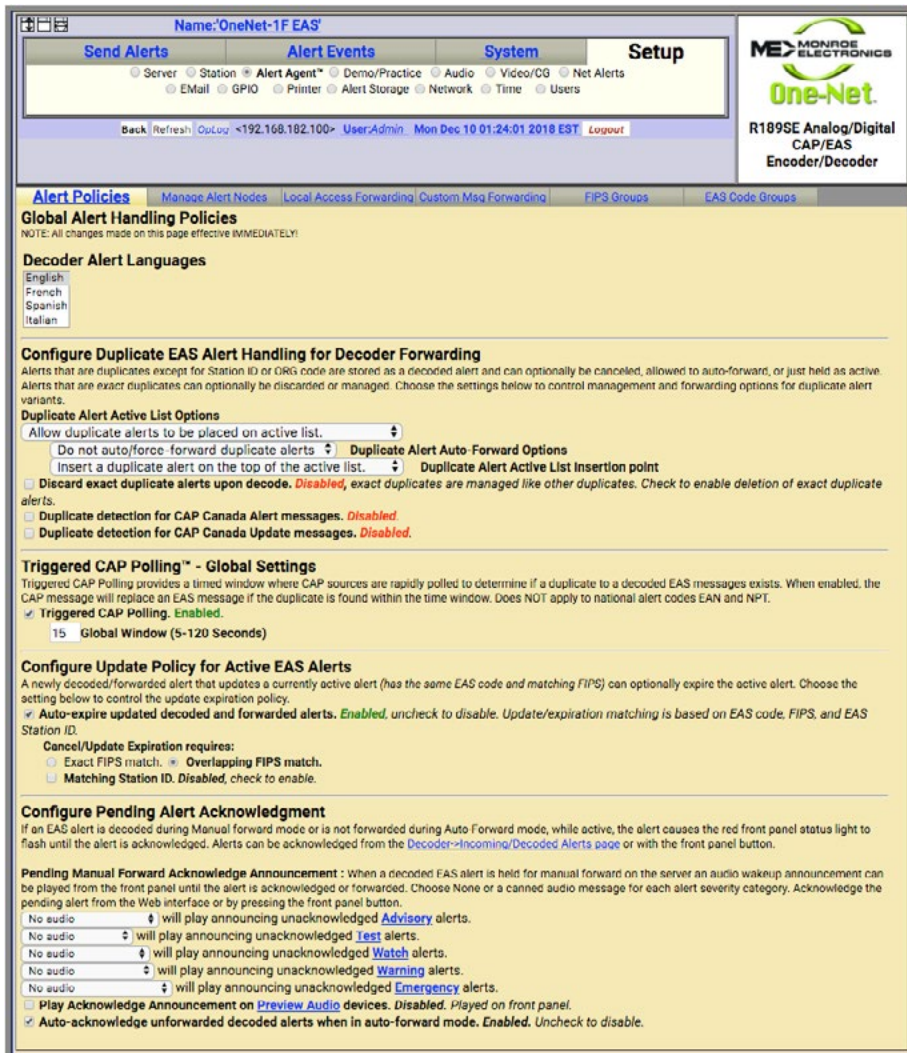
Alert Policies

The Alert Policies sub-tab is broken into four sections; Decoder Alert Language, Configure Duplicate EAS Alert Handling for Decoder Forwarding, Configure Update Policy for Active EAS Alerts, and Configure Pending Alert Acknowledgment (this sub-tab requires a Plus Package License Key). All changes to settings in this screen are immediate.



Attention

All changes to configuration settings on the Alerts Policies screen take effect immediately.



Alert Policies Screen

Decoder Alert Languages

This setting enables users to select the languages used within the EAS device. The default is English. Multiple languages may be selected using the SHIFT or CTRL keys.

Configure Duplicate EAS Alert Handling for Decoder Auto-Forwarding

An incoming EAS alert that is an exact duplicate of a previously decoded alert, is completely discarded and a message is logged in the operation log. EAS alerts that are duplicates except for Station ID or ORG code are stored as a decoded alert and can be optionally auto-forwarded or held. Use the selector to choose the setting to control manual or auto-forwarding for these alerts.

Triggered CAP Polling™ - Global Settings

When enabled, Triggered CAP Polling provides a timed window where CAP sources are rapidly polled to determine if a duplicate to a decoded EAS message exists. To enable, check the **Triggered CAP Polling** check box. Uncheck to disable. The **Global Window** time defines the amount of time after an EAS message is decoded the EAS device will rapidly poll the CAP server for a duplicate EAS message. If a duplicate CAP message is found within the configured time window, the initial EAS message will be dequeued and replaced with the more detailed CAP message. This feature does not apply to the EAN and NPT national codes. Additional Triggered CAP Polling controls can be found for individual Alert Nodes.



New Feature

Version 4.0 software introduces Triggered CAP Polling.

Configure Update Policy for Active EAS Alerts

This option allows you to expire an active alert when a new alert is decoded and updates the previous alert. When enabled, you can choose what requirements the new alert must have to expire the previous active alert.

The following is an example of this situation: Two local radio stations are being monitored. Both send out a monthly test for the same FIPS codes, with the same start time and duration, but the stations have changed the station ID. The alerts arrive several minutes apart. The EAS device has been set to auto-forward monthly tests to the given FIPS codes. The first decoded monthly test is forwarded automatically. The user has configured the duplicate alert handling to NOT auto-forward duplicate alerts that differ in Station ID or ORG code. The second alert is decoded, but is held for manual forward.

Configure Pending Alert Acknowledgment *(Requires a Plus Package License Key)*

When an EAS alert is decoded during Manual forward mode, while active, it causes the red front panel status light to flash until the alert is *acknowledged*. Alerts can be *acknowledged* from the **Alert Events > Incoming/Decoded Alerts** screen or by pressing the front panel button. In addition, some configuration options are associated with alert acknowledgment.

Pending Manual Forward Acknowledge Announcement

Each type of alert category can be configured to play-out an audio announcement on the front panel speaker during the time the alert is manually pending forward and before it has been acknowledged. Use the provided selectors to control audio announcement for each alert severity category.

Play Acknowledge Announcement on Preview Audio devices

The Audio Preview Devices are configured in the **Setup > Audio > Audio Output Levels/Test** screen. By checking this box, the Acknowledgment Announcement plays out the selected Audio Preview Devices. A Preview Audio hyperlink is provided to navigate to the Audio Preview Devices settings.

Auto-acknowledge unforwarded decoded alerts when in auto-forward mode

Checking this box automatically acknowledges any unforwarded decoded alerts while the EAS device is in auto-forward mode. The Auto-Forward Mode setting is located at **Setup > Station > Global Options** screen in the Global Forwarding Settings section.

Alert audio, if any, will play on the front panel speaker when the front panel button is pressed to acknowledge an unforwarded decoded alert

All EAS device versions provide a check box to select whether the alert voice audio message is played during Front Panel button acknowledgment of a current, active non-forwarded alert.

Manage Alert Nodes

Alert Nodes is a new concept in managing incoming EAS messages. The Alert Agent continuously monitors all incoming sources; analog – audio/radios, and digital - EAS-Net™ / CAP/ etc. then takes action if the input meets the specified criteria. To set the various properties, the Alert Agent uses Alert Nodes. An Alert Node allows the simple selection of alerting properties and defines an action based on the incoming criteria.

Alert Policies **Manage Alert Nodes** Local Access Forwarding Custom Msg Forwarding FIPS Groups EAS Code Groups

Manage Decoded Event Properties
Decoded events are screened and matched with specific properties in each section below. The first match is used. No match results in deactivation.

Incoming Decoded Event

Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN,NPT) - Only some options are configurable.

NATIONAL : Event Codes: EAN|NPT Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
All Sources	All Locations	EAS CIV WXR PEP	All Station IDs	Activate			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Live	Immediately	Off	None	Original, if any	Text-to-Speech if no audio	None

Default Decode/Forwarding Node for Monthly Tests

RMT : Event Codes: RMT ✓ Enabled Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
All Sources	All Locations	EAS CIV WXR PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Manual	As Soon As Possible	Off	None	Original, if any	Text-to-Speech if no audio	None

Default Decode/Forwarding Node for Weekly Tests

RWT : Event Codes: RWT ✓ Enabled Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
All Sources	All Locations	EAS CIV WXR PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Block Forwarding						

No Custom Decode event properties defined yet. Add first custom alert node

Default Decode/Forwarding Node for Non-National Alert Events

DFLT : Event Codes: All Codes Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
All Sources	All Locations	EAS CIV WXR PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Manual	As Soon As Possible	Off	None	Original, if any	Text-to-Speech if no audio	None

All remaining events are DEACTIVATED

Accept Changes Cancel Changes

Manage Alert Nodes Screen

The Manage Alert Nodes screen is divided into two sections: an Alert Node test (top of screen) and a list of Alert Nodes in order of priority (from top to bottom). Incoming decoded events will be evaluated by the top Alert Node and will continue down the list. The EAS device is pre-configured with four Alert Nodes – three are based on required alert events/tests: **National** (EAN & NPT), **Required Monthly Test** (RMT), and **Required Weekly Test** (RWT). These three required Alert Nodes cannot be deleted. The fourth Alert Node is named DFLT (or Default).

An example of the power and flexibility of Alert Nodes:

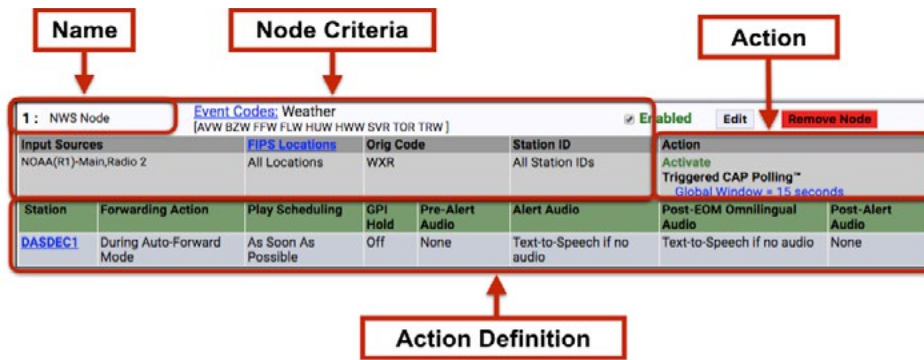
An EAS device is configured to monitor three radio sources; LP-1, LP-2, and the National Weather Service (NWS). The NWS source covers your service area as well as areas outside your service area, along with providing Required Weekly Tests. The RWT's broadcast by this NWS source duplicate RWT's received on LP-1. The NWS source is providing weather alerts for your service area and others while also providing duplicate RWT's. An Alert Node can be configured to only forward weather-related EAS alerts for your service area that are received on the NWS source. The Alert Node will ignore all other EAS alerts received from this source.

Before demonstrating how to configure an Alert Node for this example, below are some basic elements related to Alert Nodes.



Note

The Alert Node sub-tab requires the use of the Accept Changes button for any changes to take effect. There are Accept Changes and Cancel Change buttons at both the top and bottom of this screen.



Alert Nodes are simple to configure and have four basic components:

- Name
- Node Criteria
- Action
- Action Definition

Name

When adding a new Alert Node, the EAS device creates an Alert Node name (a combination of letters and numbers). Edit this name to be more descriptive of the Node's purpose. To the left of the name is a number that represents the order of the Alert Node. Changing the order of the Alert Node changes the Alert Nodes' number.

Node Criteria

At the core of each Alert Node is the Node Criteria where the decoded EAS information is processed and matched against the criteria settings established in the following five areas:

- Input Sources
- FIPS Location Codes
- EAS Event Codes
- Originator Codes
- Station ID

Input Sources

Any combination of input sources can be selected – a single radio source or a combination (radios, CAP/IPAWS, and/or EAS-NET™ sources). Select the desired input sources from the pull-down menu by clicking each item. Pressing the CTRL key while clicking input sources will allow the user to select multiple sources.

FIPS Location Codes

Clicking on the FIPS Locations pull-down menu will reveal all available FIPS Location Groups configured in the EAS device. Select the desired FIPS Location Group by clicking on it. The pull-down menu includes an **All Locations** selection as the default setting for cases when no specific FIPS Location Code Group is needed. FIPS Location Groups are configured within the **Setup > Alert Agent™ > FIPS Groups** sub-tab and can quickly be accessed by clicking the **FIPS Locations** hyperlink. Only one selection may be made from this pull-down menu.

EAS Event Codes

At the top of each Alert Node is an **Event Codes** pull-down menu where available EAS Code Groups are selected. The pull-down menu includes an **All** selection as the default setting when no specific EAS Event Code Group is needed. EAS Event Code Groups are configured within the **Setup > Alert Agent™ > EAS Code Groups** sub-tab and can quickly be accessed by clicking the **Event Codes** hyperlink. Only one selection may be made from this pull-down menu.

Orig (Originator) Codes

This is a three character ASCII code found in an EAS header which denotes the source of an EAS alert. Select one or a combination of Originator Codes from the list. Pressing the CTRL key while clicking input sources will allow the user to select multiple sources. The current FCC rules define four available ORG Codes:

- EAS – Broadcast Station/Cable System
- CIV – Civil Authority
- WXR – National Weather Service
- PEP – Primary Entry Point

Station ID

Found in the EAS header is the identification of the specific station that originated the EAS alert. Entering the desired station ID into this text field will allow EAS alerts that originate from this station ID to activate this Alert Node. Using an asterisk (*) will allow all station IDs.

Action

There are two available Action options found in this pull-down menu:

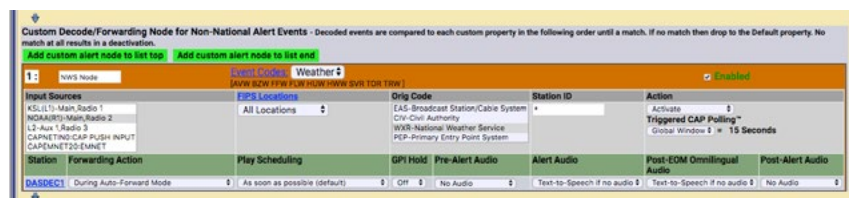
- Deactivate/Log Only
- Activate

The **Deactivate/Log Only** option will log the incoming EAS alert and perform no further actions. The Action Definition interface will not be visible and no actions may be configured.

Selecting **Activate** will make the Action Definition interface visible and configurable.

Triggered CAP Polling™ pull-down menu provides three options for node-specific configuration settings:

- Off (*will not initiate this feature for the given node criteria*)
- Global Window (*uses global time window settings*)
- Node Window (*enables use of custom time window settings*)



Editing a Custom Alert Node

Action Definition

The following settings are available when an Alert Node Action is set to **Activate**:

- Forwarding Action
- GPI Hold
- Pre-Alert Audio
- Alert Audio
- Post EOM Omnilingual Audio
- Post-Alert Audio

Forwarding Action

There are five available options from this pull-down menu:

- **Block Forwarding** – will NOT forward the EAS alert defined in this Alert Node.
- **Manual** – requires manual forwarding of the EAS alert defined in this Alert Node (GPI or manual forwarding)
- **During Auto-Forward Mode** – will automatically forward the EAS alert defined in this Alert Node when the station is in Auto-Forward Mode. When in Manual Forward Mode, users will need to manually forward the EAS alert via a GPI or web interface.
- **Force Immediately** – forces an immediate forward of the EAS alert defined in this Alert Node.
- **Force by offset time and before expiration** – displays offset settings (in minutes & seconds). Delays the forwarding of the EAS alert defined in this Alert Node by the entered offset time. If the offset pushes the EAS alert past its expiration time, the offset time will be reduced so as to forward the EAS alert within the expiration time. This alert may be forced by manual means (GPI or manual means).

Play Scheduling

When selecting any of the above **Forwarding Actions** besides Block Forwarding, the **Play Scheduling** pull-down menu becomes available.

- **As soon as possible** (default) – after the incoming alert message is decoded, it is played - beginning at the start time of the alert message.
- **As late as possible** – after the incoming alert message is decoded, it is held and then played just before the end of the valid alert time period.
- **Next minute interval** (MM:00) – the alert playout is delayed until the top of the next 60 second interval.
- **Next 30 sec. interval** (MM:00, 30) – the alert playout is delayed until the next 30 second interval.
- **Next 20 sec. interval** (MM:00, 20, 40) – the alert playout is delayed until the next 20 second interval.
- **Next 15 sec. interval** (MM:00, 15, 30, 45) – the alert playout is delayed until the next 15 second interval.
- **Next 10 sec. interval** – the alert playout is delayed until the next 10 second interval.
- **Immediately** – after the incoming alert message is decoded, it is played immediately - ignoring the start time of the alert message.

GPI Hold

In certain situations, it is desirable and acceptable to delay the forwarding of EAS alerts so as to not interfere with certain programming (i.e. commercial

content). GPI closures can be employed to hold off EAS alerts through automatic or manual means. Go to the **Setup > GPIO** screen for GPI settings.

Pre-Alert Audio

Audio WAV files can be uploaded to the EAS device and played prior to the EAS alert audio. This pull-down menu displays all the available audio WAV files stored on the EAS device. Select the desired audio WAV file by clicking it within the list. The selected file will play prior to the EAS alert defined within this Alert Node. Audio WAV files can be uploaded from the **Setup > Audio > Audio Output Levels/Test** screen.

Alert Audio

Enables multiple options for alert audio.

- **Original Audio** – plays the original alert audio contained within the EAS alert
- **Text-to-Speech if no audio** – creates and plays a text-to-speech audio file (based on the EAS alert text) if no audio file is available to play. A premium voice(s) is recommended when using this feature.
- **Text-to-Speech only** – ignores any original alert audio and forces the creation and playout of text-to-speech audio
- **Uploaded Audio WAV files** – a list of uploaded audio WAV files is available from the pull-down menu to be used during the Alert Audio section of the EAS message.

Post EOM Omnilingual Audio

This setting is only available with a valid OmniLingual™ Enable Key.

- **Original Audio** – plays the secondary language audio file contained within the EAS alert (CAP only)
- **Text-to-Speech if no audio** – creates and plays a text-to-speech audio file (based on the EAS alert text) if no secondary audio file is available to play. A premium voice(s) is recommended when using this feature.
- **Text-to-Speech only** – ignores any secondary audio files and forces the creation and playout of text-to-speech audio. This selection will provide a translation of the English text to the configured Extended Alert Languages found in the **Setup > Station > Main** sub-tab.

Post-Alert Audio

Audio WAV files can be uploaded to the EAS device and played after the EAS alert audio. This pull-down menu displays all the available audio WAV files stored on the EAS device. Select the desired file by clicking it in the list. The selected file will play after the EAS alert defined within this Alert Node. Audio WAV files can be uploaded from the **Setup > Audio > Audio Output Levels/Test** screen.

Enabled

All Alert Nodes (except for the National and DFLT) have an **Enabled** check box that allows users to enable/disable that Alert Node.

Edit

Clicking the **Edit** button on any Alert Node will allow the user to modify the settings for that particular node.



Note

In most situations, the original alert audio or text-to-speech audio are preferred. However, uploaded audio WAV files are frequently used for regular EAS tests such as the RMT. In this way the FCC EAS rules can be satisfied along with providing better quality and branded audio to the viewers.

Remove Node

Each Custom Alert Node has a red **Remove Node** button. This button will delete the corresponding Alert Node. After clicking the **Remove Node** button, the selected Alert Node will be removed from the web interface. Click the **Accept Changes** button to finalize the deletion. This deletion cannot be undone after the **Accept Changes** button has been used. Selecting the **Cancel Changes** button before clicking the **Accept Changes** button will restore the removed node.

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
All Sources	'Orleans Co' [036073]	EAS(CIV)WXR/PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Forced now	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
NOAA(R1)-Main, Radio 2	All Locations	WXR	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	During Auto-Forward Mode	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

Priority of Alert Nodes

Alert Nodes are placed in order of priority (from top to bottom). The Alert Node at the top of the list is processed first, followed by the next node down until each EAS alert reaches the DFLT Alert Node at the bottom of the screen. This is important to understand because an incoming EAS alert might meet the Node Criteria for multiple Alert Nodes. When this happens, only the first node in the priority list will perform the Action Definition of that node. Subsequent Alert Nodes with matching Node Criteria will not be processed. To make sure the Alert Nodes are in the correct order, test them with the Test Node Interface (see below). The required Alert Nodes are found at the top (National, RMT, & RWT) and bottom (DFLT) with the Custom Alert Nodes in between them. These are required nodes, but can be disabled. Changes to the order of Custom Alert Nodes are performed by clicking the up and down arrows located at the far left of each node. The order of required Alert Nodes cannot be modified.

Input Sources	FIPS Locations	Orig Code	Station ID	Action			
NWS(L2)-Aux 1, Radio 3	All Locations	EAS(CIV)WXR/PEP	All Station IDs	Activate			
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
All	Simultaneously during Auto-Forward mode	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None
1:WME 5.1	All Override or Manual	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None
2:WME 5.2	All Override or Manual	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

MultiStation Mode

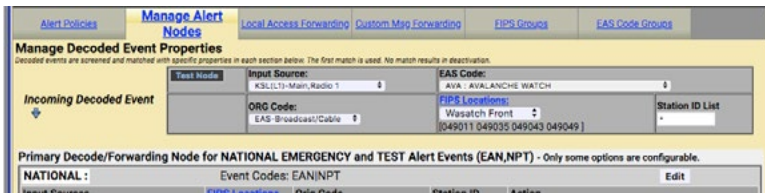
When utilizing MultiStation Mode, Alert Nodes will enable separate Alert Definition settings for each station. When a Node Criteria is matched with the incoming EAS alert, each stations' Alert Definition settings can be configured separately.

Forwarding Action, Play Scheduling, GPI Hold, Pre-Alert Audio, Alert Audio, Post-EOM Omnilingual Audio, and Post-Alert Audio settings can be defined for each station. This enables each station to customize how to handle the payout of the incoming alert and what audio is associated with that alert message.

To create a Custom Decode/Forwarding Alert Node:

- Click the green **Add custom alert node** button found below the RWT node. If this is the first custom node, there are three available button options:

- Add first custom alert node
- Add custom alert node to list top
- Add custom alert node to list end
- Once a new Alert Node is added, modify it by clicking the **Edit** button for that node.
- Assign a descriptive name
- Configure the desired Node Criteria
- Select the appropriate Action (Deactivate/Log Only or Activate)
- Configure the Action Definition settings
- Click the **Accept Changes** button



Test Node Interface Section

Test Node Interface

After creating new Alert Nodes, it is a good idea to test if they are configured properly. The Test Node interface was created for this purpose. It is located at the top of the **Manage Alert Nodes** sub-tab and has five settings and an action button along with a results field. This test simulates the conditions of an incoming EAS alert against the list of configured Alert Nodes. The test starts at the top of the list (NATIONAL) – stopping when it finds the first Alert Node with a matching Node Criteria.

The first step in running an Alert Node test is to input the test settings. They are as follows:

Input Source

This pull-down menu contains all the available sources (radios, CAP/IPAWS, and EAS-NET™, etc.) where an alert might be received. Select a source by clicking on it. Only one source may be selected when testing an Alert Node.

EAS Code

Select the desired EAS Code from this pull-down menu. Only one EAS Code may be selected.

ORG Code

Click on the appropriate Originator (ORG) Code. Only one ORG Code may be selected.

FIPS Locations

This pull-down displays a list of available FIPS Groups. Select the desired FIPS Group by clicking on it. Only one FIPS Group may be selected.

Station ID List

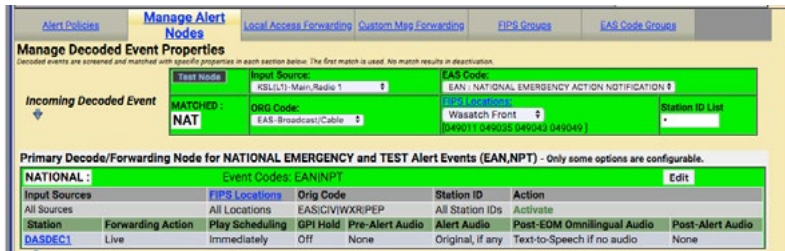
The default value for this text field is an asterisk '*'. When testing a Node for a specific Station ID, replace the asterisk with the desired Station ID.

Test Node

The Test Node button is used when all the test criteria has been entered (above). Click it to start the test.

Results Field

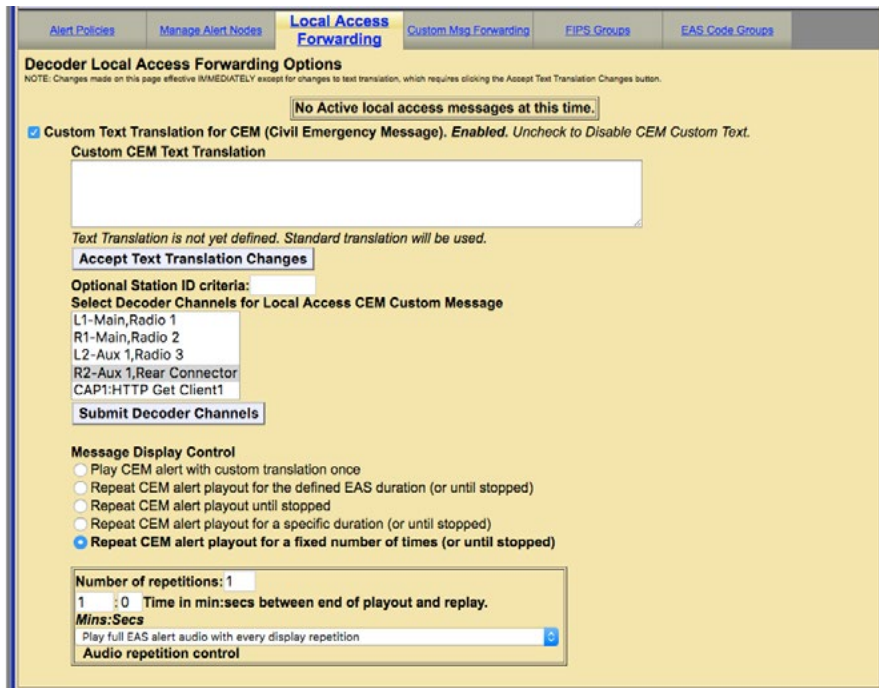
Located in the lower left corner of the Test Node interface is a blank gray box (below the Test Node button). The results of each test will be displayed here. When a match is found, the Test Node interface and the matching Alert Node will turn green and the results field will contain the word 'MATCHED' along with the name of the matching Alert Node. (See example below)



Test Node Interface Results

Local Access Forwarding

The **Decoder Local Access Forwarding** configuration sub-tab is used to configure customized forwarding play-out for decoded CEM (Civil Emergency Message) EAS alerts. This mode allows for custom alert translation text and repetition control when a CEM alert is auto-forwarded after being decoded from specific decoder channels and optionally, from a specific EAS source station (as based on decoded station ID). The mode is enabled using the check box **Custom Text Translation for CEM** (Civil Emergency Message).



Local Access Forwarding Screen

Custom Text Translation for CEM (Civil Emergency Message)

This check box controls activation of the local access forwarding feature. When enabled, as shown in the above screen shot, local access forwarding is active and can be configured. **If a local access CEM alert is decoded, it will be automatically forwarded regardless of the decoder forwarding mode.**

Local Access Message Play-out Status

The current status of Local Access Forwarding is displayed near the top of the page. When there are no active local access CEM messages being played, the status displays:

No Active local access messages at this time.

When a CEM alert is forwarded under control of Local Access Forwarding, the status window will display the: EAS devices' ID of the local access message, information about the repetition number of the play-out and when it will stop. There is a large flashing button for manually stopping the alert play-out at any time. While the message play-out is active, the **Setup > Alert Agent™ > Local Access Forwarding** screen will auto-refresh.

Sending originated CEM message with EAS ID 83!

Remaining event duration=14 mins 42 secs

THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A CIVIL EMERGENCY MESSAGE FOR THE FOLLOWING COUNTIES AREAS: Orleans, NY; AT 11:03 AM ON JUN 18, 2012 EFFECTIVE UNTIL 11:18 AM. MESSAGE FROM DASDEC.

Playing message for the first time.
Message will payout for 3 more times unless manually stopped.
Next play at Mon Jun 18 11:03:03 2012 EDT.

STOP Active Message

The same **Stop Active Message** button is available for the active alert displayed in the **Alert Events > Incoming Alerts and Incoming/Decoded Alerts** screens.

Currently Active Originated/Forwarded Alerts					
3 alert records displayed.					
Chnl/Orig	Code	ID	Start Time	End Time	Location
Orig from DASDEC (EAS)	CEM	83	Mon Jun 18 11:03:00 2012 EDT Originated Mon Jun 18 11:03:02 2012 EDT	Mon Jun 18 11:18:00 2012 EDT	Orleans, NY (036073)
			<div style="border: 1px solid black; padding: 2px; display: inline-block;">STOP Active Message</div> Goto custom message options.		
THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A CIVIL EMERGENCY MESSAGE FOR THE FOLLOWING COUNTIES AREAS: Orleans, NY; AT 11:03 AM ON JUN 18, 2012 EFFECTIVE UNTIL 11:18 AM. MESSAGE FROM DASDEC. Total EAS FSK+Audio Duration: 18.94 seconds					

Incoming/Decoded Alerts

Custom CEM Text Translation

This text, if provided, will be displayed on the video details page and sent to CG's and to network protocols (like EAS NET, SCTE18, etc.) when the alert is forwarded

When a decoded CEM alert is forwarded, the text will be displayed on the EAS device video details page, and will be sent to any serially connected character generators and network protocols. If no custom text is entered, the standard translation of the decoded alert is used. After text is entered, click on the **Accept Text Translation Changes** button to submit the changed text.



Note

Any text entered during an active alert will not be used. Custom CEM Text Translation text must be entered and accepted prior to being used by an incoming alert.

Optional Station ID criteria

A station ID filter code can be entered in the field below the CEM text box. This will limit action of local access forwarding to those CEM alerts decoded from the Decoder Local Access Forwarding configuration sub-page. It is used to configure custom forwarding play-out for decoded CEM (Civil Emergency Message) EAS alerts specified source station.

Select Decoder Channels for Local Access CEM Custom Message

This selector interface displays all available decoders on the system. Select the set of decoders for the CEM custom local access forwarding response. CEM alerts decoded on the unselected decoder channels will not trigger local access forwarding and will be processed like any other incoming decoded alert.

Message Display Control

Select an alert play-out repetition action. Each option has one or more sub-options to refine the play-out repetition period and audio.

Number of repetitions

The Message Display Control option “Repeat CEM alert play-out for a fixed number of times” is for selecting the number of times the CEM alert is replayed.

Replay period

The repeat period interface for Message Display Control options that cause repetition for certain time durations, can set the replay period to the time in minutes/seconds between end of play-out and replay.

Audio control/ audio repetition control

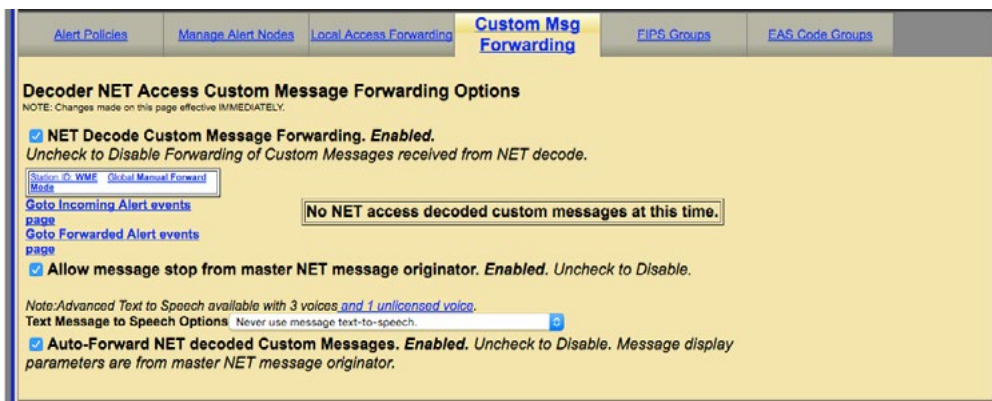
The pull-down menu allows selection of none, all, or part of the EAS audio message during the first and repeat play-outs.

Custom MSG Forwarding

The **Decoder NET Access Custom Message Forwarding Options** screen allows a user to enable EAS NET decode custom message forwarding and gives them control over how these messages are forwarded. Even in Manual Forwarding Mode, a user can auto-forward EAS NET decoded custom messages.

NET Decode Custom Message Forwarding

When enabled, it gives the operator the ability to forward decoded messages from EAS NET. If this option is disabled, custom messages that are decoded over EAS NET cannot be forwarded.



Custom Message Forwarding Screen

If the EAS device does not have any current active custom message alerts, there will be a message that says: **No NET access decoded custom messages at this time.**

If the EAS device does have a current active custom message alert, that alert will appear on the right side of the page in red.

If the **NET Decode Custom Message Forwarding** is enabled, more options appear.

Allow message stop from master NET message originator

This option allows the EAS device that sent a custom message via EAS NET to control when the alert is stopped on the receiving EAS device. If this is not enabled, the user would manually stop the alert on the receiving EAS device (if it is before the alert is done).

Text Message to Speech Options

This drop down menu gives the EAS device the ability to use a text-to-speech engine on EAS NET decoded custom alerts. There are three options:

- Never use message text-to-speech
- Use message text-to-speech only if Audio not present
- Always use message text-to-speech. Ignore Audio if present.

Auto-Forward NET decoded Custom Messages

This option gives the EAS device the ability to auto forward decoded EAS NET custom messages, even if the EAS device is in Manual Forwarding Mode.

FIPS Groups

The **FIPS Groups** sub-tab screen was first introduced within V3.0 software. Throughout the user interface there are numerous places to enter FIPS Location Codes. In an effort to eliminate redundant operations and reduce errors, FIPS code Groups were created. Users can create and modify groups of FIPS Codes in one central area and use those groups throughout the web interface. This screen is also where a list of available encoder FIPS code locations is established. The **FIPS Group** sub-tab has two sections; **Manage FIPS Location Group Lists** section and the **Configure Available FIPS for Encoder Alert Origination** section.

The screenshot displays the 'Manage FIPS Location Group Lists' interface. At the top, there are navigation tabs: Alert Policies, Manage Alert Nodes, Local Access Forwarding, Custom Msg Forwarding, **FIPS Groups**, and EAS Code Groups. Below the tabs, the main heading is 'Manage FIPS Location Group Lists' with a sub-note: 'FIPS location group lists provide a general tool for specifying FIPS locations for various operations.' A button 'Add New FIPS Group' is visible. Three groups are listed:

- 1: Name Orleans Co** (Use count: 0) with 'Edit', 'Delete Group', and 'Duplicate Group' buttons. Locations: Orleans, NY (036073) - 1 location.
- 2: Name Rochester** (Use count: 0) with 'Edit', 'Delete Group', and 'Duplicate Group' buttons. Locations: Genesee, NY (036037), Monroe, NY (036055) - 2 locations.
- 3: Name Western NY** (Use count: 1) with 'Edit' and 'Duplicate Group' buttons. Locations: Erie, NY (036029), Genesee, NY (036037), Livingston, NY (036051), Monroe, NY (036055) - 7 locations.

The bottom section is 'Configure Available FIPS for Encoder Alert Origination'. It includes dropdowns for 'Choose FIPS Subdivision' (All), 'Choose FIPS State' (United States (US) (00)), and 'Choose FIPS Counties' (All (000)). A list of 'Configured Available Encoder FIPS Locations' is shown, including Orleans, NY (036073), Monroe, NY (036055), Niagara, NY (036063), Erie, NY (036029), Genesee, NY (036037), Livingston, NY (036051), and Wyoming, NY (036121). Buttons for 'Add ->' and 'Remove Selected' are present.

Manage FIPS Location Group Lists Screen

Manage FIPS Location Group Lists

This section of the screen displays a list of existing FIPS Groups and enables users to add, edit, duplicate and delete FIPS Groups. A brand new EAS device will not have any configured FIPS code groups - they will need to be added on this screen.

Add New FIPS Group

To create a new FIPS Group click the **Add New FIPS Group** button. A new FIPS group will appear at the top of the FIPS Location Group Lists and will have an auto-generated name, starting with a series of numbers and ending in ‘_FIPS’. This group will have no defined FIPS codes and will need to be edited.

Individual FIPS Groups contain the following information and action buttons:

Name

Name of the FIPS Group.

Use Count

Number of times this FIPS Group is used throughout the web interface.

FIPS Codes List

Displays the first four FIPS codes used in the group, along with a number of FIPS code locations contained in the group.

Edit

This button opens the edit FIPS Group interface. Here FIPS codes are added and removed in the group and the group name can be edited.

Duplicate Group

Clicking this button will create a duplicate FIPS Group and place it below the original. It copies the existing group name and adds ‘.CPY’ at the end.

Delete Group

Users wanting to delete a FIPS Group can click this button. This button is only available to groups not being used throughout the web interface. (See **Use Count** above.) Once the Delete Group button is clicked, a confirmation screen will appear asking: **Are you sure you want to delete the selected FIPS group?**

User may select either:

- Yes, delete group.
- No, cancel group deletion!

The screenshot displays the 'Edit FIPS Group Section' within a web application. The top navigation bar includes links for 'Alert Policies', 'Manage Alert Nodes', 'Local Access Forwarding', 'Custom Msg Forwarding', 'FIPS Groups', and 'EAS Code Groups'. The main heading is 'Manage FIPS Location Group Lists'. Below this, a text box shows the group name '1: Name 0683254792_FIPS'. The form contains three dropdown menus: 'Choose FIPS Subdivision' (set to 'All'), 'Choose FIPS State' (set to 'United States (US) (00)'), and 'Choose FIPS Counties' (set to 'All (000)'). An 'Add ->' button is positioned to the right of the counties dropdown. A 'FIPS codes' section shows 'No Codes' and a 'Remove Selected' button. At the bottom of the form, there are 'Accept Changes' and 'Cancel Changes' buttons.

Edit FIPS Group Section

To edit a new or existing FIPS Group, click the corresponding **Edit** button. User have the ability to change the name and add/remove FIPS codes within this group. The following fields, pull-downs, and buttons are available:

Name

The EAS device automatically generates a name for new FIPS Group. Highlight the text and enter a descriptive name for this group of FIPS codes.

Choose FIPS Subdivision

A pull-down menu showing the subdivision setting of the chosen FIPS County. A selection of **All** should be used unless the county is to be subdivided. To subdivide a county:

- Select one of the FIPS Subdivisions options (North, Northeast, West, etc.)
- Select a FIPS County
- Click the **Add** button to add that subdivision to the **FIPS codes** list.

Multiple subdivisions of a single county can be added to the **FIPS codes** list by repeating the above steps. For example, both North Orleans, NY and Northeast Orleans, NY FIPS codes can be added.

Choose FIPS State

This pull-down contains a list of US States, territories and pre-defined FIPS regions. Select the desired item and the EAS device will populate the **Choose FIPS Counties** with the FIPS codes available for that area in numeric order.

Choose FIPS Counties

This area is populated with individual FIPS codes based on the selection made in the **Choose FIPS State** pull-down menu. It is from this area that FIPS codes are added to the **FIPS codes** list for the group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection.

FIPS Codes

This area represents a list of FIPS codes used in the group. Only FIPS codes found in this area will be used for processing wherever this FIPS group is selected. FIPS codes are added to this list by selecting the desired codes from the FIPS Counties list and clicking the **Add ->** button. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->

Clicking this button will add the selected **FIPS Counties** to the **FIPS codes** list area.

Remove Selection

FIPS code can be removed from the **FIPS codes** list by selecting the item and clicking the **Remove Selected** button.

Accept Changes

This button will finalize any additions, edits, and/or deletions made while editing a FIPS code group. Once clicked, the Edit FIPS group section of the interface will be removed and the screen will return to its normal state.

Cancel Changes

Pressing this button will cancel any changes made to the FIPS group and return this screen to its normal state.



Caution

Check to make sure **All** is selected in the **Choose FIPS Subdivision** drop-down menu. Selecting another option in this menu will sub-divide the selected **FIPS Counties** and may result in EAS alerts being missed. Double check that subdividing a county will trigger the proper alerts.

Configure Available FIPS for Encoder Alert Origination

The **Send Alerts** tab is where users configure and send alerts from the EAS device. A list of FIPS codes for available locations where these alerts may be sent is configured in the lower section of the screen. The interface operates similarly as the edit FIPS group interface:

Choose FIPS Subdivision

A pull-down menu showing the subdivision setting of the chosen FIPS County. A selection of **All** should be used unless the county is to be subdivided. To subdivide a county:

- Select one of the FIPS Subdivisions options (North, Northeast, West, etc.)
- Select a FIPS County
- Click the **Add** button to add that subdivision to the **FIPS codes** list.

Multiple subdivisions of a single county can be added to the **FIPS codes** list by repeating the above steps. For example, both North Orleans, NY and Northeast Orleans, NY FIPS codes can be added.

Choose FIPS State

This pull-down contains a list of US States, territories and pre-defined FIPS regions. Select the desired item and the EAS device will populate the **Choose FIPS Counties** with the FIPS codes available for that area in numeric order.

Choose FIPS Counties

This area is populated with individual FIPS codes based on the selection made in the **Choose FIPS State** pull-down menu. It is from this area that FIPS codes are added to the **FIPS codes** list for the group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection.

FIPS Codes

This area represents a list of FIPS codes used in the group. Only FIPS codes found in this area will be used for processing wherever this FIPS group is selected. FIPS codes are added to this list by selecting the desired codes from the FIPS Counties list and clicking the **Add ->** button. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->

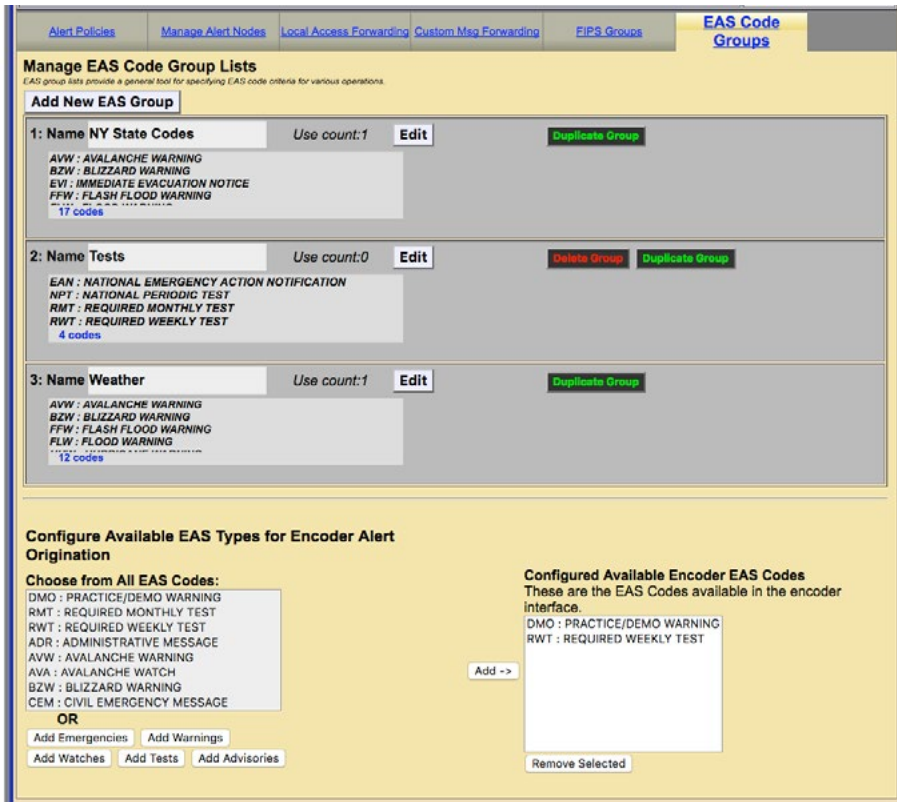
Clicking this button will add the selected **FIPS Counties** to the **FIPS codes** list area.

Remove Selection

FIPS code can be removed from the **FIPS codes** list by selecting the item and clicking the **Remove Selected** button.

EAS Code Groups

EAS Code Groups were first introduced with V3.0 software. There are numerous places to enter EAS codes within the web interface. EAS Code Groups were created to eliminate redundant operations and reduce errors. The EAS Code Groups sub-tab is divided into two sections. The **Manage EAS Code Group Lists** section provides controls to add, edit, duplicate and delete these groups. The **Configure Available EAS Types for Encoder Alert Origination** section is where users establish a list of available encoder EAS codes.



EAS Code Groups Sub-Tab

Manage EAS Code Group Lists

The top section of this screen shows a list of configured EAS Code Groups and enables the user to add, edit, duplicate and delete these groups.

Add New EAS Group

To add a new EAS Group, first click the **Add New FIPS Group** button. A new EAS group will appear at the top of the EAS Code Group Lists and have an automatically generated name starting with a series of numbers and ending in ‘_EAS’. This group will have no defined EAS codes and will need to be edited.

EAS Code Groups contain the following information and action buttons:

Name

The name of the EAS Code.

Use Count

Number of times this EAS Code is used throughout the web interface.

EAS Codes List

Displays the first four EAS codes used in this group along with a number of EAS codes contained in this group.

Edit

This button opens the edit EAS Code interface where EAS codes are added and removed within this group and where the group name can be edited.

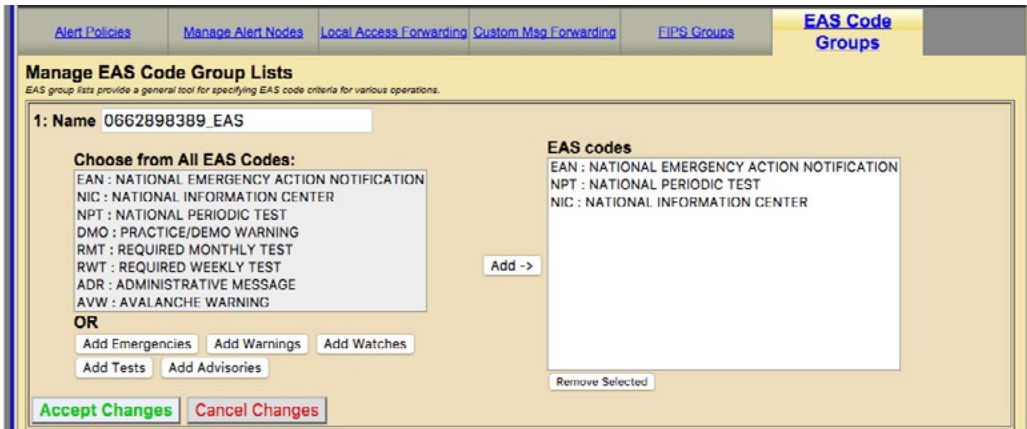
Duplicate Group

Clicking this button will create a duplicate EAS Code Group and place it below the original. The duplicate group copies the existing group name and adds ‘.CPY’ to the end of it.

Delete Group

Users wanting to delete a EAS Code can click this button. This button is only available to groups not being used throughout the web interface. (see Use Count) Once the Delete Group button is clicked, a confirmation screen will appear asking: **Are you sure you want to delete the selected EAS Filter group?** User may select either:

- Yes, delete group.
- No, cancel group deletion!



Edit EAS Code Group Section

To edit a new or existing EAS Code Group, click the corresponding **Edit** button. The user will have the ability to change the name and add/remove EAS codes within this group. The following fields, pull-downs, and buttons are available:

Name

An automatically generate name is found in the **Name** field. Highlight the text in this field and enter a descriptive name for this group of EAS codes.

Choose from All EAS Codes:

This area contains all the EAS codes. It is from this area (and the **Quick Add** buttons just below) that EAS codes are added to the **EAS codes** list for this group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection. Both a mouse scroll (while the mouse hovers over this area) and keyboard up/down arrows will allow users to scroll the entire list of codes.

Quick Add Buttons

These five buttons, located just below the **Choose from All EAS Codes:** area, will quickly add their respective codes to the EAS codes list – foregoing the use of the **Add ->** button. The five Quick Add buttons are:

- **Add Emergencies** – contains all emergency related codes
- **Add Warnings** – contains all the warning codes
- **Add Watches** – contains all the watches codes
- **Add Tests** – contains all the test codes
- **Add Advisories** – contains all the advisory codes



Attention

EAN, NPT, and NIC codes are automatically added to new or empty EAS Code Groups to insure they are utilized when filtering in any area of the web interface. These national codes may be removed in instances where they are not needed.

EAS Codes

This area displays a list of EAS codes used in the group. Only EAS codes found in this area will be used for processing wherever this EAS group is selected. EAS codes are added to this list by selecting the desired codes from the **Choose from All EAS Codes** list and clicking the **Add ->** button. Alternatively, clicking the Quick Add buttons will add the associated codes to this area. Items are removed from this list by selecting the item(s) and clicking the **Remove Selected** button.

Add ->

Clicking this button will add the selected **Choose from All EAS Codes** to the **Configured Available Encoder EAS codes** list area.

Remove Selection

EAS code can be removed from the **EAS codes** list by selecting the item and clicking the **Remove Selected** button.

Accept Changes

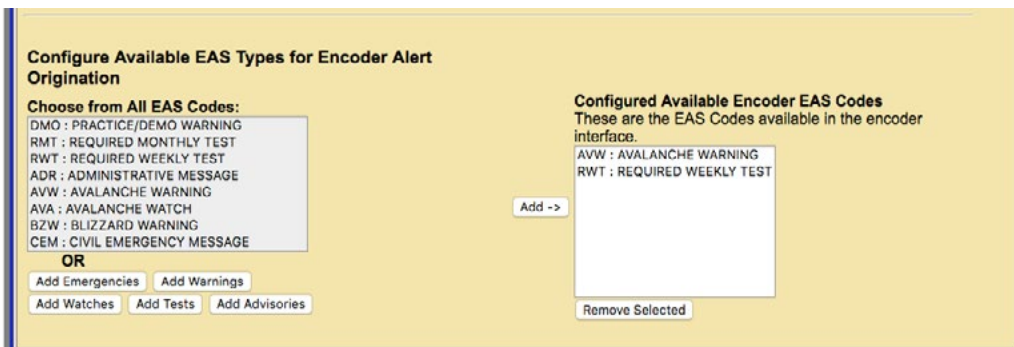
This button will finalize any additions, edits, and/or deletions made while editing a EAS code group. Once clicked, the Edit EAS code group section of the interface will be removed and the screen will return to its normal state.

Cancel Changes

Pressing this button will cancel any changes made to the EAS code group and return this screen to its normal state.

Configure Available EAS Types for Encoder Alert Origination

The **Send Alerts** tab is where users can configure and send alerts from the EAS device. A list of EAS codes for available locations where these alerts may be sent is configured in the lower section of this screen. The interface operates similarly as the edit EAS code group interface.



Configure Available EAS Types for Encoder Alert Origination Section

Choose from All EAS Codes:

This area contains all the EAS codes. It is from this area (and the **Quick Add** buttons just below) that EAS codes are added to the **EAS codes** list for this group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection. Both a mouse scroll (while the mouse hovers over this area) and keyboard up/down arrows will allow users to scroll the entire list of codes.

Quick Add Buttons

These five buttons, located just below the **Choose from All EAS Codes:** area, will quickly add their respective codes to the EAS codes list – foregoing the use of the **Add ->** button. The five Quick Add buttons are defined above.

Configured Available Encoder EAS Codes

This area represents a list of available EAS codes when sending alerts. Only EAS codes found in this area will be available to the user. EAS codes are added to this list by selecting the desired codes from the **Choose from All EAS Codes** list and clicking the **Add ->** button or by using the **Quick Add** buttons. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->

Clicking this button will add the selected **Choose from All EAS Codes** to the **Configured Available Encoder EAS codes** list area.

Remove Selection

FIPS code can be removed from the **EAS codes** list by selecting the item and clicking the **Remove Selected** button.

STATION SETUP

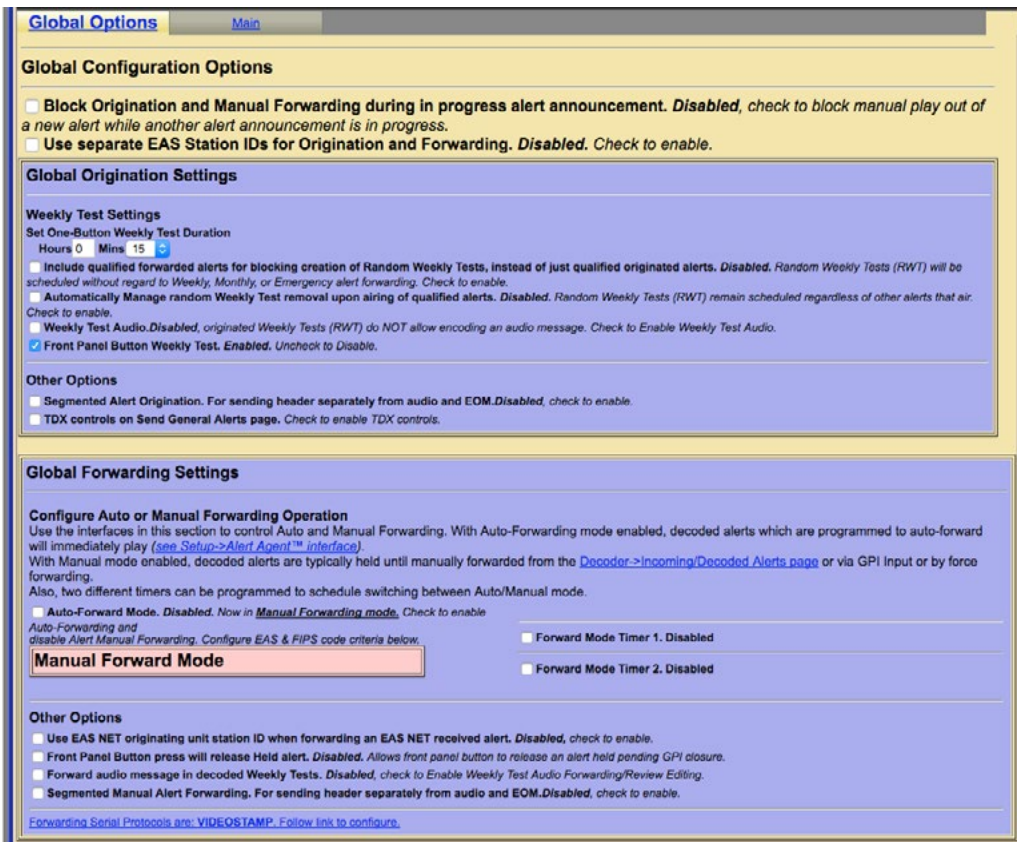
The **Station** radio button within the **Setup** tab is where station alert originations and alert forwarding settings are located. The origination settings primarily focus on Required Weekly Test settings. There are two standard sub-tabs: **Global Options** and **Main**.

The standard **Station** sub-tabs are described as follows:

Sub-Tab	Description
Global Options	Configuration of global origination (Required Weekly Tests) and forwarding settings. Auto-Forward Mode settings are found here.
Main	Station specific ID, language settings in addition to origination and forwarding settings

When using **MultiStation** mode, the web interface displays additional sub-tabs, one for each station and a simultaneous station override sub-tab. Using these additional settings, the EAS device can handle each stations' ID, languages, origination, and forwarding settings separately.

Sub-Tab	Description
Global Options	Configuration of global origination (Required Weekly Tests) and forwarding setting. The Auto-Forward Mode settings are found here.
Simultaneous Station Override	Simultaneous ID, language settings in addition to origination and forwarding settings
Station 1 - 5	Station specific ID, language settings in addition to GPIO handling, origination and forwarding settings. The number of station sub-tabs will depend on license key – with MultiStation 2 or 5.



Station Setup Screen

Global Options

Block Origination and Manual Forwarding during in progress alert announcement

Check to block manual play-out of a new alert while another announcement is in progress. If left unchecked, the alerts will play sequentially.

Use separate EAS Station IDs for Origination and Forwarding

Enables the user to configure a different **EAS Station ID** for the Origination Settings and the Forwarding Settings. These settings are found within the **Setup > Station > Main** screen. A valid Plus Package License Key is required.

Global Origination Settings

This section of the screen has two distinct parts: **Weekly Test Settings** and **Other Options**.

Weekly Test Settings

Set One-Button Weekly Test Duration

Input the duration of the RWT in hours and minutes. The default time is 15 minutes.

Include qualified forwarded alerts for blocking creation of Random Weekly Tests, instead of just qualified originated alerts.

Random Weekly Tests (RWT) will be scheduled without regard to Weekly, Monthly, or Emergency alert forwarding. Check to enable.

Automatically Manage Tests random Weekly Test removal upon airing of qualified alerts

Random Weekly Tests (RWT) remain scheduled regardless of other alerts that air. Check to enable.



Note

The minimum duration of any EAS alert is 15 minutes. This time setting represents the duration of the alert itself, and does not reflect the amount of time the alert is broadcast.

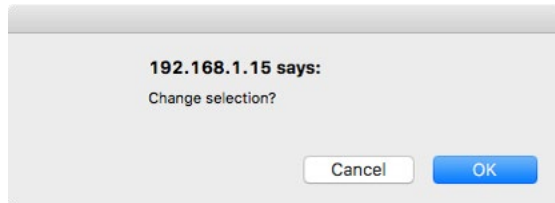
Weekly Test Audio

Default is disabled. This controls whether the originated Weekly Test (RWT) can be constructed with an audio message. The audio message is configured within the **Weekly Test Settings** inside the **Origination Settings** section of the **Setup > Station > Main** screen labeled **Optional Alert Audio Announcement**. – this option requires a valid Plus Package license key.

Front Panel Button Weekly Test

Check this box to initiate an RWT using the front panel button.

A confirmation page has been added when making changes to FIPS Groups and the Audio File selectors within the **Required Weekly Test** settings due to the importance of these settings.



Other Options

All these other options require a Plus Package License Key

Segmented Alert Origination

Default is disabled. This controls whether the option for segmented alert origination is available on the **Send Alerts> General Alerts** screen. Segmented alert origination is when the alert header and attention signal are played with a pause for live audio voice dub. A separate button allows the play-out of audio files and EOM. (In EAS, the End of Message (EOM) is signaled by the final three FSK audio bursts.)

TDX controls on Send general EAS page

Check to enable TDX controls (requires a TDX license key) found within the **Send Alerts > General Alerts** screen. Requires a valid TDX license key.

Global Forwarding Settings

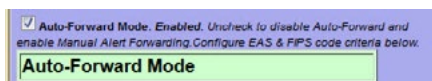
Configure Auto or Manual Forwarding Operation

One essential decision that an EAS participant must make is whether to run an EAS decoder in Auto-Forward mode or Manual Forwarding mode. This section provides the controls over these two options.

The text box on the left side of this section indicates the current forwarding state. It will display either “Auto-Forward Mode Enabled” or “Manual Forward Mode”. The same information is also displayed on the Alert Events > Incoming Alerts pages. To set the Auto-Forward Mode or the Manual Forward Mode look to the check box to on the right side of this section.

Auto-Forward Mode

Check the first check box to enable Auto-Forwarding. Uncheck to select Manual Forwarding. A large button that says “Manual Forward Mode” or “Auto Forward Mode” will be displayed.

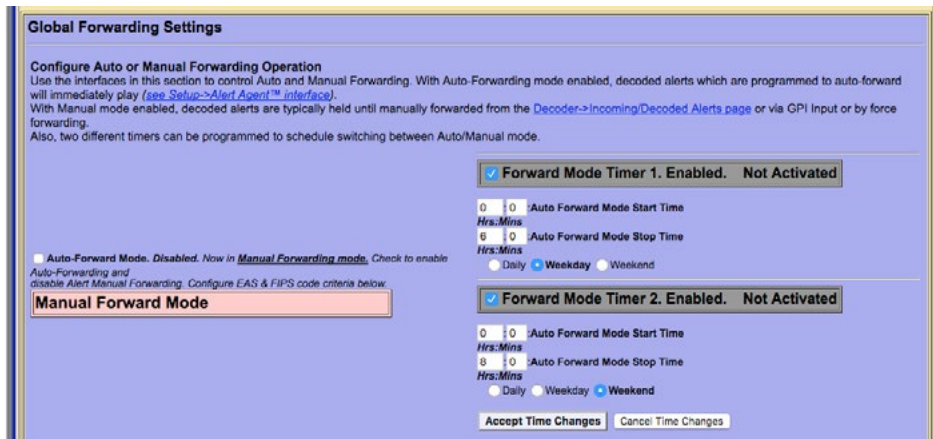


Note

Emergency National Activation (EAN) and National Periodic Test (NPT) alerts always forward automatically.

When manual forwarding is set, the web interface or GPI input contact closures must be used to actively forward any unforwarded alerts from the Alert Events > Incoming/Decoded Alerts screen.

During Auto-Forward mode, the EAS device forwards alerts without review or intervention provided they pass the currently configured Auto-Forwarding criteria.



Global Forwarding Setting with Timers enabled

Forward Mode Timers

All licensed versions feature two Forward Mode Timers that can be enabled independently to automatically switch the EAS device between Manual and Automatic Forwarding modes. The timers can be set to run on a daily basis, or just on weekends or weekdays. Each timer has a time setting for enabling Auto-Forwarding and later disabling Auto-Forwarding. Active timers override the check box for setting Auto/Manual Forward Mode. The timers allow a station to schedule auto-forwarding when unmanned and manual forwarding at other times. For both timers, the start and stop time fields need to be modified by the system administrator to configure when the EAS device will go into Auto-Forward mode and when will go back to Manual mode. In the screen shot above, Auto-Forward Mode is active from midnight to 6:00am on Weekdays and from midnight to 8:00am on Saturday and Sunday.

Other Options

Use EAS NET originating unit station ID when forwarding an EAS NET received alert

Check to enable.

Front Panel Button press will release Held alert

Allows front panel button to release an alert held pending GPI closure.

Forward audio message in decoded Weekly Tests

If a decoded Required Weekly Test (RWT) has audio, it will be forwarded. This is uncommon, but can occur. When disabled, decoded RWT alerts with audio will discard the audio portion of the RWT during forwarding.

Segmented Manual Alert Forwarding

If enabled, manual forwarding will provide buttons to send the alert header and attention signal separately from audio and EOM. This provides an opportunity to dub in live audio. Uncheck to disable.

Main

The screen provides controls to set the basic values to construct an EAS alert and contains three sections; general station settings, Origination Settings, and Forwarding Settings.

EAS Station ID

Type up to 8 characters in this text field to identify the Station ID. This code is included in all originated alerts, both manually forwarded and automatically forwarded alerts.

Uses Server Timezone:

Displays the configured time zone. To change this setting, go to **Setup > Time**.

Primary Alert Language

This pull-down menu is used to select the primary alert language. A list of available languages is displayed.

Extended Alert Language

A list of available languages is displayed within this box. Select one language by clicking it. Multiple languages may be selected by using the CTRL key when making additional selections.

Omit serial/audio/video/stream play out for non-national alerts

Check to NOT play alert through serial/audio/video/stream outputs. Useful for only sending alert through non-streaming Net Alert interfaces. Applies to both Origination & Forwarding.

GPI Alert Hold

Optionally designate GPI inputs to hold alerts (until closure or during closure). When using the last two options, a list of GPI's is available for selection.

- Do not use GPI Alert Hold
- Designated GPIs Hold alert while Closed
- Designated GPIs Hold alert while Open

Global Options **Main**

Station Configuration

EAS Station ID WME Uses Server Timezone: Mountain

Primary Alert Language English

Extended Alert Languages English Spanish

Omit serial/audio/video/stream play out for non-national alerts. Disabled, check to NOT play alert through serial/audio/video/stream outputs. Useful for only sending alert through non-streaming Net Alert interfaces. Applies to both Origination & Forwarding.
[Decoder Languages, Duplicate Handling, Update Policy, etc - Goto Alert Policies page.](#)

Do not use GPI Alert Hold GPI Alert Hold - Optionally designate GPI inputs to hold alerts (until closure or during closure).

Origination Settings

EAS Origination (ORG) Code
 EAS-Broadcast Station/Cable System
 CIV-Civil Authority
 WXR-National Weather Service

Use custom text for origination (ORG) code string. Enabled, uncheck to disable.
 A BROADCASTER Custom Origination (ORG) Code
 Translation. The phrase 'HAS ISSUED' follows this string in the translation.

Non-national alert play scheduling .
 Play As soon as possible (default)

Weekly Test Settings

Optional Pre-Alert Audio Announcement Played before the EAS header audio.
 No Audio

Optional Post-Alert Audio Announcement Played after the EAS EOM audio.
 No Audio

Automatic Random Required Weekly Test Generation. Enabled. Uncheck to disable (effective immediately).
 Note: Override Random Weekly Test will play the RWT audio, with override station FIPS and override station EAS ID, only on internal audio output.
IMPORTANT: This test will not play on stations or multiplexer!

FIPS Group
 Western NY

1. United States (000000) NOT USED!
 2. New York (036000)
 3. Genesee, NY (036037)
 4. Livingston, NY (036051)
 5. Monroe, NY (036055)
 6. Niagara, NY (036063)
 7. Orleans, NY (036073)

Required Weekly Tests are automatically generated.
 Notes: 1. If 1st time is greater than 2nd time, alert is scheduled from 0 hrs Midnight to 2nd time or 1st time to 23:59.
 2. A random Automatic Weekly test is only scheduled if no weekly tests have been originated during the current week (Sun-Sat).
 3. If changes are made, a previously scheduled weekly test must be manually cancelled before a new test will be scheduled within the new time frame. See [Alert Events->Originated Alerts.](#)

Between Time and Time
 0 : 0 : 6 : 30 :
 Hrs: Mins Hrs: Mins
 Accept Time Changes Cancel Time Changes

On days: Checked days are candidates for RWT, unchecked days are omitted (effective immediately).
 Sun Mon Tue Wed Thu Fri Sat

Forwarding Settings

Global forward mode is Auto.
 Retranslate EAS alert text. Use forwarding station ID and timezone. Disabled, decoded translation will be used; check to enable.

[Goto Alert Agent Settings page](#) [Goto Alert Agent Policies](#)

Main Sub-tab Screen

Origination Settings

EAS Origination (ORG) Code

The ORG code is a standard part of the EAS audio protocol. It is placed in the EAS alert message when the encoder originates an EAS alert. The same code is used for forwarded alerts. MultiStation operation allows this value to be overridden per station definition. This code categorizes the type of organization sending the EAS. Use the selection menu to choose the EAS Origination code for your system:

- EAS – Broadcast station or cable system
- CIV – Civil authorities
- WXR – National Weather Service
- PEP – Primary Entry Point System

Custom text for origination (ORG) code string

Default is disabled. The origination codes are given a standard text translation when an encoded EAS alert is sent to a video display. When an EAS origination code is used, the alert text will start with the phrase “A Broadcast or Cable System has issued.” Checking the Custom Text option allows a custom translation to be used instead.

In the screen shot above, Custom Text is enabled. When enabled, a text entry box is displayed in which you can enter the organization name issuing the alert for Custom Origination (ORG) Code Translation. In the screen shot, the phrase, “A BROADCASTER” has been entered as the custom text. The EAS translation text will use this phrase instead of the generic “A Broadcast or Cable System.” The phrase “HAS ISSUED” follows the custom organization name in the alert translation.

Non-national alert play scheduling

Set the play scheduling for the originating alert. The options are as follows:

- **As soon as possible** (default) – after the incoming alert message is decoded, it is played - beginning at the start time of the alert message.
- **As late as possible** – after the incoming alert message is decoded, it is held and then played just before the end of the valid alert time period.
- **Top of next minute interval** (MM:00) – the alert payout is delayed until the top of the next 60 second interval.
- **Next 30 sec. interval** (MM:00, 30) – the alert payout is delayed until the next 30 second interval.
- **Next 20 sec. interval** (MM:00, 20, 40) – the alert payout is delayed until the next 20 second interval.
- **Next 15 sec. interval** (MM:00, 15, 30, 45) – the alert payout is delayed until the next 15 second interval.
- **Next 10 sec. interval** – the alert payout is delayed until the next 10 second interval.

Weekly Test Settings

Optional Pre-Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played prior to the EAS header audio.

Optional Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played following the EAS header audio and the attention two-tone signal. Only available if option is enabled within the **Setup > Station > Global Options (Weekly Test Audio** check box)

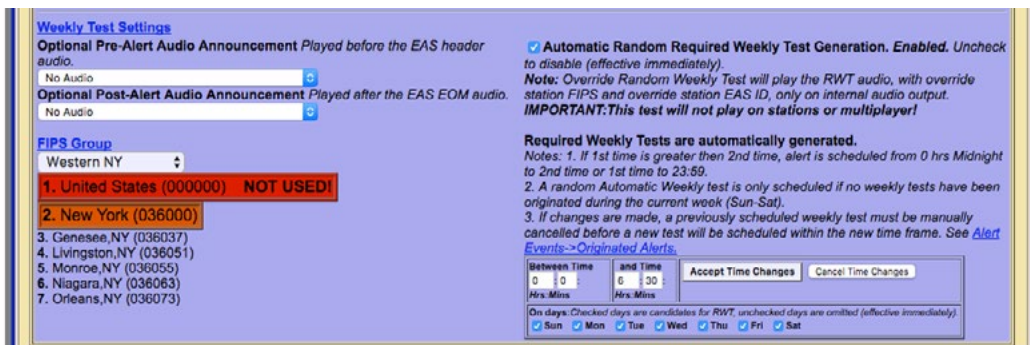
Optional Post-Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played after the EAS end of message (EOM) audio.

FIPS Group

Make a selection from the pull-down list to designate the desired FIPS Codes Group.

Notice the color coding of the United States code (000000) in red and the state-wide code (New York in the below example) in orange. The EAS device will block the use of the United States FIPS code and any ‘wildcarded’ state codes when originating alerts along with including the text “NOT USED”. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but likely not very common.



Weekly Test Settings Section

Automatic Random Required Weekly Test Generation

The check box allows you to enable Required Weekly Tests to be automatically generated at a random time within a pre-selected time frame for specifically selected days. If enabled, controls are displayed that allow setting the time period and the days for which the test will be scheduled.

Between Start Time and End Time

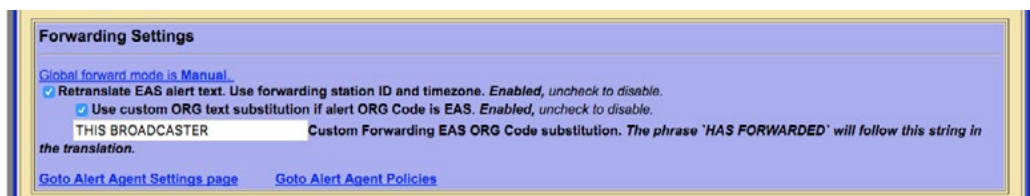
Enter start time, then end time, in hours and minutes.

On days

Check the days the Required Weekly Test could be generated. The RWT will not occur on a day that is unchecked.

Time Configuration Notes

- When configuring the time period, if first time is greater than the second time, the alert will be scheduled at a random time from 0 hrs. Midnight to second time or first time to 23:59. If the first time period is less than the second, the alert will be scheduled at a random time between the first and the second time entry.
- A random Automatic Weekly test is only scheduled if no weekly tests have been originated during the current week (Sun-Sat).
- If changes are made, a previously scheduled weekly test must be manually cancelled before a new test will be scheduled within the new time frame. Go to **Alert Events > Originated Alerts** to view and/or cancel any scheduled originated alerts.



Forwarding Settings

Retranslate EAS alert text. Use forwarding station ID and time zone

To retranslate the EAS alert text, check the box. When not checked the decoded translation will be used.

Use custom ORG text substitution if alert ORG Code is EAS

When checked a text field appears for a custom originator code (ORG). Enter the desired EAS ORG code.

Simultaneous Station Override (MultiStation Mode)

MultiStation mode option enables one EAS device to provide complete EAS coverage for up to five co-located stations or program streams with individual station ID's and logging. GPIO's can be set for each stream according to Station ID, FIPS and/or Event Code. A good portion of the MultiStation specific settings are configured within the **Setup > Station** screens. After the MultiStation license key is installed, the **Main** sub-tab is re-titled **Simultaneous Station Override** and one 'Station' sub-tab is added for each station. A MultiStation 2 will add **Station 1** and **Station 2** sub-tabs while MultiStation 5 will add **Station 1**, **Station 2**, **Station 3**, **Station 4**, and **Station 5** sub-tabs.

The screenshot shows the 'Simultaneous Station Override' configuration interface. At the top, there are tabs for 'Global Options', 'Simultaneous Station Override', and five individual station tabs labeled '1.Station.1' through '5.Station.5'. The main content area is titled 'Multistation Interface Configuration' and contains several sections:

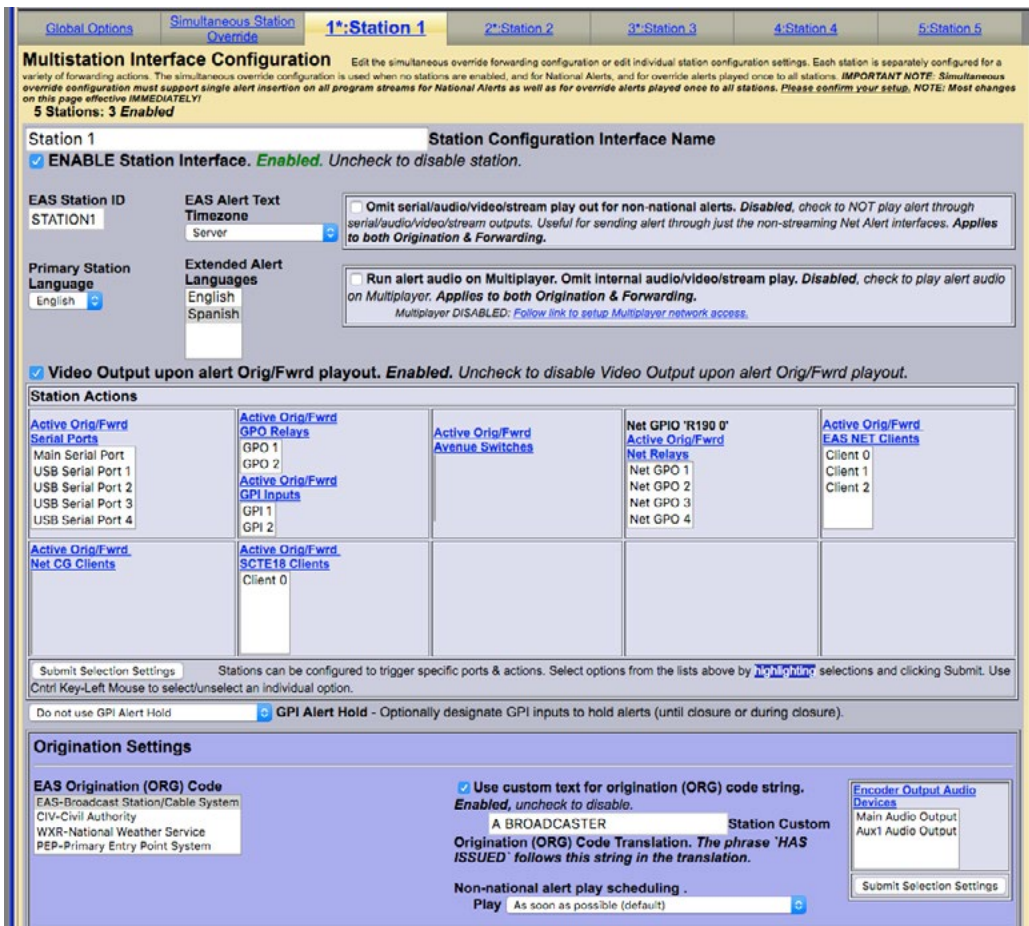
- Simultaneous Station Override Configuration:** Includes fields for 'EAS Station ID WME', 'Uses Server Timezone: Mountain', 'Primary Alert Language: English', and 'Extended Alert Languages: English, Spanish'. There is a checkbox for 'Omit serial/audio/video/stream play out for non-national alerts' and a 'GPI Alert Hold' section.
- Origination Settings:** Includes 'EAS Origination (ORG) Code' (set to 'A BROADCASTER'), a checkbox for 'Use custom text for origination (ORG) code string', and 'Non-national alert play scheduling' set to 'Next 10 sec interval'.
- Weekly Test Settings:** Includes a 'FIPS Group' dropdown menu with a list of locations: Western NY, Erie, NY (036029), Genesee, NY (036037), Livingston, NY (036051), Monroe, NY (036055), Niagara, NY (036063), Orleans, NY (036073), and Wyoming, NY (036121).
- Forwarding Settings:** Includes a checkbox for 'Retranslate EAS alert text' and 'Use custom ORG text substitution if alert ORG Code is EAS', with a field for 'THIS BROADCASTER'.

Simultaneous Station Override Sub-Tab

The **Simultaneous Station Override** sub-tab has the same controls as the **Main** sub-tab did. The simultaneous override configuration settings are used when no stations are enabled, for national alerts, and for override alerts played once to all stations. **Weekly Test Settings** are only available in this sub-tab if every station sub-tab is disabled.

Station 1 – 5 Sub-Tabs (MultiStation Mode)

Station sub-tabs are displayed when a valid MultiStation license key is enabled. MultiStation 2 will add 2 station sub-tabs and MultiStation 5 will add 5 station sub-tabs. Each Station sub-tab has the exact same controls as the others – enabling users to make configuration for each channel individually. All Station sub-tabs screens contain three sections: general station settings, Origination Settings, and Forwarding Settings.



Station 1 Sub-Tab

The majority of the Station sub-tab configuration settings are described in the Main Sub-tab (above). The following descriptions will highlight specific differences.

Multistation Interface Configuration

Station Configuration Interface Name

Text field that labels the Station sub-tab. The purpose of this name is to label the sub-tab and is not used or included in any EAS alerts messages. Each Station sub-tab starts with a number (1-5) and colon (:) along with a default name of 'Station' followed by a number. In the above example the Station Configuration Interface Name is 'Station 1' and is displayed on the sub-tab as '1*:Station 1'. The asterisk (*) denotes that the Station Interface is enabled for that station.

ENABLE Station Interface

This check box enables the station interface for this sub-tab. Checking it will make the following configuration settings active.

EAS Station ID

Type up to 8 characters in this text field to identify the Station ID for this sub-tab. This code is included in all originated alerts, both manually forwarded and automatically forwarded alerts.

EAS Alert Text Timezone

The MultiStation mode allows stations in differing time zones to be configured in the same EAS unit. The default setting is 'Server' which maintains the same time zone that was configured in the **Setup > Time** screen. To change to a different time zone, click the pull-down menu and click the desired selection.

Primary Station Language

This pull-down menu is to select the primary alert language for this sub-tab. Select from the list of available languages.

Extended Alert Languages

A list of available extended alert languages is displayed within this box. Select one language by clicking it. Multiple languages may be selected by using the CTRL key when making additional selections.

Omit serial/audio/video/stream play out for non-national alerts

Check to NOT play alert through serial/audio/video/stream outputs. Useful for only sending alert through non-streaming Net Alert interfaces. Applies to both Origination and Forwarding.

Run alert audio on Multiplayer

Due to the limited number of audio outputs in relation to the number of stations controlled by the EAS device in MultiStation mode, Digital Alert Systems/Monroe Electronics provides an optional MultiPlayer. The MultiPlayer is a separate 1RU chassis that provides up to 5 completely independent EAS audio channels playable at any time. To enable the play out of EAS audio from a MultiPlayer, check this box.

Video Output upon alert Orig/Fwrld payout

For EAS units with internal Video Out; when checked, this setting will utilize the internal video output to generate a full screen alert page for this station.

Station Actions

This section represents a series of serial, GPIO, EAS Net, NET CG's, and SCTE-18 client configuration settings for this station. Select the appropriate settings and click the **Submit Selection Setting** button. Multiple selections can be made by using the CTRL key when making selections.



Note

A MultiPlayer will require proper setup prior to being configured in this screen. Follow the Quick Start Guide included with the MultiPlayer before checking this box.

Station Sub-Tab Origination Settings Section

Origination Settings

The Origination Settings are exactly the same with the exception of the **Encoder Output Audio Devices** settings.

Encoder Output Audio Devices

A list of available encoder output audio devices is presented. Select the desired output and click the **Submit Selection Settings**. Multiple selections can be made by using the CTRL key when making selections.

It is important to note that automatic random **Required Weekly Tests** may be generated for each enabled station. This interface gives users the ability to generate those random RWT's on differing time and day schedules.

Forwarding Settings

Retranslate EAS alert text. Use forwarding station ID and timezone. *Enabled, uncheck to disable.*
 Use custom ORG text substitution if alert ORG Code is EAS. *Enabled, uncheck to disable.*
THIS BROADCASTER Station Custom Forwarding EAS ORG Code substitution. *The phrase 'HAS FORWARDED' will follow this string in the translation.*

Forwarding Audio Output Devices
Main Audio Output
Aux1 Audio Output
Submit Selection Settings

Station Auto-Forwarding Configuration
Global override station auto-forwarding must be enabled to allow station level auto-forwarding. Station level alert auto-forwarding timers are optional. Station level auto-forwarding properties are configured on the Setup > Alert Agent™ pages!

Global forward mode is Auto.
 Auto forward alerts when global auto-forward mode is selected. *Enabled, uncheck to disable and force this station to require manual forward.*

Forward Mode Timer 1. Enabled. **ACTIVATED!**
0 : 0 : Auto Forward Mode Start Time
Hrs:Mins
23 : 59 : Auto Forward Mode Stop Time
Hrs:Mins
 Daily Weekday Weekend

Forward Mode Timer 2. Enabled. **Not Activated**
0 : 0 : Auto Forward Mode Start Time
Hrs:Mins
23 : 59 : Auto Forward Mode Stop Time
Hrs:Mins
 Daily Weekday Weekend

Accept Time Changes Cancel Time Changes
[Goto Alert Agent Settings](#) [Goto Alert Agent Policies](#) [Goto EAS Group setup](#) [Goto FIPS Group setup](#)

Station Sub-Tab Forwarding Settings Section

Forwarding Settings

The Forwarding Settings are exactly the same with the exception of the **Forwarding Output Audio Devices** settings.

Forwarding Output Audio Devices

A list of available forwarding output audio devices is presented. Select the desired output and click the **Submit Selection Settings**. Multiple selections can be made by using the CTRL key when making selections.

Station Auto-Forwarding Configuration

Auto-Forward mode timers may be configured for each station to accommodate differing program schedules. These control settings are described in detail in the **Setup > Station > Main** screen.

DEMO/PRACTICE SETUP

This page allows you to enable the Practice/Demo operation mode. You can configure alert parameters for a practice and test run of decoding and forwarding. By generating a trial decoded DMO (Demo/Practice Warning) alert, rather than having to wait until an actual alert is received, you can simulate the behavior of any incoming decoded alert on the EAS DEVICE. The actual alert is generated within the **Alert Events > Incoming/Decoded Alerts** screen. (See [Chapter 6 - Incoming/Decoded Alerts](#) for more details). Once generated, all the forwarding buttons and edit/review options for the active alert are available for operation. This feature is especially useful for testing MultiStation operation.

Options on this page configure availability of the Run DEMO button, and FIPS codes and audio for the DMO alert.



Warning

BE CAREFUL! Forwarding any Demo/Practice Warning (DMO) will take it to AIR. Examine if Auto-Forward Mode is enabled before use. Make sure your EAS broadcast system is off line during practice.

Demo/Practice Screen

Configure One-Button DEMO/Practice and Forwarding Test

Allow DEMO Decode/Forwarding Test

When enabled, the **Add Demo Decoded Alert** button is available on the **Alert Events > Incoming/Decoded Alerts** screen.

Set FIPS locations for One-Button DEMO Test

This list is used to select the FIPS codes for the DEMO alert. The list is generated from the **Configure Available FIPS for Encoder Alert Origination** section of the **Setup > Alert Agent™ > FIPS Groups** screen. If a FIPS code is not available from the list, follow the **FIPS list can be configured** hyperlink to add the FIPS code to the available FIPS list.

Select a FIPS code from the list and click the **Add Selected FIPS** button to add to the **Current FIPS locations for One-Button DEMO Decode/Forwarding Test**. Multiple selections can be made using the CTRL key when making selections or they can be added one at a time.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but likely not very common.

Current FIPS locations for One-Button DEMO Decode/Forwarding Test

Contains a list of FIPS codes intended for use with the Demo/Practice Warning test. Each FIPS code has a pull-down menu for subdividing the FIPS location. The default value is 'All'. To delete a FIPS code from this list, click the corresponding **Remove** button.

Roll EAS station IDs three times

When checked, will roll EAS station ID three times. Left unchecked, EAS station ID will roll once.

Preempt an in-progress alert announcement as a test

Check to enable. Make sure blocking during in-progress alert announcements is disabled to run this test. This setting requires Administration-level permission to enable. All other users will see grayed text.

When DMO event is forwarded, forward live and bypass criteria (like EAN, NPT)

Will simulate a national live alert. This setting requires Administration-level permission to enable. All other users will see grayed text.

Select Alert Audio Message

This selector allows an audio message file to be selected for the audio message portion of the DMO alert.

Under the Select Alert Audio Message pull-down menu, a hyperlink labeled **To upload audio files goto Setup Audio Output Levels and Tests** is provided to go to the **Setup > Audio Output Levels/Tests** screen where users can upload and listen to the available audio files (See the [Audio Setup](#) section of this chapter).

A link labeled **To Run Demo alert goto Alert Events Incoming/Decoded Alerts** is provided to go to the Incoming/Decoded Alerts screen within the Alert Events tab. Demo/Practice alerts may be added and forwarded from this location.

Allow *Forward active RMT with original decoded audio* GPI to forward this Demo alert

This option allows an unforwarded DMO (Practice/Demo Warning) alert to be forwarded by the ***Forward active RMT with Original decoded audio*** GPI.

EAS Origination (ORG) Codes

Displays a list of available EAS Origination (ORG) Codes. Select one of the codes by clicking on it. This code will be used with the Demo/Practice EAS message.

NET ALERTS SETUP

There are up to six sub-tabs within the **Setup > Net Alerts** page. Valid license keys will display the appropriate sub-tabs.

Sub-Tab	Description
DVS168	Configuration of a single DVS-168/EARS client for sending EAS alerts..
EAS NET	Provides a variety of methods to exchange data (including alert notifications) between EAS devices and other remote hosts. Includes support for multiple DVS-168 network clients. This sub-tab replaces the DVS168 sub-tab (above) when enabled. Requires valid EAS NET and Encoder license keys.
CAP Decode	Enables communication with Common Alerting Protocol (CAP) servers such as FEMA's IPAWS. Requires a valid CAP Plus license key.
DVS644 (SCTE18)	Offers communication with edge decoders and some of the latest digital set-top-boxes to send alert messages. This, in conjunction with Stream MPEG, provides a complete digital solution in one box for cable EAS requirements. Requires a valid DVS644 (SCTE18) license key.
Stream MPEG	An EAS device can uni-cast or multicast an MPEG2 video/audio details page. Requires a valid Stream MPEG 1/2 license key.
Net CG	Communication with network-based character generators is configured via this interface.
Net Switch	Network-based control of external switching devices.
Net GPIO	External GPIO devices are configured and controlled through this interface. DASDEC Only.
Hub Controller	External GPIO devices are configured and controlled through this interface. One-Net Only.

Most of the Net Alert interfaces can be separately enabled / disabled per feature and per client interface. The standard Networked GPIO supports FIPS programmable LAN based relay triggering during alerts and alert states.

If a required network interface is not available, it can be enabled using the License Key Manager interface under **Setup > Server > Main/License**. (See the [Server Setup - Main/License](#) section of this chapter) License keys may be purchased from Digital Alert Systems/Monroe Electronics.

All of the **Setup > Net Alerts** options require the use of the **Accept Changes** button for submitting changes.

MultiStation mode: When MultiStation mode is enabled, the Net Alert client interfaces used per station are selectable. A station can choose to NOT use an enabled Net Alert interface. The station assignment options do not allow reprogramming of a Net Alert interface – just its inclusion. Also, the specific included Net Alert interface MUST be enabled for the station to be able to trigger its action. This allows specific Net Alert interfaces to be assigned to different stations and thereby trigger a Net Alert action only when a specific station is active. Configure individual station Net Alert assignments within the desired station sub-tab screen under **Setup > Station**.

DVS 168

The DVS168 sub-tab provides an interface to a single DVS-168 client. If the DVS-168 sub-tab is available, use this screen to enable this protocol for forwarding and/or sending alerts.



Note

For configurations requiring more than a single DVS-168 interface, an EAS NET license key is needed.

DVS168 Sub-tab

Alert Forwarding to DVS168/EARS device.

Placing a check in this box will allow received EAS alerts to be forwarded through the EAS device and sent out using the DVS-168 protocol. A gray **DVS168/EARS client 1 connection info** interface will be displayed when this options is checked.

Encoder Alert Send to DVS168/EARS device.

Placing a check in this box will allow originated alerts to be sent out using the DVS-168 protocol. If not already displayed, a gray **DVS168/EARS client 1 connection info** interface will be displayed when this option is checked.

Alert Forwarding and sending to DVS168/EARS Client

Once forwarding and/or sending have been enabled, four information fields must be configured to identify the DVS-168/EARS host. See above screenshot. Enter the IP address, the IP port, the FTP user and password, select Audio File Sample Size, and the Audio File Sample Rate (Default is 16000 Sample/sec). Alerts with all FIPS codes can be forwarded by placing a check mark in the box to enable all FIPS to trigger DVS168/EARS device. Alerts for specific FIPS areas can also be filtered/ passed through the protocol. Remove the check mark from the box that says

All FIPS codes trigger the DVS168/EARS device to enable FIPS forwarding control. When configured, select a FIPS codes group that will be used to check against the incoming forwarded alert. If any of these FIPS are included in the incoming forwarded alert, the alert will be sent to the DVS-168 client.

Remove the check mark from the box that says All EAS codes trigger the DVS168/EARS device to enable EAS forwarding control. When configured, select an EAS code group that will be used to check against the incoming forwarded alert. If any of the EAS codes are included in the incoming forwarded alert, the alert will be sent to the DVS-168 client.

When an alert is forwarded to a DVS-168 client, a WAV file of the EAS audio and a text file of the alert details are constructed. These are FTP'd to the DVS-168 client. A socket is temporarily opened from the EAS device to the DVS-168 client, and a control message is sent that describes the alert. The Operation Log will log each of these actions and their success/ failure.

EAS NET

There are three sections on the EAS NET sub-tab: EAS NET Decoding, Web audio streaming, and EAS NET Clients.

Configure EAS NET Decoding

EAS Net Decoding is included with the EAS NET license key.

Basic Operation

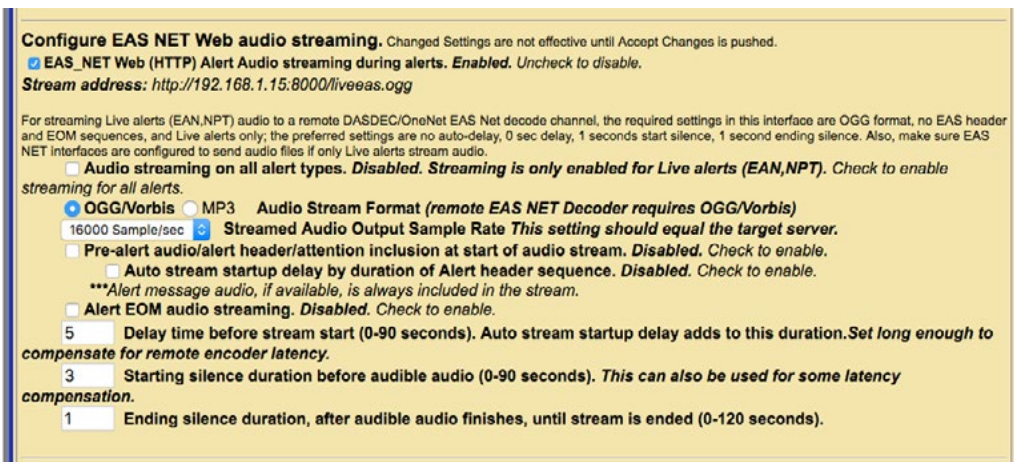
EAS NET operates by sending optional audio, optional text translations, and an EAS event notification file from an EAS device to a remote device over LAN or WAN. There are some differences depending on the chosen EAS NET protocol. SSH STDIN Only does not offer sending of digital audio WAV files or text translations. DVS-168, a legacy protocol, does not send the same type of event notification data as the other protocols. For everything but DVS-168, the remote host/server device is sent as an event text file or ASCII data sequence that contains a set of key value style data lines describing the EAS alert. For every protocol but SSH STDIN Only and DVS-168, the text event file by default is copied into the remote host file EAS_NET_ALERT under the remote user home directory. This filename and path can be overridden when configuring the client schema file. A standard set of information fields is sent in the text file, but the actual names of the keys can be custom edited per client according to a programmable schema. Each client can be set to use the Default or a custom edited schema. The EAS device EAS NET client interface provides a schema editor to create specialized schemas.

EAS NET Decoding Section

There is only one check box button to enable EAS NET decode. Check the check box labeled **EAS_NET decode from remote EAS NET sending devices**. The EAS device will then be able to receive alerts sent via EAS NET send from a properly configured remote EAS device. EAS NET decoded alerts are clearly labeled in the **Alert Events > Incoming/Decoded Alerts** screen as being received from input channel EAS NET. The alert event files are stored in a separate disk storage area from audio decoded alerts. Other than those differences, EAS NET decoded alerts are handled the same as alerts decoded from the audio inputs. Click the **Accept Changes** button to save changes.

Configure EAS NET Web audio streaming

EAS Net Client Web audio streaming is included with the EAS NET license. This provides a convenient way to stream live alert audio over a network. This is used primarily to provide live EAN/NPT audio from EAS NET sent to an EAS NET client device (including another EAS device). The stream is not an MPEG transport stream. It is an http audio stream. Remote clients must actively load the URL for the stream in order to play it. This can be done via most modern media players. An EAS device with EAS NET decode will automatically use this audio stream as a live input for EAS audio as needed. Refer to the screen shot below.



EAS NET Web Audio Streaming Section

EAS_NET Web (HTTP) Alert Audio streaming during alerts

Enable this check box to generate live web streamed audio during alerts. The default values of the options are designed to work for EAN/NPT.

Audio Streaming on all alert types

This check box controls audio streaming for National Alerts (EAN/NPT) or all alert types. For testing purposes, the check box **Audio streaming on all alert type** can be enabled to allow all alert types to have audio streaming. Make sure to use this button to test live audio for any remote EAS device EAS NET decoder.

Audio Stream Format

You can select either OGG/Vorbis or MPEG Layer 3 (MP3) audio. For audio to a remote EAS device EAS NET decoder, use OGG.

Audio Output Sample Rate

The correct value for this depends on the destination. For audio to a remote EAS device EAS NET decoder, use the output sample rate selected on the remote EAS device. Choices are 16000, 32000, 44100, and 48000 samples/sec.

Pre-Alert audio/alert header/attention inclusion at start of audio stream

Alert EOM Audio Streaming

These three check box options are included for control of the total content of the alert audio that is streamed. For purposes of this interface, alert audio consists of three parts:

- Pre-Alert audio/EAS Alert FSK header/Alert Attention signal
- Alert audio voice message
- Alert FSK EOM audio

No matter the choices, the second part, alert audio voice message, if it exists, is always streamed. Any combination of these options will work when streaming to a remote EAS device EAS NET decoder. The default is to not stream the header or EOM sequence, just the audio voice message. Use the options as required by the specific application on a remote server.

To review, the options allow the inclusion/exclusion of:

- Pre-Alert audio/EAS Alert FSK header/Alert Attention signal
- EAS alert FSK EOM

Delay time before stream start, Starting silence duration, Ending silence duration

These options allow streaming to be delayed by the duration of the alert header. Three numeric text fields allow entry of three additional audio delay components. Each delay is in seconds and applies to a specific location during the audio stream. Use as needed for the specific application.

Configure EAS NET Clients

Two check boxes are displayed for enabling EAS_NET during alert forwarding and origination.

Forwarded Alerts can be sent to EAS_NET devices

This check box enables EAS_NET send processing during alert forwarding. It can be enabled / disabled at any time.

Encoder Originated Alerts can be sent to EAS_NET devices

This check box enables EAS_NET send processing during alert origination. It can be enabled / disabled at any time.

Decoded Alerts Can be sent to EAS_NET devices

This check box enables EAS_NET send processing during alert decoding. Decoded alerts can be sent to another EAS_NET device without forwarding and putting it on the air.



Note

At least one of these check boxes must be enabled to allow editing of EAS_NET clients.

Configure EAS NET Clients. Except for Add/Delete Clients, changed Settings are not effective until Accept Changes is pushed.

Master Switches

- Forwarded Alerts can be sent to EAS.NET devices. *Disabled.* Check to enable.
- Encoder Originated Alerts can be sent to EAS.NET devices. *Enabled.* Uncheck to disable.
- Decoded Alerts can be sent to EAS.NET devices. *Disabled.* Check to enable.

Configure EAS NET Client Connection

*Client 0 ↓ Select EAS.NET client Add EAS.NET Client Interface (effective immediately)

There is 1 defined client interface (max is 8). Duplicate EAS.NET Client Interface (effective immediately)

15 EAS NET Timeout in seconds (for advanced use only). Delete this EAS.NET interface (effective immediately)

Client 0	Client Interface Name
<input checked="" type="checkbox"/> ENABLE Client Interface. <i>Enabled.</i> Uncheck to disable client.	

Event Data Protocol

- EAS NET
- Common Alert Protocol (CAP) PureCAP™ - Source CAP File PureCAP™ Plus - Embedded Source CAP File
- Advanced Emergency Alerting Table (AEAT) Container

Interface last ran Thu Nov 15 08:47:40 2018: [Click link to see EAS.NET Event data file.](#)

EAS NET only at Orig (omit Fwrd and Decode send) ↓ **EAS NET Event Send Options** (decode send options require Decoded Alerts Master Switch)

- Send EAS NET prior to alert audio payout. *Disabled.* Client syncs EAS NET alert info send with alert audio payout.
- Check to enable EAS NET alert info send prior to alert audio payout.
- EAS NET prior send is only needed with EAS NET compatible equipment that requires sync with alert audio payout via GPI control or Extended Status Play control. Prior send is incompatible with EAS.NET Web audio streaming!
- Send Live alerts (EAN,NPT). *Enabled.* This EAS NET Client forwards Live alerts (EAN,NPT). Uncheck to disable Live alert forwarding.

Event/Ancillary Data IP control options:

192.0.0.185

Remote Host Address

(name if DNS enabled or dot.decimal)

Secure Copy ↓ EAS.NET Event Transfer Protocol

22 Remote EAS NET Host Port

First (Main) Ethernet ↓ Local network device (provides return IP address)

- Automatic internal connection test every 5 minutes. *Enabled.*
- Test connection (Note: Save any config changes before using Test buttons)

dasdec_netin EAS.NET User (if sending to DASDEC, preferred user name is dasdec_netin)

[Follow this link to find SSH Public Encryption Key.](#)

Current Schema DASDEC ↓

[Edit/Review Schema](#) [Delete Schema](#)

[Click on link to see EAS.NET schema data file.](#) See schema for target paths and names of data files.

Ancillary Data File control options:

- Send Composite EAS Audio file. *Disabled.* Composite Audio file will NOT be sent. Check to enable file send.
- Omit composite audio for Live alerts (EAN,NPT). *Disabled.*

Configure EAS NET Client Connection Section

Configure EAS_NET Client Connection

Once enabled, you can create configurations for up to 8 EAS_NET clients. Each client can be independently enabled and disabled, allowing an easy way to stop or restart a client for a specific region.

If no client configurations exist, or if you want a new one and less than 8 clients exist, click the **Add EAS_NET Client Interface** button to create a new interface configuration.

To edit an existing client interface, select the named client from the **Select EAS_NET client** pull-down menu and edit the fields provided in the table underneath.

To delete a client configuration, select the client and click on: **Delete this EAS_NET interface.**

To duplicate an existing client interface (*a different name will be automatically generated; less than 8 clients must exist*), select the **Duplicate EAS_NET Client Interface** button. This is the best way to create new client interfaces that are mostly the same as an existing one except for the IP address.

During alert processing, the Operation Log will log the success or failure of the EAS_NET forwarding/origination action per client.

EAS NET uses a flexible set of LAN communication protocols to send EAS data to a remote device. Generally, the remote device needs to have running software that understands EAS NET files and data formats in order for anything useful to be triggered by an EAS NET event. All EAS NET protocols will send an alert event data notification file or ASCII data string from the EAS device to the EAS NET remote server host. Most protocols allow for sending separate data files (like audio WAV files).



Caution

EAS_NET client configuration addition, duplication, and deletion is immediate and cannot be canceled.

Various information fields must be configured to identify and correctly communicate to the EAS NET remote client. Common to all are:

Client Interface Name

This text box allows the user to give the client interface a descriptive name. These names appear in the selection list.

Client Enable/Disable

This check box enables and disables the EAS NET client.

Event Data Protocol

Enables the user to configure the desired protocol for the EAS NET client. The available options are:

- **EAS NET** – Digital Alert Systems/Monroe Electronics' exclusive communications protocol software enabling EAS data and audio transmission over a TCP/IP network for up to eight (8) EAS-NET compatible platforms.
- **Common Alert Protocol (CAP)** – standard CAP v1.2 FEMA/IPAWS profile 1.0 text
- **PureCAP™ - Source CAP File** – forwards the original CAP message without modification for separate processing.
- **PureCAP™ Plus - Embedded Source CAP File** – this file wrapper contains only those languages appearing in the original CAP source. If the output languages are not present then EAS NET will not send.
- **Advanced Emergency Alerting Table (AEAT) Container** – protocol used in support of the Advanced Emergency Alerting (AEA) part of ATSC 3.0 - generating a proprietary XML file and sending it to various downstream devices.

Remote Host Address

Displays the IP address of the remote EAS NET host where the EAS NET event info is sent.

EAS NET Event Transfer Protocol

Displays the event transfer protocol (the LAN communication method used to send the alert event data). Depending on the event transfer protocol, other configuration fields may be necessary or optional. Some protocols require passwords, others use encryption keys. Most provide for optional data file connections. The event transfer protocol options are:

- **Secure Copy (SCP)** – Uses the Secure Shell (SSH) network protocol for both the data file transfers and event file transfer. No passwords are needed for any of the Secure Shell protocols (**1.3**). Instead, the EAS device public ssh key id (under /root/.ssh/id_dsa.pub and also displayed at the bottom of the **System > Status > Network** screen) must be added into the remote host's authorized ssh keys list. The keys provide for encrypted data transfer and for secure authentication without a password.
- **Secure Shell STDIN Only (SSH)** – Uses the Secure Shell (SSH) network protocol for the event file transfer. No data files can be sent. This protocol requires that the receiving device read the EAS NET event file from standard input from within the shell script. In such a configuration, SCP and SSH login to the EAS NET user will not present to the remote platform shell.
- **Secure Shell STDIN & Copy (SSH with SCP)** – This is a variation on protocol #2 above. The event file is sent as in #2, but the Web interface will display a field to enter a second user account for sending data files to the remote host. The Secure Shell (SSH) network protocol is used for both transfers.



New Feature

Support for PureCAP Plus is new in version 4.0.



New Feature

Support for Advanced Emergency Alerting (AEA) is new in version 4.0.



Note

The **EAS_NET Event Transfer Protocol** pull-down menu selection will dictate the available configuration settings within this screen. The following configuration setting descriptions represent the most commonly used. Not all settings will be available for the selected EAS_NET Event Transfer Protocol. See **Other possible EAS NET Client Configurations Options** (below).

- **FTP Copy** – Uses the File Transfer Protocol (FTP) network protocol for both the data file transfers and event file transfer. A password is required. FTP does not encrypt or secure passwords during transmission. The password is sent in clear text to the remote host FTP daemon. If security is an issue, do not use or design an FTP based EAS NET scheme. Some FTP daemons refuse passive port connections. Use the provided check box to enable a non-passive connection if needed.
- **TCP Event Notification** – Uses a TCP socket from the EAS device to the remote host to send the alert event file. For sending the optional data files, one of FTP or SSH SCP network protocols can be selected. A valid user account on the remote host must be entered. The information described above for passwords and keys apply, depending upon the chosen data protocol.
- **DVS168/EARS** – This is a special case of EAS NET. A TCP socket is used to communicate an event notification, while FTP is used to send data files.
- **Legacy Mediaroom** – This is a special protocol bundled under EAS NET when the Microsoft® Mediaroom™ option is licensed.
- **Mediaroom2** – This is a special protocol bundled under EAS NET when the Microsoft® Mediaroom™ option is licensed. This is in accordance with the Mediaroom 2.0 software.
- **MINERVA** – This is a special protocol bundled under EAS NET when the Minerva option is licensed. A TCP socket is used to communicate an EAS event notification as per the Minerva protocol.
- **WideOrbit** – This is a special protocol bundled under EAS NET when the EAS NET Automation option is licensed.
- **RCS Nexgen** – This is a special protocol bundled under EAS NET when the EAS NET Automation option is licensed.

Event Data IP control options (or Event/Ancillary Data IP control options)

Remote EAS NET Host IP Address

Enter the host name or IP address of the remote host computer

EAS_NET Event Transfer Protocol

- Secure Copy
- Secure Shell STDIN Only
- Secure Shell STDIN & Copy
- FTP Copy
- TCP Event Notification
- DVS168/EARS
- Legacy Mediaroom
- Mediaroom2
- MINERVA
- WideOrbit
- RCS Nexgen

Remote EAS NET Host Port

The field displays the port on the remote EAS NET host where the EAS NET event info is sent.

FTP Ancillary Data File control options

EAS NET User

Displays the user account name on the remote device. Files sent to the remote host will by default be copied relative to this account home directory.

Current Schema

The schema determines key names of the information fields sent to the EAS NET client's remote host. It also determines file names and paths for any files sent to the remote host. The schema can be edited by clicking on the **Edit/Review Schema** button.

Other possible EAS NET Client Configuration Options

Not all of these options will appear for every EAS NET transfer protocol.

Client sends EAS NET alert info during alert play-out

When this option is enabled (checked) the EAS NET alert info is sent out prior to alert play-out. EAS NET prior send is only needed with EAS NET compatible equipment that depends upon GPI controlled delayed alert play-out.

SSH Public Encryption Key link.

The SSH based protocols provide this link to the display of the EAS device public key. This must be copied to the remote host's authorization file.

Composite Audio File Send

When enabled (checked) a composite WAV file of the entire EAS audio track will be sent as a separate file to the EAS NET client's remote host. File name/path on the remote host are determined by the schema.

EAS Audio File send

When enabled (checked) the individual audio sections of the EAS alert will be sent as separate files to the EAS NET client's remote host. File names/path on the remote host are determined by the schema.

Translation File Send

When enabled (checked) the EAS text Translation will be sent as a separate file to the EAS NET client's remote host. File name/path on the remote host are determined by the schema.

Translation File Newline Control

When enabled (checked) the EAS text Translation has all newline characters removed. When disabled, the EAS text Translation includes newline characters.

Video Start Delay Factor (0-10 seconds)

When set to a non-zero value, this adds delay time to the video start time reported in the EAS NET event file. This can be useful to handle latency between the EAS device and the EAS NET remote host.

Duration Extension Time (seconds)

This allows extra time to be added to the internally calculated duration time in the EAS NET event file. Alert Duration == Audio Duration + Extension Time



Note

The schema does not set the values of the client interface fields.

All FIPS codes trigger. **Disabled.** Specific FIPS Codes control EAS_NET device triggering (EAN,NPT with FIPS 000000 override). Check to enable all FIPS codes triggering of EAS_NET device.

FIPS Group
 Western NY ▾
 Erie,NY (036029)
 Genesee,NY (036037)
 Livingston,NY (036051)
 Monroe,NY (036055)
 8 locations

All EAS codes trigger. **Disabled.** Specific EAS Codes control EAS_NET device triggering. Check to enable all EAS Codes triggering of EAS_NET device.

EAS Group
 Tests ▾
 EAN : NATIONAL EMERGENCY ACTION NOTIFICATION
 NPT : NATIONAL PERIODIC TEST
 RMT : REQUIRED MONTHLY TEST
 RWT : REQUIRED WEEKLY TEST
 4 codes

All incoming alert Station IDs trigger. **Disabled.** Specific Station IDs control EAS_NET device triggering (applies to EAN,NPT). Check to enable any Station ID triggering of EAS_NET device.

Source alert FCC EAS Station IDs criteria string
(only use to match specific incoming alert station IDs; up to 8 character each, separate each source EAS station ID with a | char. eg. STAT1|STAT2 matches for the two FCC EAS station identifiers STAT1 or STAT2). The * character matches all FCC EAS Station ID.

Do not use GPI triggers **GPI Trigger** - Optionally designate GPI inputs/states required to use this net interface.

File system paths and names in EAS NET can include text substitution patterns.
 \$(ID) is replaced with the alert ID. \$(EAS) is replaced with the 3 letter alert EAS code. \$(bstid) is replaced with the Simultaneous Override Encoder Station ID name.
 \$(mstid) is replaced with the Multistation Encoder Station ID name. \$(stidx) is replaced with the alert Station index(0 for base, 1-5 for multistation). \$(ext) For Audio files only, \$(ext) is replaced by the audio file extension (eg. wav or mp3). \$(YY) and \$(YYYY) are replaced with the current year\$(MM) and \$(DD) are replaced with the current month and day.\$(hh),\$(mm),\$(ss) are replaced with the current hours,minutes, and seconds. \$(lang) is replaced by language name.

All FIPS / EAS Codes Trigger Section

All FIPS codes trigger

If enabled, all alert FIPS codes will trigger the EAS NET client interface. In the above screen shot this option is disabled. Set the check box to enable/disable FIPS code filtered trigger control. If disabled, the alert FIPS codes are filtered for at least one specific match as a way to control whether or not EAS NET is triggered. Alerts for specific FIPS areas can be filtered as a way to control whether or not EAS NET is triggered. If All FIPS is disabled, select a FIPS codes group from the **FIPS Group** pull-down menu. That group of FIPS codes are included in the incoming active forwarded/originated alert and the alert will be sent using the EAS NET client. With careful use of this feature, and with multiple clients, one EAS device can serve many different regions at the same time.

When you finish making changes, click **Accept Changes** button to save the configuration.

DVS168/EARS devices

DVS168/EARS can be selected as an option on the EAS NET Event Transfer Protocol selector. See the screen shot below. Like the other EAS NET protocols, the EAS NET remote host IP address and port must be entered. This would be the address and port of the DVS168/EARS server. Standard DVS168 uses FTP to send data files, so an EAS NET FTP user and password value must also be entered for a standard client configuration. However, there is an option to disable the FTP send. This is for servers that do not support handling digital file data but can be alerted by the DVS168 event protocol. If this option is checked the FTP user and password values are not displayed or needed since the audio and video files will not be sent.



Note

Since EAS NET is used in conjunction with third-party management software (on the remote host), configuration details will depend upon the exact third-party solution. Often instructions will be provided by this party. Configure the EAS NET client interface as required.

Configure EAS NET Client Connection

*Client 0 **Select EAS_NET client**
 There is 1 defined client interface (max is 8).
 15 EAS NET Timeout in seconds (for advanced use only).

Add EAS_NET Client interface (effective immediately)
 Duplicate EAS_NET Client interface (effective immediately)
 Delete this EAS_NET interface (effective immediately)

Client 0 **Client Interface Name**
 ENABLE Client Interface. Enabled. Uncheck to disable client.

EAS NET only at Fwms or Orig (omit Decode send) **EAS NET Event Send Options** (decode send options require Decoded Alerts Master Switch)
 Send EAS NET prior to alert audio payout. Disabled. Client syncs EAS NET alert info send with alert audio payout.
 Check to enable EAS NET alert info send prior to alert audio payout.
 EAS NET prior send is only needed with EAS NET compatible equipment that requires sync with alert audio payout via GPI control or Extended Status Play control. Prior send is incompatible with EAS NET Web audio streaming!
 Send Live alerts (EAN,NPT). Enabled. This EAS NET Client forwards Live alerts (EAN,NPT). Uncheck to disable Live alert forwarding.

Live alert (EAN,NPT) EOM options
 Forced EAT-EOM mode: Send DVS168 EAT-EOM at end of EAN,NPT live alerts (provides Cisco DNCS an end force tune command)
 Live alert (EAN,NPT) EOM is given a new message ID. Enabled. DVS168 spec does not mandate this behavior. Use depends on DVS168 server. Cisco DNCS requires this setting to be enabled!

Event Data IP control options:
 Remote EAS NET Host IP Address
 DVS168/EARS **EAS_NET Event Transfer Protocol**
 4098 Remote EAS NET Host Port
 Automatic internal connection test every 5 minutes. Enabled.
 Test connection (Note: Save any config changes before using Test buttons)
 Alert file FTP. Check to disable alert file FTP to DVS168/EARS device.

FTP Ancillary Data File control options:
 EAS_NET User
 EAS_NET Password
 Short file names. Disabled. This supports the original version DVS168 file names. Check to force short file names (under 16 bytes) for Evertz DVS168 compatible equipment.
 Send alert text for Live Alerts (EAN,NPT). Disabled. NOT sending alert text for Live alerts is the Normal Model! Check to FTP the alert text to DVS168/EARS device. Used to for Evertz DVS168 compatible equipment.
 Pre-transfer batch FTP command mode. Disabled. Standard FTP Enabled. Check to enable pre-transfer batch FTP command. Check and configure this if DVS168/EARS connection is being made, but files are failing to transfer.
 Non-Passive, regular FTP port connection. Disabled. **Passive FTP port connection.** Check to enable non-passive, regular FTP port connection. Check this if FTP connection is being made, but files are failing to transfer.
 Voice message only audio file send. Disabled. Sending all EAS audio is the Normal Model! All EAS Audio is sent to this DVS168/EARS device. Check to FTP just the voice message portion of the alert audio to DVS168/EARS device.

Configure EAS NET DVS168/EARS Client Section

Two other options unique to the DVS168 protocol are also provided.

1. To send just the EAS alert audio message, instead of the EAS FSK header and EOM audio and attention audio, use the provided check box. Before using this option, it is important to make sure your local EAS plan allows the FSK audio to be discarded.
2. Alert duration data format: typically in minutes, some DVS-168 interpreters have coded this differently. The selector provides two other interpretations.

The DVS168 protocol does not provide a programmable schema. For DVS168, the data schema is predefined and the schema selection is not displayed. As with the other EAS NET protocols, the Video Start Delay time, the Duration Extension time, and FIPS based net alert triggering are all configurable.

When you finish making changes, click **Accept Changes** to save the configuration.

DVS168/EARS Operation

When a forwarded/originated EAS alert is to be sent using a DVS-168 EAS NET client, a TCP socket is temporarily opened from the EAS device to the DVS-168 remote host. If this succeeds, and the alert is a non-national alert (and FTP is enabled), a WAV file of the EAS audio and a text file of the alert details are FTP'd to the DVS-168 remote server host. Then a control message is sent over the TCP socket that describes the alert and provides names for the data files. For non-national alerts, this is the only notification by TCP needed. For EAN and NPT national alerts, the audio is not generated or sent, since EAN/NPT alert audio is live and of undetermined duration. When the alert ends, a second control message is sent over the TCP socket to signal the end of the national alert. After this, the socket connection is "torn-down." The Operation Log will log each of these actions and their success or failure.

CAP Decode

There are two sections to configure in the CAP Decode sub-page: **Configure Common Alerting Protocol (CAP) Decoding** and **Remote CAP Server Setup**.

Configure Common Alerting Protocol (CAP) Decoding. Effective when Accept Changes is pushed.

CAP decode. *Enabled. Uncheck to disable.*

[See all CAP messages.](#) [See all EAS from CAP messages.](#) [See errored CAP messages.](#)

View Global CAP options (uncheck to remove view).

Logging options(Note: These options can dramatically increase log size. None are required.):

- Log storage location of CAP alerts. *Enabled. Uncheck to disable.*
- Log duplicate CAP alerts. *Disabled. Check to enable.*
- Log Non-Public (Restricted & Private) message reception. *Disabled. Check to enable.*
- Log Non-EAS messages for EAS inputs. *Disabled. Check to enable.*

Other options:

- Move unrecognized XML to error folder. *Disabled. Recommended only for troubleshooting. Check to enable.*

Remote CAP server setup.

DNS is Enabled (75.75.75.75)

*IPAWS CAP

There are 2 defined client interfaces (max is 10).
Decode Channel: 'CAP1'

IPAWS CAP	Client Interface Name
<input checked="" type="checkbox"/> ENABLE Client interface. <i>Enabled. Uncheck to disable client.</i>	

CAP Decode Sub-Tab



Note

To quick connect to the FEMA CAP Server and the Canadian NAAD system, see [instructions](#) located at the end of this section.

Configure Common Alerting Protocol (CAP) Decoding

CAP Decode

This check box enables or disables CAP decoding for the EAS device. Set it to enable to see all of the available options for CAP Decoding.

View Global CAP Options

This section of the web interface deals with logging and XML file handling.

Log storage location of CAP alerts

Will log the storage location of incoming CAP alerts.

Log duplicate CAP alerts

Duplicate CAP alerts will be logged separately.

Log Non-Public (Restricted & Private) message reception

Enables the logging of non-public CAP alerts

Log Non-EAS messages for EAS inputs

Non EAS messages will be logged

Move unrecognized XML to error folder

When an unrecognized XML file is detected, it is placed in the error folder. This option is recommended for trouble shooting purposes.

Remote CAP Server Setup Section

Remote CAP Server Setup

Select CAP Input Client

This pull-down menu allows you to choose which CAP client you are configuring. The default clients are: CAP PUSH INPUT and HTTP Get Client1.

The CAP PUSH INPUT is available if you want to Receive CAP Alerts from a remote push server. Note: this option is not used often as FEMA would have to know all of the specific IP addresses that it was pushing CAP Alerts to. Because FEMA does not know your EAS devices' IP Address location, it is not going to push an alert to you this way. **It is recommended that this client interface is disabled.**

For the HTTP Get Client1 default option, you can choose between a few CAP Polling Protocols. Choose between HTTP, HTTPS, SSH and the IPAWS Open 2.0 option.

Add, Duplicate and Delete this CAP Interface

These buttons add a new CAP Client Interface - duplicate the one that is currently being edited, or delete the one that is currently being edited.

Client Interface Name

Choose a name for the specific Client Interface that you will configure.

ENABLE Client Interface

Check this box in order to enable the configured or new client to become active to EAS NET CAP Alerts.

CAP Poll Protocol

Choose between HTTP, HTTPS, SSH and the IPAWS Open 2.0 option.

- **WWW HTTP Get (Web URL)** - Use this option to poll from a WWW Server (CAP XML, EDXL-DE, NOAA Atom, RSS pages).
- **WWW Secure HTTPS Get** - Use this option to poll a WWW HTTPS Secured Server (CAP XML, EDXL-DE, Atom, RSS)
- **Secure Shell Get** - Use this option to poll a SSH Server (CAP XML, EDXL-DE, Atom, RSS)
- **IPAWS Open 2.0 Get** - IPAWSOPEN provides access to national and localized CAP formatted EAS alerts. Enter the web host address (without https or http; e.g. apps.fema.gov and you must have DNS enabled to connect). A default IPAWS URL path and internal manufacturer specific PIN is provided. Admin users can view and edit the URL path and other options under the advanced option setup.

Under each of those polling options are very similar credentials that need to be filled out in order to connect to the servers. The following list will show most of those options.



CAP Server Connection Status

The green and red text just below the **Poll CAP from IPAWS Open 2.0 Server** text displays the current status of the CAP server connection (Connected or Not Connected) along with the amount of up or down time. While in the Connected state, the interface will display the time and date of the last received alert.

CAP Server Host Address

This is the address of the server that you want to receive CAP Alerts from. In order to use a URL, a DNS connection must be enabled. Go to Server Network Configuration section at **Setup > Network** to change your DNS options or use the hyperlink.

URL path portion and/or remote path and file name

Put the URL path of the server that you want to receive CAP Alerts from.

Poll Interval in Seconds

This is the number of seconds the EAS device will take before it checks for another CAP Alert.

Assigned Station ID

Use this value to give the server that you are receiving CAP Alerts from an ID that will appear on the log of Decoded alerts.

CAP alerts with any FIPS codes will be converted to EAS

This option, when enabled, will convert CAP Alerts that are sent to any FIPS location to EAS on the EAS device. It is recommended this option be **DISABLED** as you won't need to know all of the cap alerts that are going on around the country. When this option is disabled, enter the desired FIPS Group. The FCC requires reception of CAP Alerts for your county, and your entire state - not every specific county in the state, but the option that gives you the entire state FIPS code.

Quick Connect to IPAWS CAP Server

To quick connect to the FEMA CAP Server, create a new client and follow the options in the screen shot below.

1. Navigate to the **Setup > Net Alerts > CAP Decode** screen
2. Ensure DNS is enabled (**Setup > Network**)
3. Click the **Add CAP Client Interface** button (just below the *DNS is Enabled* text)
4. Enter a descriptive name in the **Client Interface Name** field (i.e. IPAWS)
5. Select **IPAWS Open 2.0 Get** from the **CAP Poll Protocol** pull-down menu
6. Within the **Poll CAP from IPAWS Open 2.0 Server** section:
 - a. Enter **apps.fema.gov** in the **CAP IPAWS server host address** text field
 - b. Enter **IPAWSOPEN_EAS_SERVICE/rest/update** in the URL path text field
7. Click the **View Advanced Options** check box
 - a. Select **IPAWS_Valid-until-11-08-2019.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu
8. Select the desired FIPS Group
(This FIPS Group should include the United States code [000000], your state's code, and any county codes for your service area.)
9. Click the **Accept Changes** button
10. Check to see the EAS device is connected. Green text under the **Poll CAP from IPAWS Open 2.0 Server** section header should read **✓ Connected**.



New Feature

FEMA has updated their XML Digital Signature Certificate Authority (CA) Name. The new CA has been added to version 4.0.

The screenshot shows the 'CAP server configuration' interface. It includes sections for 'CAP Input client', 'Client Interface Name', 'CAP Poll Protocol', 'Poll CAP from IPAWS Open 2.0 Server', 'View Advanced Options', and 'FIPS Group'. Numbered callouts (1-10) highlight specific configuration steps: 1. 'DNS is Enabled (75.75.75.75)'; 2. 'Add CAP Client Interface' button; 3. 'Add CAP Client Interface' button; 4. 'Client Interface Name' field; 5. 'IPAWS Open 2.0 Get' selection; 6. 'Poll CAP from IPAWS Open 2.0 Server' section with 'Connected' status; 7. 'View Advanced Options' checked; 8. 'XML Digital Signature Certificate Authority (CA) Name' dropdown; 9. 'Accept Changes' button; 10. 'CAP IPAWS server host address' and 'URL path' fields.

IPAWS CAP Server Interface Screen

Quick Connect to NAAD CAP Server (CAP Canada)

To quick connect to the Canadian **National Alert Aggregation and Dissemination (NAAD)** system server, create a new client and follow the options in the screen shot below.

1. Navigate to the **Setup > Net Alerts > CAP Decode** screen
2. Ensure DNS is enabled (**Setup > Network**)
3. Click the **Add CAP Client Interface** button (just below the *DNS is Enabled* text)
4. Enter a descriptive name in the **Client Interface Name** field (i.e. NAAD)
5. Select **CAP Canada IP Get** from the **CAP Poll Protocol** pull-down menu
6. Enter **streaming1.naad-adna.pelmorex.com** in the **CAP Canada NAAD server host address** text field
7. Enter **capcp1.naad-adna.pelmorex.com** in the **NAAD previous alert download host name** text field
8. Select **Pelmorex-digicert-verisign-symantic-ENVCAN-CA.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu
9. Click the **Accept Changes** button
10. Check to see the EAS device is connected. Green text under the **Poll Canada CAPCP from NAAD IP Server** section header should read **✓ Connected**.

The screenshot shows the 'CAP server configuration' page. At the top, a green box labeled '2' highlights 'DNS is Enabled (192.0.0.1)'. Below it, a button labeled '3' says 'Add CAP Client Interface'. A section labeled '4' shows 'Client Interface Name' set to 'NAAD'. A section labeled '5' shows 'CAP Poll Protocol' set to 'CAP Canada IP Get'. A section labeled '6' shows 'CAP Canada NAAD server host address' set to 'streaming1.naad-adna.pelmorex.com'. A section labeled '7' shows 'NAAD previous alert download host name' set to 'capcp1.naad-adna.pelmorex.com'. A section labeled '8' shows 'XML Digital Signature Certificate Authority (CA) Name' set to 'Pelmorex-digicert-verisign-symantic-ENVCAN-CA.crt'. A section labeled '9' shows the 'Accept Changes' button. A section labeled '10' shows a green checkmark and 'Connected' under the 'Poll Canada CAPCP from NAAD IP Server' header.

CAP Canada / NAAD Server Interface Screen



New Feature

Canadian authorities have updated their XML Digital Signature Certificate Authority (CA) Name. The new CA has been added to version 4.0.



Attention

Enabling the **Honor EnvCan Broadcast Intrusive requests** setting should only be exercised in coordination with Environment Canada. Do not check/enable this feature prior to consulting with EnvCan.



Attention

The **Honor SOREM Broadcast Immediate requests** setting should be checked/enabled in compliance with Canadian CLF guidance.



Attention

Check/enable the **Only process alerts with EnvCan Broadcast Intrusive or SOREM Broadcast Immediate** if it is intended to **ONLY** transmit messages designated as Broadcast Immediate by alerting authorities.

DVS644 (SCTE18)

Configure DVS644 (SCTE-18) Clients

DVS644/SCTE18 is a SCTE standard for encapsulating EAS alert data into an MPEG transport stream format (as an MPEG system table) for delivery to MPEG client devices (such as set-top boxes and cable ready TVs). The EAS device has a sophisticated and powerful implementation of this standard.

This feature requires the DVS644/SCTE18 license. When DVS644/SCTE18 support is available on the EAS device, the sub-tab for this feature appears under **Setup > Net Alerts**. Two check boxes are displayed for enabling DVS644/SCTE18 during alert forwarding and origination.

Alert Forwarding to DVS644/SCTE18/CEAM devices

Enabling this check box allows SCTE18 send processing during alert forwarding.

Encoder Originated Alerts Sent to DVS644/SCTE18/CEAM devices

Enabling this check box allows SCTE18 send processing during alert origination.

At least one of these check boxes must be enabled to allow editing of DVS-644/SCTE18 clients. In the screen shot below, the Alert Forwarding is enabled.

If either of the first two check boxes are enabled, the **Configure DVS644(SCTE-18) CEAM Client Connection** interface appears allowing the user to add and configure a DVS644(SCTE18) client.

Add DVS644(SCTE-18) CEAM Client Connection

Clicking this button will enable the user to create, configure, and manage a single or multiple DVS644(SCTE18) client(s).

Use Audio Delay

This check box will also appear allowing the audio to be delayed so as to synchronize the audio and video content. The Audio Delay setting is found in **Setup > Audio > Decoder Audio** at the bottom of the screen – Alert audio delay.

The screenshot shows the 'Configure DVS644(SCTE-18) Clients' interface. At the top, there are navigation tabs: EAS NET, CAP_Decode, **DVS644 (SCTE18)**, Net.CG, Net_Switch, and Hub_Controller. Below the tabs, the main content area is titled 'Configure DVS644(SCTE-18) Clients. Except for Add/Delete Clients, changed Settings are not effective until Accept Changes is pushed.' It contains several sections: 1. Alert Forwarding: A checked checkbox 'Alert Forwarding to DVS644/SCTE-18/CEAM devices. Enabled. Uncheck to disable.' and an unchecked checkbox 'Encoder Originated Alert Sent to DVS644/SCTE-18/CEAM devices. Disabled. Check to enable.' 2. Use Audio Delay: A checked checkbox 'Use Audio Delay. Enabled. DVS644/SCTE 18 message send is delayed by Alert audio payout delay time. This allows a time delay for DVS644/SCTE 18 synchronization to video/audio. Uncheck to disable use of alert audio payout delay. Applies to both origination and forwarding. Audio Alert delay is 6 seconds. Follow link to modify.' 3. Configure DVS644(SCTE-18) CEAM Client Connection: A sub-header '(client IP & program values apply to both Origination and Forwarding)'. It includes a dropdown for 'Client 0', a 'Select DVS644 client' button, and three buttons: 'Add DVS644(SCTE18) Client Interface (effective immediately)', 'Duplicate DVS644(SCTE18) Client Interface (effective immediately)', and 'Delete this DVS644(SCTE18) interface (effective immediately)'. Below this, it states 'There is 1 defined client interface (max is 64)'. 4. Client 0 Configuration: A section for 'Client 0' with a 'Client Interface Name' field. It has a checked 'ENABLE Client Interface. Enabled. Uncheck to disable client.' checkbox. Fields include: 'Remote Host Unicast or Multicast IP Address' (empty), 'Remote Host Port' (5050), 'Multicast TTL (0..200)' (0), 'Advanced DSG Delivery. Disabled. Using Standard MPEG2 Transport Stream Delivery. Check to enable Advanced DSG Delivery.' (unchecked), 'In-Band. Disabled. Using Out-Of-Band PID=1FFC. Check to enable In-Band PID=1FFB.' (unchecked), 'Details Video OOB ID' (0), 'Details Audio OOB ID' (0), 'Details InBand Major Channel' (0), and 'Details InBand Minor Channel' (0). 5. Bottom Section: A checked checkbox 'Send internal EAT control event at EAN,NPT End of Message. Enabled. NOTE! This may be REQUIRED for ending force tune during EAN and NPT National alerts by some downstream STBs and other SCTE18 receiving devices!'. Below it are two disabled checkboxes: 'Exception Channel List. Disabled. Check to enable Exception Channels.' and 'In-Band Details Channel Descriptor (Tag=0x00). Disabled. Check to enable In-Band Details Channel Descriptor.'

DVS644/SCTE18 Sub-Tab

Configure DVS644 (SCTE-18) CEAM Client Connection

Up to 64 DVS644/SCTE18 client interfaces may be defined. Each one can have a unique configuration and can send the SCTE-18 EAS protocol data to different IP addresses. During alert play-out processing, the Operation Log will log the success or failure of the DVS644/SCTE18 forwarding/origination action per client. Individual client interfaces may also be enabled and disabled. Every enabled client configuration is triggered for whichever action of alert forwarding and alert origination is currently enabled.

Select DVS644 client

This pull-down menu contains the names of the existing client interfaces. It also prints the current number of defined client interfaces. The maximum number of client interfaces is 64. Choose the named existing client interface to edit.

Add / Duplicate / Delete DVS644 (SCTE18) Client Interface Buttons

Users can create configurations for up to 64 DVS644 (SCTE-18) CEAM (Cable Emergency Alert Message) clients.

If no client configurations exist or a new configuration is needed, click the **Add DVS644(SCTE18) Client Interface** button to create a new interface configuration.

To delete a client configuration, select the desired client from the Select DVS644 client pull-down menu and click **Delete this DVS644(SCTE18) interface button**.

To duplicate an existing client interface, select the **Duplicate DVS644(SCTE18 Client Interface** button. A different name will be automatically generated. This is the ideal way to create many client interfaces that are mostly the same except for the IP address.

Client Interface Configuration Table

Client Interface Name

Use the **Client Interface Name** text entry field to name each client.

ENABLE Client Interface

Use this check box to enable/disable a client interface at any time. Each client can be independently enabled and disabled allowing an easy way to stop/ restart using a client for a specific region.



Caution

DVS644/SCTE18 client configuration addition, duplication, and deletion are immediate and cannot be canceled.

Configure DVS644(SCTE-18) CEAM Client Connection (client IP & program values apply to both Origination and Forwarding)

*Client 0 ▾ Select DVS644 client
There is 1 defined client interface (max is 64).

Add DVS644(SCTE18) Client Interface (effective immediately)
Duplicate DVS644(SCTE18) Client Interface (effective immediately)
Delete this DVS644(SCTE18) interface (effective immediately)

Client 0 **Client Interface Name**

ENABLE Client Interface. **Enabled.** Uncheck to disable client.

Remote Host Unicast or Multicast IP: 0
Address: 5050 Remote Host Port: 0
Multicast TTL (0..200): 0

Details Video OOB ID: 0
Details Audio OOB ID: 0
Details InBand Major Channel: 0
Details InBand Minor Channel: 0

Advanced DSG Delivery. **Disabled.**
Using Standard MPEG2 Transport Stream Delivery.
Check to enable Advanced DSG Delivery.
 In-Band. **Disabled.** Using Out-Of-Band PID=1FFC.
Check to enable In-Band PID=1FFB.

MPEG2 TS Continuity Counter Options
 Reset Continuity Counter with every message
 Reset Continuity Counter with every event
 Do not reset Continuity Counter

Send internal EAT control event at EAN,NPT End of Message. **Enabled.** NOTE! This may be REQUIRED for ending force tune during EAN and NPT National alerts by some downstream STBs and other SCTE18 receiving devices!

Exception Channel List. **Disabled.** Check to enable Exception Channels.

In-Band Details Channel Descriptor (Tag=0x00). **Disabled.** Check to enable In-Band Details Channel Descriptor.

In-Band Exception Channels Descriptor (Tag=0x01). **Disabled.** Check to enable In-Band Exception Channels Descriptor.

Audio File Descriptor (Tag=0x02). **Disabled.** Check to enable Audio File Descriptor.

MPEG Audio Sync Private Descriptor (Tag=0xE1). **Disabled.** Check to enable MPEG Audio Sync Private Descriptor.

NDS Tune Private Descriptor (Tag=0xE8). **Disabled.** Check to enable NDS Tune Private Descriptor.

Generic Private Descriptor. **Disabled.** Check to enable Generic Private Descriptor.

Set Alert type priority selection
(NOTE: EAN are always 15)
Low:3 ▾ Advisories
Low:3 ▾ Tests
Low:3 ▾ Watches
Medium:7 ▾ Warnings
High:11 ▾ Emergencies
Highest:15 ▾ National Test

NPT initial duration 120 secs. **Disabled.**
Will be 0 like EAN.

Immediate Start. **Disabled.** Alert Start Time on Receiving Device based on Encoder Clock Time.
Check to set immediate start time.
 Multiple Language Alert Text. **Disabled.**
Send Alert Text at all priority levels ▾ Alert Text Control
Never repeat alert send ▾ Alert Repeat Control
2 Alert Message Transmission Duplication Count (1-20)
0 Additional Start Delay Time (seconds).
Start Delay == (Audio Delay if enabled) + Additional Time
DVS644/SCTE 18 message send delay time = 6 seconds.
0 Duration Extension Time (seconds).
Alert Duration == Audio Duration + Extension Time
(max total is 120 seconds)

All FIPS codes trigger. **Enabled.** All FIPS locations will trigger DVS644/SCTE-18/CEAM device. Uncheck to choose specific triggering FIPS.

All EAS codes trigger. **Enabled.** Alerts with any EAS code will trigger DVS644/SCTE18 send. Uncheck to choose specific triggering EAS Codes.

DVS-644/SCTE18 Client Configuration Interface Section

Various information fields must be configured to identify and correctly communicate to the DVS-644/SCTE18 client. The basic fields are the **Remote Host Unicast or Multicast** and **Remote Host Port**. Enter these addresses according to the specific DVS-644/SCTE-18 target server. Often this is an MPEG-2 multiplexor, such as a Stream Encryptor Modulator, serving a defined set of digital cable channels.

Multicast TTL

This value determines the number of router hops that are allowed during multicast of the DVS644/SCTE18 Cable Alert Message before the UDP message is blocked. Enter a sufficiently large value (from 0 to 200) if you are multicasting. Multicasting requires the proper configuration of a network outside the EAS device.

Advanced DSG Delivery

Defaults to Disabled. The default method for delivering the DVS644/SCTE18 Cable Alert Message MPEG2 system table uses a standard MPEG2 Transport Stream. Check to switch to Advanced DSG delivery. Use DSG delivery for communicating with DOCSIS Standard Gateway equipment.

If **Advanced DSG delivery** is used then the text field option for setting the **Network MTU** (Max transmission unit) is available. The default is 1500 but can be set lower if needed based on a specific network.

If **standard MPEG2 transport stream delivery** is used, then the following option is available:

In-Band

Check to Enable. If not checked (disabled) then **Out-of-Band (OOB)** communication of the DVS-644/SCTE18 message is made.

The DVS-644/SCTE18 Cable Alert Message is an MPEG2 system table structure, typically placed into the MPEG2 Transport stream and routed to the downstream cable set top boxes (STB) or SCTE-18 enabled TV's. The ultimate target for the DVS-644/SCTE18 alert message is a set-top box (STB) or a cable ready TV. The actual EAS alert handling is performed by the STB or TV, and although standard practices exist for these actions, differences do exist. The processing of the Cable Alert Message on the STB determines the actual response to the alert seen by a viewer. For alerts below a certain priority (by default, this would be the highest priority, 15), a crawl message is typically run on the video display for every channel. For alerts at or above this priority, the video channel is forced to a details channel. Based upon whether this channel is available at the STB as In-Band or Out-of-Band, set the **Details Major/Minor number** or the **Details Video/Audio OOB** channel numbers. This details channel is where the highest priority force tune alerts are switched. EAN/NPT will always cause a force tune to this channel.

Details Video OOB ID/ Details Audio OOB ID

When the alert details channel is an Out-of-Band channel, set the provided video/audio channel field. An audio channel designation is not required when there is another means to provide the alert audio. A value of 0 means not used.

Details In-Band Major / Minor Channel

These two fields are for programming the digital in-band Major/Minor channel number of the in-band force tune details channel. A value of 0 means not used.

MPEG2 TS Continuity

Each MPEG-2 Transport Stream packet contains an incriminating Continuity Counter (CC) number (ranging from 0-15). This value is used to determine if any packets are lost, repeated, or out of sequence. Manufacturers of downstream MPEG devices may deal with the CC value in dissimilar ways. For this reason there are three separate settings.

Reset Continuity Counter with every message (default setting)

When you send an MPEG-2 / SCTE-18 alert event, the CC will start with a value of zero (0) and increment appropriately. If the alert is repeated (via the **Alert Repeat Control**), the CC will be forced to a value of zero (0) at the beginning of each message.

Reset Continuity Counter with every event

Each MPEG-2 / SCTE-18 alert event will begin with the CC set to zero (0) and will increment appropriately. The CC will not be forced to zero (0) until a new alert event is generated.

Do no reset Continuity Counter

The CC will always increment appropriately and will not be forced to a value of zero (0).

Exception Channel List. Enabled. Uncheck to disable.

Add Exception Channel Entry

1. WROC.1	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	8	1	Remove
2. WROC.2	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	8	2	Remove
3. WHEC.1	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	10	1	Remove
4. WHEC.2	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	10	2	Remove
5. WHEC.3	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	10	3	Remove
6. WHAM.1	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	13	1	Remove
7. WHAM.2	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	13	2	Remove
8. WHAM.3	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	13	3	Remove
9. WXXI.1	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	21	1	Remove
10. WXXI.2	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	21	2	Remove
11. WXXI.3	<input checked="" type="checkbox"/> In-band. Enabled. Uncheck to enable Out-of-Band.	21	3	Remove

Exception Channel List Section

Send internal EAT control event at EAN,NPT End of Message

Enabling this check box will send an Emergency Action Termination (EAT) at the end of both an EAN or NPT to indicate the emergency action is over.

Exception Channel List

This interface allows specific In-Band and Out-of-Band channels to be excluded from the alert response of the STB. These channels have their own EAS. When enabled, the interface allows the creation of any number of exception channels.

In-Band Details Channel Descriptor (Tag=0x00). Enabled. Uncheck to disable.
Provides an optional pointer to the details channels in a descriptor for in-band use only.

Details RF Channel
 Details MPEG-2 PAT Program Number

In-Band Details Channel Descriptor Section

In-Band Details Channel Descriptor (Tag=0x00)

Provides an optional pointer to the details channels in a descriptor for in-band use only.

MPEG Audio Sync Private Descriptor (Tag=0xE1). Enabled. Uncheck to disable.
Provides MPEG audio start/stop signals in a private descriptor.
NOTE: **Alert Repeat Control** must be set to repeat the alert transmission for audio sync to function.

Audio/Video Stream Multicast IP Address (set to empty for unicast stream)
 Audio/Video Stream Port
 Audio Stream PID (In Hex, default is 45)
 Audio/Video Stream Source IGMPv3 IP Address (optional)
 Input Port options. Disabled. Check to enable Input Port Options.

MPEG Audio Sync Private Descriptor Section

MPEG Audio Sync Private Descriptor

Check to enable the MPEG Audio Sync Private Descriptor - a special private descriptor for synching a EAS device MPEG2 A/V stream to the DVS644/SCTE18 message processor. Use of this method requires custom support by the DVS644/SCTE18 message processor.

NDS Tune Private Descriptor

Check to enable the NDS Tune Private Descriptor method - a special private descriptor for synching a EAS device to an NDS system. Use of this method requires custom support by the DVS644/SCTE18 message processor.

Generic Private Descriptor

Check to enable an interface to create one static DVS644/SCTE18 Private Descriptor. Use of this method requires custom support by the DVS644/SCTE18 message processor.

Set Alert Type Priority / FIPS & EAS Code Triggers Section

Alert Type Priority Selection

Use this interface to configure the associated priority number for EAS alert codes. The scheme is based upon five EAS groups: Advisories, Tests, Watches, Warnings, and Emergencies. The exact alerts that fall into each category are defined on the EAS device at **System > Help > EAS Codes**.

DVS644/SCTE18 provides for 16 priority values (0-15). However, reserved uses for most values means that in practice, priority values are 0, 3, 7, 11 and 15, with 15 being the highest priority alerts. The priority of 0 has a special meaning. An alert sent with 0 priority will establish a new set-top box or TV sequence number. The sequence number is incriminated (modulo 32) whenever an alert is sent with updated information. The EAS device supports this reset mode by allowing an alert to be set to 0 priority. This setting should only be used for one alert and then changed to 1-15. There is also a field to extend the alert duration past the default EAS device audio duration. Keep in mind that the maximum allowed time for a DVS644/SCTE18 message is 120 seconds.

NPT initial duration 120 secs

When unchecked, the NPT initial duration is 0 – which means this live alert is open-ended. Once the EOM is reached a second message with a 5 second duration is sent which ends the NPT alert. By selecting this check box, a fixed duration of 2 minutes is forwarded within the NPT.

Immediate Start (Alert Start Time)

This check box sets the EAS Alert message start time on the receiving device. When enabled, the start time of the alert on the receiving device is immediate upon reception. When disabled (unchecked), the Alert Start Time is set to use a clock-based start time. The actual time used is the EAS alert UTC.



Caution

If a clock time is used, it is CRITICAL that the EAS device and the receiving device be time synchronized.

Multiple Language Alert Text

Allows SCTE-18 to send multiple language translations to the SCTE-18 connected device.

Alert Text Control

This pull-down menu programs when the alert text section of the DVS-644/SCTE18 message is sent, based on alert priority. It allows text to not be sent if the priority becomes higher than a specified value and allows the STB to omit alert text crawls when a force tune to a details channel is made based upon alert priority.

Alert Repeat Control and Alert Message Repeat Period

The EAS device can be configured to periodically resend the alert message, with the DVS644/SCTE18 Cable Alert message field **alert time remaining** field decremented automatically. This is controlled using the **Alert Repeat Control** selections. The options are based on alert priority, allowing repetition to be invoked for alerts above a given priority. When repetition is selected, the **Alert Message Repeat Period** field for entering the time period (in seconds from 6 to 60) is also displayed.

Alert Message Transmission Duplication Count (1-20)

When a forwarded/originated alert is sent to a DVS-644 client at a specific IP address, the DVS-644/SCTE-18 MPEG-2 system table is generated and sent to the MPEG multiplexor client. Programming this interface controls the number of times the table is sent as a duplicate, from 1 - 20 times, to insure downstream reception.

Additional Start Delay Time (seconds)

This check box allows time to be added before the DVS644/SCTE18 Cable Alert Message is first sent over the network. The formula for the delay time is: Start Delay == (Audio Delay if enabled) + Additional Time.

Duration Extension Time (seconds)

This field allows extra time to be added to the alert duration programmed into the Cable Alert Message **alert time remaining** field. The maximum time allowed for this field is 120 seconds. This can be used to guarantee a minimum amount of time for short Weekly Test alerts. The formula for the Alert Duration is: *Alert Duration == Audio Duration + Extension Time (max total is 120 seconds)*.

All FIPS codes trigger

If enabled, all alert FIPS codes will trigger the DVS644/SCTE18 client interface. In the above screen shot this option is disabled. Set the check box to enable/disable FIPS code filtered trigger control. If disabled, the alert FIPS codes are filtered for at least one specific match as a way to control whether or not DVS644/SCTE18 is triggered. Alerts for specific FIPS areas can be filtered as a way to control whether or not DVS644/SCTE18 is triggered. If All FIPS is disabled, select FIPS Groups from the pull-down menu. If any of these FIPS codes are included in the incoming active forwarded/originated alert, the alert will be sent using the DVS-644/SCTE18 client. With careful use of this feature, and with multiple clients, one EAS device can serve many different cable regions at the same time.

All EAS codes trigger

If enabled, all EAS codes will trigger the DVS644/SCTE18 client interface. In the above screen shot this option is disabled. Set the check box to enable/disable EAS code filtered trigger control. If disabled, then the alert EAS code is filtered for a specific match as a way to control whether or not DVS644/SCTE18 is triggered. If All EAS is disabled, select EAS Group from the pull-down menu. If the EAS codes of an active forwarded/originated alert matches any included in the EAS Group, the alert will be sent using the DVS-644/SCTE18 client. With careful use of this feature, and

with multiple clients, one EAS device can serve many different cable regions at the same time.

When you finish making changes, click **Accept Changes** to save the configuration.

Stream MPEG

If Streaming MPEG hardware/software is available on the EAS device, a sub-tab will display under **Setup > Net Alerts** that allows configuration of up to two client targets. As in the other Net Alert pages, use the Alert Forwarding and/or the Encoder Alert stream check boxes to enable/disable the use of streaming MPEG clients when alerts are forwarded and/or originated.

The screenshot shows the 'Stream MPEG' sub-tab in a web interface. At the top, there are navigation tabs: EAS.NET, CAP_Decode, DVS644 (SCITE18), **Stream MPEG**, Net.CG, Net_Switch, and Net_GPIQ. Below the tabs, a yellow banner reads: 'Configure MPEG Streaming Clients. Except for Add/Delete Clients, changed Settings are not effective until Accept Changes is pushed.' There are two checked checkboxes: 'Forwarded Alerts stream MPEG. Enabled. Uncheck to disable.' and 'Encoder Originated Alerts stream MPEG. Enabled. Uncheck to disable.' The main section is titled 'Configure MPEG Streaming Client Connection' with a note: '(Video output must be Enabled! Client network connection values apply to both Origination and Forwarding)'. A link says 'No audio playout delay period (min 6 secs recommended). Follow link to edit.' Below this are two columns of settings: 'MPEG2 D1-704' with 'MPEG 1/2 Video Format' and '3000000' 'Video Bitrate (100000-10000000)'; and 'MPEG1: Layer2' with 'MPEG Audio Format', '96Kbits/sec' 'MPEG Audio Bitrate', and '32K samples/sec' 'MPEG Audio Sample rate'. There are two buttons: 'Add Streaming MPEG Client Interface (effective immediately)' and 'Delete this Streaming MPEG interface (effective immediately)'. A dropdown menu shows '*Client 0' and 'Select Streaming MPEG client' with a note 'There is 1 defined client interface (max is 2)'. Below this is a detailed configuration for 'Client 0' with a 'Client Interface Name' field. It includes a checked 'ENABLE Client Interface. Enabled. Uncheck to disable client.' checkbox, and fields for 'Remote Host Unicast or Multicast IP Address' (226.2.2.2), 'Remote Host Port' (8102), and 'Multicast TTL (1..200)' (7). There are radio buttons for 'Media Stream Control': 'Audio+Video' (selected), 'Audio Only', 'Video Only', and 'Disable Audio & Video'. Below these are fields for 'MPEG2-TS Program Association Table(PAT)/Program Map Table(PMT) Program Number' (1), 'MPEG2-TS PMT PID (in Hex, default is 42)' (42), 'Audio Stream PID (in Hex, default is 45)' (45), and 'Video Stream PID (in Hex, default is 44)' (44). There are two checkboxes: 'All FIPS codes trigger. Disabled. Specific FIPS Codes control MPEG streaming (EAN,NPT with FIPS 000000 override). Check to enable all FIPS codes triggering of MPEG streaming.' and 'All EAS codes trigger. Disabled. Specific EAS Codes control MPEG streaming. Check to enable all EAS codes triggering of MPEG streaming.' Below these are dropdown menus for 'FIPS Group' (All Locations) and 'EAS Group' (All). At the bottom are 'Accept Changes' and 'Cancel Changes' buttons.

Stream MPEG Sub-Tab

Addition/deletion, configuration, and enable/disable for each client interface is handled like other Net Alert interfaces described above. Unlike those interfaces, there are a few global settings that affect all streaming clients. These control the video/audio format and encoding bitrate of the stream (from the hardware). The user can also program Audio/Video, Audio only, or Video only being encoded. To account for the latency of starting up stream encoding and actually streaming, a delay of a few seconds is needed before audio is played for a net forwarded/originated alert. Audio delay status and a link to the configuration field for audio delay is provided.

Streaming MPEG requires very few configuration fields. A unicast or multicast IP address must be set, along with a port. The Multicast TTL value must be set high

enough to insure the multicast data is sent past all the LAN routers between the EAS device and the destinations. Also, as with the EAS NET and DVS-644 interfaces, FIPS and EAS code-based triggering is supported per client.

Net CG

This page allows configuration of up to five client targets for running alert crawls. The Net CG units must support Ethernet and be connected to the same LAN as the EAS device. As in the other Net Alert pages, use the Alert Forwarding and/or the Encoder Originated Alert check boxes to enable/disable the use of Net CG clients when alerts are forwarded and/or originated.

Net CG Sub-Tab

Addition/duplication/deletion, configuration, and enable/disable for each client interface is handled just like other Net Alert interfaces described in previous chapters.

The first option: **Client Interface Name** allows the user to name the CG to reduce confusion between multiple devices.

ENABLE Client Interface

Check this box in order to enable the specific client you have created or selected to edit.

Select a Protocol Option

Select the CG that pertains to your situation. The list of compatible Network CGs are, COMPIX NewsScroll, COMPIX Autocast, Simple Chyron Intelligent IF, Raw Chyron IntellIF & ChyTV, Simple ChyTV IF, CODI Net CG, Cayman Graphics, Fox Splicer/DCM, Inovonics RDS730.

Remote CG Net Host IP and Port

In this field, type the IP address and the port of the CG that is on the same network connection that your DASDEC is on.

All FIPS codes trigger

Check to enable all alerts, regardless of FIPS codes, to trigger a crawl on the target Net CG clients. Uncheck to only allow alerts for specific FIPS areas to trigger the crawl. When unchecked, you can select from the FIPS Group pull-down menu. Alerts to any FIPS code within the group will be sent to the remote Net CG clients.

All EAS codes trigger

If enabled, all EAS codes will trigger the Net CG client interface. Set the check box to enable/disable EAS code filtered trigger control. If disabled, the alert EAS code is filtered for a specific match as a way to control whether or not the target Net CG client is triggered. If All EAS is disabled, select an EAS Group from the pull-down menu. If the EAS code of an active forwarded/originated alert matches any of the EAS codes within that group, the alert will be sent using the Net CG client. With careful use of this feature, and with multiple clients, one EAS device can serve many different regions at the same time.

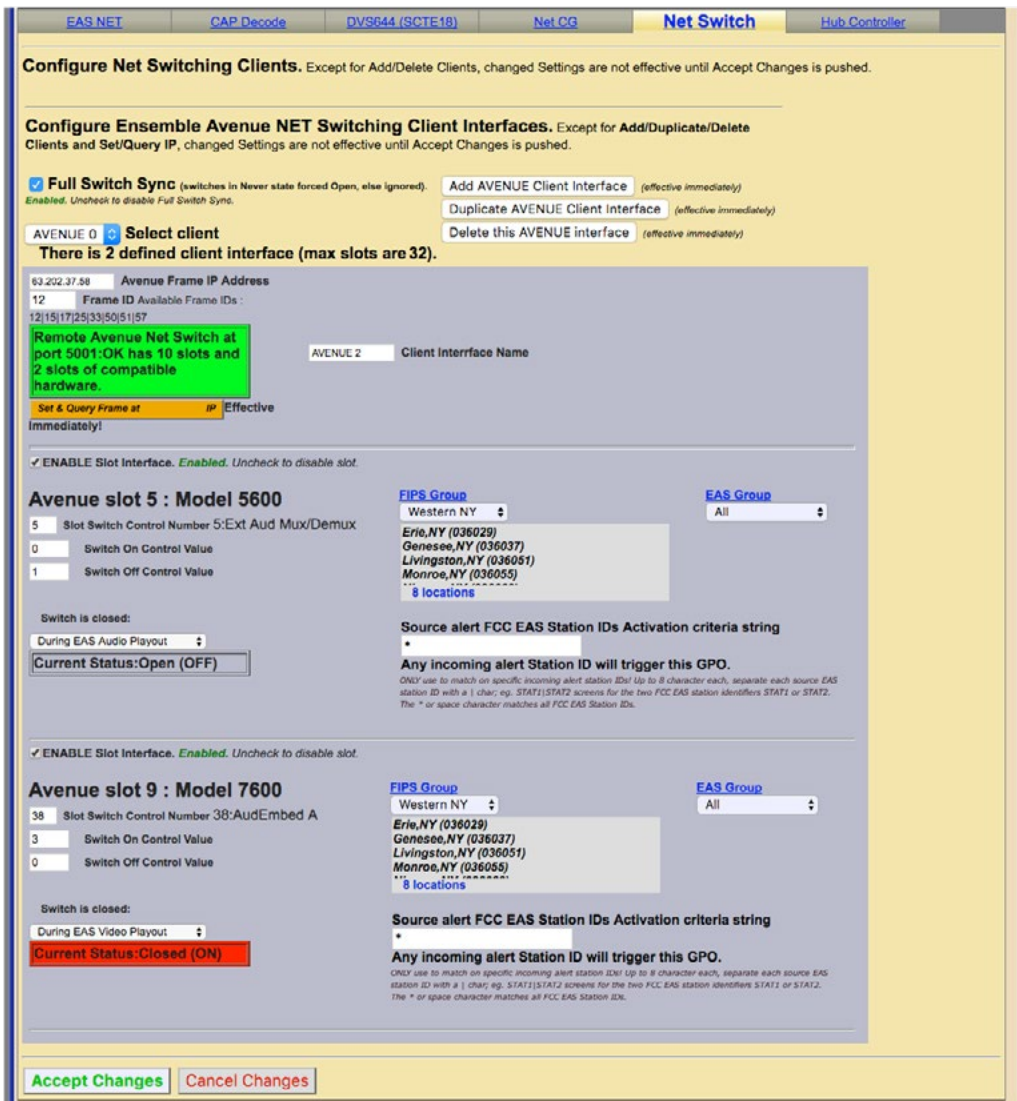
All incoming alert Station IDs trigger

This is additional filter criteria for activation of this Net CG client. Enter the desired Station ID or Station ID's (separated by a '|') into this text field – up to 8 characters for each ID. This Net CG client will not activate without matching this station ID(s). The default value is the wildcard character (*). All station ID's will activate this Net CG client when using that character.

When you finish making changes, click the **Accept Changes** button to save the configuration.

Net Switch

The **Net Switch** sub-tab enables control of an Ensemble Designs Avenue™ 7600 HD/SD Embedder/Disembedder for EAS alert audio switching. Utilizing the onboard audio channel swap and shuffle capabilities of the Avenue 7600 module, users can switch between EAS alert audio (assigned to AES 7/8) and 5.1 program audio (AES 1/2, 3/4, 5/6). The Net Switch sub-tab is displayed with a valid Plus Package license key.



Net Switch Sub-Tab

Configure Net Switching Clients

Click the **Add AVENUE Client Interface** button to add a new Net Switching Client. This action will create a new client interface named AVENUE 0. This descriptive name can be changed by typing new text in the **Client Interface Name** text field.

Avenue Frame IP Address

Enter the IP address of the Avenue frame.

Frame ID

Enter the Frame ID from the list of Available Frame IDs below this text box.

ENABLE Slot Interface

Check this box to enable the interface for the card/module located within the defined Avenue frame slot.

Slot Switch Control Number

Enter the slot number of the desired card/module.

Switch On Control Value

Enter the switch on control value.

Switch Off Control Value

Enter the switch off control value.

Switch is closed:

This pull-down menu provides a choice of actions within the EAS device that will trigger the Avenue module.

The actions can be tied to alert FIPS Groups, EAS Groups, and specific EAS Station IDs. To add FIPS code filtering, click the desired selection from the **FIPS Group** pull-down menu. Active alerts containing any of the FIPS codes contained in the selected FIPS Group will trigger that relay (close the contact) while the associated condition is true. Repeat the same process selecting an EAS code group from the **EAS Group** pull-down menu. When selecting "All" from either the FIPS Group or EAS Group pull-down menus, no filtering will take place.

The default value in the **Source alert FCC EAS Station IDs Activation criteria string** is an asterisk (*). This is a wildcard that will not filter for specific Station IDs. Only enter text in this field to match on specific incoming alert Station IDs. Up to 8 character each, separate each source EAS station ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2).

Hub Controller / Net GPIO

This sub-tab under **Setup > Net Alerts** is a standard feature on a EAS device to allow remote, LAN connected GPIO relays and inputs to be associated to active alerts. **Hub Controller** is used in a One-Net and **Net GPIO** is used in a DASDEC. Both have the exact same controls and are grouped together in this manual for that reason. The EAS device supports the following equipment:

- Monroe Electronics – R190A Hub Controller (four relays)
- Monroe Electronics – R197 Audio Switch
- Monroe Electronics – R198 AES Audio Switch
- Titus - W300
- Control by Web – WebRelay-Quad (four relays)
- Control by Web – WebRelay-Dual (two relays)
- Dataprobe – iPIO-8 (eight relays)

This interface page provides for the creating, duplicating, deleting and configuring client connections for up to eight LAN positioned relays. This type of hardware provides an inexpensive and convenient way to expand the contact closures relays of the EAS device. Since these relays can be placed on a LAN, and controlled by the EAS device remotely, they can be used to trigger actions during alerts without extra wiring. Configuration is much like other Net Alert pages. Up to 8 clients can be configured and active at a time.

When you finish making changes on this page, click the **Accept Changes** button to save the configuration.

Configure Net GPIO Connection

Below is a description of the client interface controls.

Select client

Use the pull-down menu to select the client interface to examine or configure.



Attention

An Ensembles Designs Avenue 5035 (1RU Frame) or 5030 (3RU Frame) System Control module is required for switching audio from an EAS device.



Note

This interface supports both the Avenue 5600 Embedder/Disembedder and 7600 HD/SD Embedder/Disembedder. As of the writing of this manual, the Avenue 5600 has been discontinued and is no longer available.



Attention

Because a Net GPIO unit must be continually queried via HTTP for an input contact closure, this option is slow compared to GPIO input hardware that is directly a part of the EAS device. Thus this option requires the contact closure to last for at least one second in order to be detected.

Listen for Net GPIO Input

When enabled this check box causes the EAS device to listen for input contact closures from the Net GPIO units. This option only works if at least one of the connected Online Net GPIO units supports inputs. As of EAS device version 8.0, only the Web Relay Dual unit supports inputs. **Only enable this option when an input from a Net GPIO unit is required.**

Add / Duplicate / Delete NetGPIO Client Interface

You can create configurations for up to 8 Net GPIO clients.

- If no client configurations exist, or if you want a new one, click the **Add NETGPIO Interface** button to create a new interface configuration.
- To delete a client configuration, select the client and click on **Delete this GPIO interface**.
- To duplicate an existing client interface (a different name will be automatically generated), select the **Duplicate NETGPIO Client Interface** button. This is the best way to create many client interfaces that are mostly the same except for the IP address.

Close EAS Audio Relay, Open EAS Audio Relay

Manual overrides intended for test purposes. Pressing either button will either close or open any audio relays programmed for audio playout. This will control both the internal relays and the Net Controller / Net GPIO relays programmed for audio playout.



Caution

Net GPIO client configuration addition, duplication, and deletion is immediate and cannot be canceled.

The screenshot shows the 'Hub Controller' sub-tab configuration page. At the top, there are navigation tabs: EAS.NET, CAP_Decode, DVS644 (SCTE18), Net.CG, Net.Switch, and Hub.Controller. The main heading is 'Configure Hub Controller Clients. Except for Add/Duplicate/Delete Clients and Change Model Type, changed Settings are not effective until Accept Changes is pushed.' Below this, there is a 'Select client' dropdown set to 'R190 0' and a note '1 defined client interface and 4 allocated ports (max of 32 ports)'. There are three buttons: 'Add Hub Controller Client Interface (effective immediately)', 'Duplicate Hub Controller Client Interface (effective immediately)', and 'Delete this Hub Controller interface (effective immediately)'. Below these are 'Close EAS Audio Relay' and 'Open EAS Audio Relay' buttons. A checked checkbox 'ENABLE Client Interface. Enabled. Uncheck to disable client.' is present. The 'IP Address' field is empty with a warning 'IP address syntax is not valid!'. The '#Utilized Ports (max=4; unutilized=0)' is set to 4. The 'Name' field is 'R190 0' and the 'Model' is 'R190'. The 'Relay 1' section shows 'Relay is closed: During EAS Audio Playout', 'FIPS Group: Western NY', and 'EAS Group: All'. A list of locations is shown: 'Erie, NY (036029)', 'Genesee, NY (036037)', 'Livingston, NY (036051)', and 'Monroe, NY (036055)'. Below this is a 'Source alert FCC EAS Station IDs Activation criteria string' field with an asterisk. A note states 'Any incoming alert Station ID will trigger this GPO. ONLY use to match on specific incoming alert station IDs! Up to 8 character each, separate each source EAS station ID with a | char; eg. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2. The * or space character matches all FCC EAS Station IDs.' Below are sections for 'Relay 2', 'Relay 3', and 'Relay 4', each with a 'Relay is closed:' dropdown set to 'Never'. At the bottom are 'Accept Changes' and 'Cancel Changes' buttons.

Hub Controller / Net GPIO Sub-Tab

ENABLE Client Interface

Enables/disables the use of the Net GPIO client interface.

IP Address

Enter the IP address of a remote NET GPIO target unit. No port number is needed, as these units all use HTTP port 80. Once the address is entered, the status of the connection is shown in a display directly below the IP address field. If the unit can be contacted, a green status box shows the successful connection. If not, a red status box shows that the connection cannot be made.

Name

Allows the client interface to be given a descriptive name.

Model

Select from one of the three supported models from the pull down menu. Make sure the model fits the intended target.

Password

If the Net GPIO unit supports a password and is configured to require a password, enter it here.

NET GPIO Output Relay

Each client provides up to 4 relays. A variety of EAS device alert states can be used to trigger a relay. The following is a list of various triggering actions:

- Never
- During EAS Audio Payout
- Momentarily at start of EAS Audio Payout
- Momentarily at end of EAS Audio Payout
- Momentarily at start and end of EAS Audio Payout
- During EAN Audio Payout (During Live EAN/NPT Audio Payout)
- During EAS Video Payout
- During Main Serial EAS Payout
- Momentarily at start of decoded EAS
- Momentarily at start of unforwarded, decoded EAS
- Pending manual forward of decoded EAS
- Pending acknowledgement of unforwarded, active decoded EAS
- During EAS alert cued (confirm general origination)
- During hold of EAS until GPI closure
- During hold of EAS during GPI closure
- During Internal Balanced Audio Payout
- During Audible parts of segmented live EAS Audio
- During audio preview
- During Global Auto-Forward mode enabled
- During Station Auto-Forward mode enabled

NET GPIO Input Action

The Web Relay Dual client provides 2 inputs. A variety of actions can be triggered on the EAS device when a contact closure is made on these inputs. The following list shows the various actions. These selectors are only available when **Listen for Net GPIO Input** is enabled and only for Hub Controller / Net GPIO units that support input.

- None
- Issue Weekly Test (RWT) upon closure
- Start segmented live EAS on closure; more closures skip to EOM
- Acknowledge unforwarded active alert and play decoded audio
- Acknowledge unforwarded active alert and/or play decoded audio
- Forward active decoded EAS upon closure
- Forward active RMT with original decoded audio
- Preview RMT substitute alert audio
- Preview active decoded alert audio
- Re-enable forwarded EAS alert
- Originate cued alert
- Hold or Release Non-National EAS alerts
- Allow or Block net/serial interface operation
- Light Front Panel Alert LED while closed
- Toggle Global Auto Forward mode upon closure
- Toggle Station Auto-Forward mode closure

The actions can be tied to alert FIPS Groups, EAS Groups, and specific EAS Station IDs. To add FIPS code filtering, click the desired selection from the **FIPS Group** pull-down menu. Active alerts containing any of the FIPS codes contained in the selected FIPS Group will trigger that relay (close the contact) while the associated condition is true. Repeat the same process selecting an EAS code group from the **EAS Group** pull-down menu. When selecting "All" from either the FIPS Group or EAS Group pull-down menus no filtering will take place.

The default value in the **Source alert FCC EAS Station IDs Activation criteria string** is an asterisk (*). This is a wildcard that will not filter for specific Station IDs. Only enter text in this field to match a specific incoming alert Station IDs. Up to 8 characters each, separate each source EAS station ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2).

When you finish making changes, click the **Accept Changes** button to save the configuration.



Note

The option "During Audible parts of segmented live EAS Audio" requires a valid Plus Package license key.

GPIO SETUP

The Setup GPIO page allows the user to program and display the state of the General Purpose Inputs and Outputs (GPIO) settings. GPIO wiring is provided by connectors on the back panel of the EAS device or through networked attached units.. The state of the Front Panel button and the Internal Balanced Audio output is included in the GPIO table display.

Auto-Refresh Timer

With a valid Plus Package license key the web interface displays an **Auto-Refresh Timer** pull-down menu in the left corner of the screen header. This allows the page to refresh every 15, 30, or 60 seconds. This feature can be used to automatically view updates to the GPIO status.

The GPIO web interface contains the following sections:

- **Server GPIO Table**
- **Programmable GPIO**
- **Expansion GPIO Input / Output Tables** (when configured with an Expansion GPIO option)
- **Network GPIO Table** (if a network-attached GPIO unit is configured)

The screenshot shows the 'GPIO Setup' screen. At the top, there's a header with the name 'DASDEC-1F EAS' and a logo for Digital Alert Systems. Below that is a navigation bar with 'Send Alerts', 'Alert Events', 'System', and 'Setup' tabs. The 'Setup' tab is selected, showing radio button options for 'Server', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'E-Mail', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. The 'GPIO' option is selected. Below this is an 'Auto-Refresh Off' dropdown and a 'Logout' button. The main content area is titled 'DASDEC Server GPIO Table' and contains a table with columns for input/output names and current status. Below the table are two buttons: 'Close EAS Audio Relay' and 'Open EAS Audio Relay'. The bottom section is titled 'Programmable GPIO Input Actions' and 'Programmable GPIO Output Relay', with various configuration options for FIPS and EAS groups and locations.

GPIO Setup Screen

Server GPIO Table

The top section of this page displays the current status of the built-in GPIO hardware. The top row displays the status of the inputs. The first input is the state of the Front Panel button. This is not available as a GPIO input but uses the internal GPIO circuitry. The next two columns show the programmed actions and current closure state for GPIO inputs 1 and 2. The second row displays the status of the relay outputs and of the internal audio/pass-through relay. The first two columns show the programmed triggers and current closure state for GPIO outputs 1 and 2.

Two buttons are placed under the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio. The companion button, **Open EAS Audio Relay**, sends the command to open all relays programmed to EAS audio payout.



Note

Changes made to the GPIO actions/relay associations are immediate and the screen updates instantly.



Caution

The **Close/Open EAS Audio Relay** buttons apply to ALL relays assigned to EAS audio payout – both internal and external (Net Controller / Net GPIO) relays. Make sure the use of these buttons does not negatively impact regular EAS operations.

Programmable GPIO Input / Output Actions

Programmable options are GPIO Input 1, GPIO Input 2, GPIO Output 1 Relay, and GPIO Output 2 Relay. The available pull-down menu selections will vary depending on the enabled license keys. Pay close attention to the following descriptions to view the appropriate pull-down menu options.

GPIO Input 1

A pull-down menu allows GPIO Input 1 to be programmed to do one of the following:

- None
- Issue Weekly Test (RWT) upon closure
- Start segmented live EAS on closure; more closures skip to EOM (△)
- Acknowledge unforwarded active alert and play decoded audio
- Acknowledge unforwarded active alert and/or play decoded audio (△)
- Forward active RMT with original decoded audio (△)
- Preview RMT substitute alert audio (△)
- Preview active decoded alert audio (△)
- Forward active decoded EAS upon closure
- Re-enable forwarded EAS alert
- Forward active decoded EAS once to all upon closure (§)
- Re-enable EAS alert forwarded once to all (§)
- Originate cued alert (△)
- Hold or Release Non-National EAS alerts
- Allow or Block net/serial interface operation
- Light Front Panel Alert LED while closed
- Toggle Global Auto Forward mode upon closure
- Run Custom Message (▼)

A valid Plus Package license key is required to view/select any of the above items with a (△) symbol. MultiStation is required to view/select the above items with a (§) symbol. Custom Message Pro is required to view/select the above item with a (▼) symbol.

GPI Input 2

A pull-down menu allows GPIO Input 2 to be programmed to do one of the options below. The same pull-down menu options from GPI Input 1 are available for GPI Input 2.

GPIO Output 1 Relay

This selection box allows for programming the GPI Output 1 closure. Set according to the condition that needs to be monitored. The following is a list of the available pull-down menu selections:

- Never
- During EAS Audio Playout
- Momentarily at start of EAS Audio Playout
- Momentarily at end of EAS Audio Playout
- Momentarily at start and end of EAS Audio Playout
- During EAN Audio Playout (During Live EAN/NPT Audio Playout) (X)
- During EAS Video Playout
- During Main Serial EAS Playout

- Momentarily at start of decoded EAS
- Momentarily at start of unforwarded, decoded EAS (X)
- Pending manual forward of decoded EAS (X)
- Pending acknowledgement of unforwarded, active decoded EAS (X)
- During EAS alert cued (confirm general origination)
- During hold of EAS until GPI closure
- During hold of EAS during GPI closure
- During Audible parts of segmented live EAS Audio
- During audio preview (X)
- During Global Auto-Forward mode enabled (X)
- During Station Auto-Forward mode enabled (X)

GPIO Output 1 Activation Filter Configuration

Choose the FIPS Group and/or EAS Group that will control which alerts trigger the applicable programmed GPIO output 1 relay. Items in the above GPI Output Relay pull-down menu list that contain an (X) do not offer FIPS Group and/or EAS Group filtering.

GPI Output 2 Relay

This pull-down menu allows for programming the GPI Output 2 Relay. Operation of this relay is the same as GPI Output 1 Relay above.

GPIO Output 2 Activation Filter Configurations

Choose the FIPS Group and/or EAS Group that will control which alerts trigger the applicable programmed GPIO output 1 relay. Items in the above GPI Output Relay pull-down menu list that contain an (X) do not offer FIPS and/or EAS Group filtering.

GPIO Pending Alert Activation Filter Configuration

Choose FIPS Group and EAS Group to control which active pending alerts trigger the GPIO Output 1 or 2 Relay for states **Pending manual forward of decoded EAS** or **Momentarily at start of unforwarded, decoded EAS** or to control which alerts are forwarded when GPIO Input 1 or 2 is set to **Forward active decoded EAS upon closure**.

This interface is only present when the GPI Input 1 or 2 is programmed to **Forward active decoded EAS upon closure**, or when the GPIO Output 1 or 2 Relay is set to close **Pending manual forward of decoded EAS**. This interface allows the selection of FIPS Groups and EAS Groups filtering criteria to be applied to the programmed GPI input action or to be applied to an alert that would trigger either GPIO 1 Relay or GPIO 2 Relay closure. Use this interface to narrow down active alerts that will be forwarded upon GPI input contact closure or to narrow which active unforwarded alerts trigger a relay closure. To use the interface, select the desired group from the **FIPS Group** and/or **EAS Group** pull-down menu. All selections are immediately active once the desired group is selected.

The remainder of the GPIO screen provides status displays for:

- Expansion GPIO
- Multiplayer GPIO
- Hub Controller / Net GPIO

Display Expansion GPIO Status (uncheck to remove view)

DASDEC Server Expansion GPIO Input Tables			
Exp Input 1 : Unused Current Status:Open (OFF)	Exp Input 2 : Unused Current Status:Open (OFF)	Exp Input 3 : Unused Current Status:Open (OFF)	Exp Input 4 : Unused Current Status:Open (OFF)
Exp Input 5 : Unused Current Status:Open (OFF)	Exp Input 6 : Unused Current Status:Open (OFF)	Exp Input 7 : Unused Current Status:Open (OFF)	Exp Input 8 : Unused Current Status:Open (OFF)
DASDEC Server Expansion GPIO Output Tables			
Exp Output 1 : Unused Current Status:Open (OFF)	Exp Output 2 : Unused Current Status:Open (OFF)	Exp Output 3 : Unused Current Status:Open (OFF)	Exp Output 4 : Unused Current Status:Open (OFF)
Exp Output 5 : Unused Current Status:Open (OFF)	Exp Output 6 : Unused Current Status:Open (OFF)	Exp Output 7 : Unused Current Status:Open (OFF)	Exp Output 8 : Closed during EAS Audio Current Status:Open (OFF)

Expansion GPIO Status Table

Display Expansion GPIO Status

If the EAS device is configured with an internal expanded GPIO card, the **Display Expanded GPIO Status** check box will appear on this screen and there will be a sub-tab labeled **Expansion GPIO** within the **Setup > GPIO** menu. Click this check box to view the Expansion GPIO Table where the status of each GPIO input and output is shown. Configuration of the Expansion GPIO is performed within the **Setup > GPIO > Expansion GPIO** sub-tab.

Display Multiplayer GPIO Status

The **Display Multiplayer GPIO Status** check box will appear if the EAS device is configured with an external MultiPlayer (for MultiStation support). Click this check box to view the Multiplayer GPIO Table where the status of each GPIO input and output is shown. Programming of these GPIOs is performed within the Multiplayer sub-tab within **Setup > GPIO**. To setup a new Multiplayer, go to **Setup > Audio > Multiplayer**. Configuration of the MultiPlayer is performed on the **Setup > GPIO > Multiplayer GPIO** screen. (See below for more details)

Display Net GPIO Status

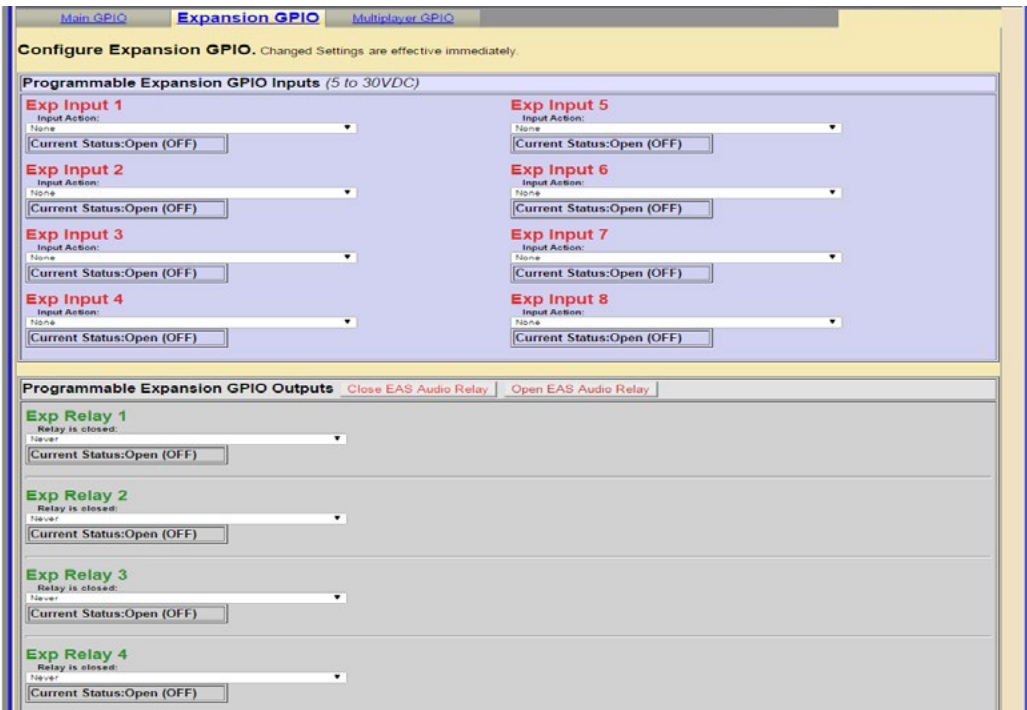
If the EAS device is configured with an external Hub Controller / Net GPIO unit, the **Display NET GPIO Status** check box will appear. Click this check box to view the Hub Controller / Net GPIO Table where the status of each GPIO is shown. To add, delete and configure a Hub Controller / Net GPIO unit go to **Setup > Net Alerts > Hub Controller / Net GPIO** screen.

MultiStation Mode

When MultiStation mode is enabled, the configured GPIO outputs are selectable for each station. A station can choose to NOT use a GPIO output. The station assignment options do not allow reprogramming of a relay, just its inclusion. This allows specific GPIO outputs to be assigned to different stations and thereby recognized as triggering an action because a specific station is active. Configure per station used GPIO output relays on the proper station interface configuration page under **Setup > Station** and use the appropriate station sub-tab(s).

Expansion GPIO

When an Expansion GPIO board is installed, the **Expansion GPIO** sub-tab is available within the **Setup > GPIO** menu. This factory installed option adds 8 more GPIO inputs and 8 more GPIO outputs. The configuration of these inputs and outputs is performed in this sub-tab.



Expansion GPIO Sub-Tab

This configuration screen works the same way as other GPIO settings. The screen is divided into two sections: **Programmable Expansion GPIO Inputs** and **Programmable Expansion GPIO Outputs**.

Programmable Expansion GPIO Inputs

The GPIO inputs are labeled **Exp Input 1 – 8**. Each input has an **Input Action** pull-down menu where users select the desired action based on triggering that input. The pull-down menu options are the same as the GPIO Input 1 selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Input Action** pull-down menus.

Programmable Expansion GPIO Outputs

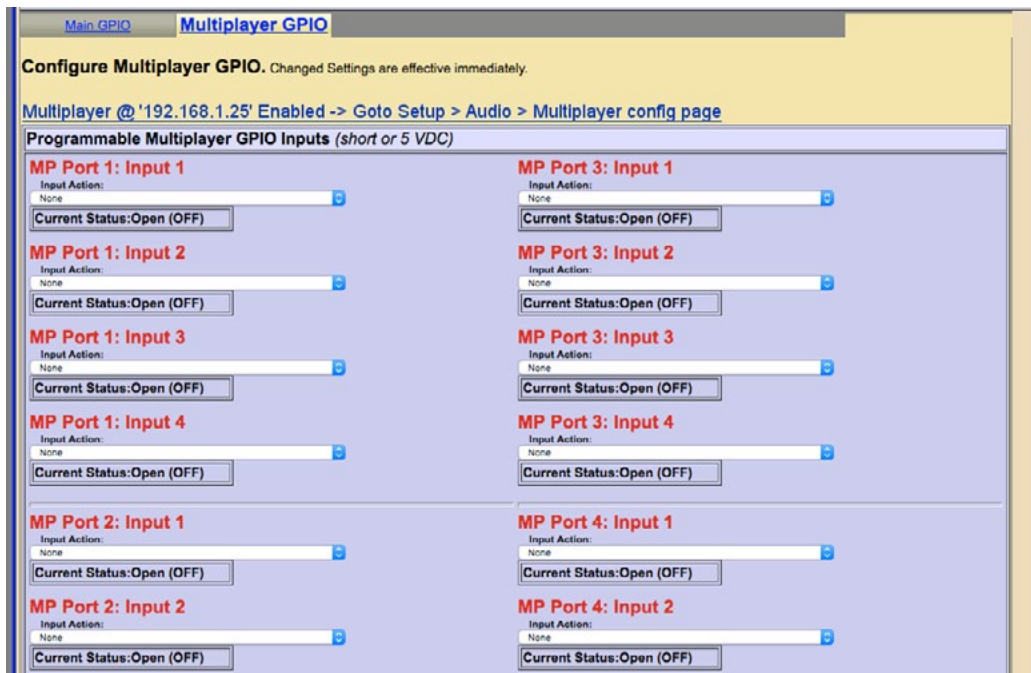
The GPIO outputs are labeled **Exp Relay 1 – 8**. Each output has a **Relay is closed** pull-down menu where users select the desired action to close the associated relay. The pull-down menu options are the same as the GPIO Output 1 Relay selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Relay is closed** pull-down menu.

After selecting an option from the **Relay is closed** pull-down menu, **FIPS Group**, **EAS Group** and **Station ID** filtering is available for most options.

Two buttons are located at the top of the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio payout. The companion button, **Open EAS Audio Relay**, sends the command to open all relays that are programmed to EAS audio payout.

Multiplayer GPIO

In situations that require an additional EAS audio playout channel (i.e. MultiStation mode), an external MultiPlayer can be added. Along with the four audio channels, the MultiPlayer includes four GPIO inputs and two GPIO outputs per audio channel. When configured, a MultiPlayer sub-tab will appear within the **Setup > GPIO** menu. MultiStation and MultiPlayer options require a valid Plus Package license key.



MultiPlayer Sub-Tab

This configuration screen works in the same way as the other GPIO settings. The screen is divided into two sections: **Programmable MultiPlayer GPIO Inputs** and **Programmable MultiPlayer GPIO Outputs**.

Programmable MultiPlayer GPIO Inputs

Each MultiPlayer audio channel (or MP Port) is numbered (1 - 4). The web interface label 'MP Port 1: Input 3' represents GPIO input 3 on MultiPlayer port 1. There is an **Input Action** pull-down menu where users select the desired action based on triggering that input. The pull-down menu options are the same as the GPIO Input 1 selections listed above.

Programmable MultiPlayer GPIO Outputs

The GPIO outputs are labeled by MP Port (1 - 4) and relay number (1 - 2). The web interface label 'MP Port 2: Relay 1' represents GPIO output relay 1 on MultiPlayer port 2. Each output has a **Relay is closed** pull-down menu where users select the desired action to close the associated relay. The pull-down menu options are the same as the GPIO Output 1 Relay selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Relay is closed** pull-down menu.

After selecting an option from the **Relay is closed** pull-down menu, **FIPS Group**, **EAS Group** and **Station ID** filtering is available for most options.

Two buttons are located at the top of the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio playout. The companion button, **Open EAS Audio Relay**, sends the command to open all relays programmed to EAS audio playout.

The **Current Status** [Open (OFF) or Closed (ON)] is displayed below each Input Action pull-down menu.

For more information regarding the installation and configuration of a MultiPlayer, see the [Quick Start Guide](#) included with the MultiPlayer or download it from the Digital Alert Systems/Monroe Electronics website.

PRINTER SETUP

A basic task associated with EAS is printing logs of alert activity. The EAS device allows multiple means to retrieve alert event information for printing logs:

- Logs can be printed from a host computer using the web browser interface
- Logs/reports can be e-mailed from the EAS device and printed on a local/network printer (see [Setup > EMail](#))
- Individual alerts can be printed directly from the EAS device

The first two options require some manual intervention. The third option and the topic of this section, will enable the automatic printout of EAS alerts as they occur. Using this approach means that each alert will print on an individual page.

Connecting to a Network Computer or Via USB

- To connect to a printer via USB, plug the printer into a USB port located on the back of the EAS device. Then click the **Follow Link to CUPS Printer Administration/Configuration** hyperlink. Click on the **Printers** tab at the top of the page. If the printer you have plugged in shows up on the page you must click **SET THE PRINTER AS THE DEFAULT PRINTER**. Then print a test page to make sure it works.
- To connect to a Network computer, go to **Setup > Printer** from a web browser interface. Click the **Follow Link to CUPS Printer Administration/Configuration** hyperlink. On the CUPS homepage, click **Add Printer**. Fill out all the information. You will need to know the IP address of the computer on the network, as well as information about the brand and model.

It is important to set your printer up as the default printer. Even if you have only one printer, at the end of your setup, you need to set that printer as default. This option is the way that CUPS communicates with the EAS device. If you do not set the printer to default, it will not work.



Attention

When filling out the Add New Printer text fields, make sure NOT to use the following characters: “/”, “#”, or space.



There is a thorough App-note on the website about connecting your printer via the Network. Go to http://www.digitalalertsystems.com/resources_application_notes.htm and find the App-note that pertains to connecting a printer to the EAS device.

Configuration

Printer Configuration.

Printer output can be automatically triggered upon alert decoding, origination, forwarding and other events. Check the appropriate toggle to set printer output events. Printing configuration is managed by the CUPS system. [Follow Link to CUPS Printer Administration Configuration](#)

Automatic Printer Output upon Alert Decode. *Disabled. Check to enable*

Automatic Printer Output upon Alert Origination. *Disabled. Check to enable*

Automatic Printer Output upon Alert Forwarding. *Disabled. Check to enable*

Automatic Weekly Printout of EAS Event Report. *Enabled. Uncheck to Disable Weekly Printout of EAS Event Report*

Automatic Monthly Printout of EAS Event Report. *Enabled. Uncheck to Disable Weekly Printout of EAS Event Report*

Automatic Monthly EAS Event Report is Categorized. *Disabled. Check to enable*

Send data a Postscript to printer. *Disabled. Check to enable*

[Accept Changes](#) [Cancel Changes](#)

[Print Test Page](#)

Printer Status

```
scheduler is running
system default destination: Eng_MCO_Print
device for Eng_MCO_Print: socket://192.168.1.22:9100
Eng_MCO_Print accepting requests since Thurs Jun 9 15:46:01 2016
Printer Eng_MCO_Print is idle. enabled since Tue Jun 19 13:01:46 2012
```

Printer Configuration Screen

There are seven check box options available, check to enable. They are:

Automatic Printer Output upon Alert Decode

When enabled, a report will be printed whenever an EAS alert is decoded.

Automatic Printer Output upon Alert Origination

When enabled, a report will be printed whenever an EAS alert is originated.

Automatic Printer Output upon Alert Forwarding

When enabled, a report will be printed whenever an active decoded EAS alert is forwarded.

Automatic Weekly Printout of EAS Event Report

When enabled, a report will be printed at midnight on Sunday morning of the previous weeks' worth of EAS activity.

Automatic Monthly Printout of EAS Event Report

When enabled, a report will be printed at midnight on the morning of the first day of the month of the previous months' worth of EAS activity.

Weekly and Monthly EAS Event Report is Categorized

When enabled, this option puts all of the prints in groups by type, and then puts them in order by date and time. The order is originated alerts, forwarded alerts, and then decoded alerts.

Send data as Postscript to printer

When enabled, Postscript data will be sent to the default printer.

Use the **Accept Change** button to save changes to this page.

Below the printer options is a system status report about the configured line printer.

When a printer is configured, the expired alert status reports displayed on the **Alert Events > Incoming, Incoming/Decoded, Forwarded Alerts, Originated/Forwarded Alerts, Originated, and All Alerts** screens provide a **Print** button. You can use the Print button to test printing as well as to print reports of retrieved events.

ALERT STORAGE SETUP

The Alert Storage Management configuration screen has storage options that enable custom event storage management by timed deletion of the following event types:

- Decoded alerts
- Forwarded alerts
- Originated alerts
- CAP alerts

Alert Storage Management configuration

Decoded, Forwarded, and Originated alerts can be saved indefinitely or for a given time period. Use the controls below to configure alert storage options.
NOTE: Disk storage space is automatically kept to a minimum of 100MB. This policy can result in old alert event audio and error files being automatically deleted and the hold time period being automatically shortened.

Decoded alert timed cleanup. Enabled. Decoded alerts will be saved for the following number of days, then moved to a holding areas for 14 days, then audio is deleted and header archived. Uncheck to Disable Decoded alert cleanup.
Decoded alerts save period (180 or more days) 365

Forwarded alert timed cleanup. Enabled. Forwarded alerts will be saved for the following number of days, then moved to a holding areas for 14 days, then audio is deleted and header archived. Uncheck to Disable Forwarded alert cleanup.
Forwarded alerts save period (180 or more days) 365

Originated alert timed cleanup. Enabled. Originated alerts will be saved for the following number of days, then moved to a holding areas for 14 days, then audio is deleted and header archived. Uncheck to Disable Originated alert cleanup.
Originated alerts save period (180 or more days) 365

CAP file timed deletion. Disabled. Check to Enable CAP file deletion after a specific time period.

Archived header file timed deletion. Disabled. Check to Enable Archived file deletion after a specific time period.

Decoder error events timed deletion. Disabled. Check to Enable Decoder error events deletion after a specific time period.

CAP Error events save period (1 or more days, 5 recommended) 5

Admin can cleanup specific expired alerts. Disabled. Check to Enable.

Rebuild Event Display Cache Files on Startup. Enabled.

[Accept Changes](#) [Cancel Changes](#)

Storage Space Chart for root device '/dev/sda3'

Total :	125927Mbytes (100%)
Used :	4263Mbytes (3%)
Available :	115268Mbytes (92%)
Reserved :	6396Mbytes (5%)

[Decoded Alerts: 301Mbytes](#) (of which [Archived alerts](#) uses 4.4Kbytes)
[EAS NET Decoded Alerts: 12Kbytes](#) (of which [Archived alerts](#) uses 4.0Kbytes)
[CAP EAS Decoded Alerts: 4.9Mbytes](#) (of which [Archived alerts](#) uses 4.5Kbytes)
[CAP Alerts: 12Mbytes](#)
[CAP Errors: 4.0Kbytes](#)(0 files)
[Forwarded Alerts: 113Mbytes](#) (of which [Archived alerts](#) uses 4.2Kbytes)
[Originated Alerts: 1.9Mbytes](#) (of which [Archived alerts](#) uses 9.3Kbytes)
[Decoding Error Files: 2.3Mbytes](#)
[Audio Files: 511Kbytes](#)

Minimum available space is maintained between 300 MB and 150 MB.

Alert Storage Setup Screen

By default, all event type data is configured to stay available on the EAS device for 365 days (unless the storage space drops below the minimum size of 100MB). Each event type is given a separate deletion control check box with a separately configurable deletion period. When enabled, event data (sound and text files) are deleted after the user-entered number of days. Timed deletion can also be completely disabled for any of the event types.

Deletion of an event consists of removing audio and text data. Event header text files are moved to the archive and always kept. Deletion does not purge the EAS device of its record of a past EAS event.

Storage Space Chart

Towards the bottom of the screen is a chart of the current storage space use. The chart shows the total capacity, the used space, available space, and reserved space in Megabytes. The storage space is further analyzed by specific alert event types. Hyperlinks are provided for each alert event type to guide the user to a directory of files for that specific alert event type.

Minimum space is maintained between 300 MB and 100 MB. If the EAS device available storage space drops below 100 Megabytes, the oldest events will be chosen for automatic deletion. This process is initiated after every alert event and at midnight every night. If a minimum space condition is detected, event data is deleted until at least 300 MB of space becomes available. The deletion time periods are also automatically adjusted downward if needed to reflect the dates of the deleted events.

Chapter 6: Alert Events Tab

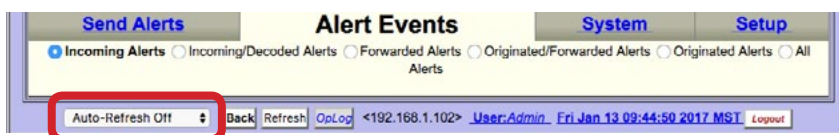
The **Alert Event** menu has six radio button options:

Radio Button	Description
Incoming Alerts	Displays the following: <ul style="list-style-type: none">• Status of Incoming and Active Decoded alerts Unacknowledged alerts can be forwarded and Demo Decoded alerts can be added from this screen.
Incoming/Decoded Alerts	Displays the following: <ul style="list-style-type: none">• Status of Incoming and Active Decoded alerts• Expired Decoded Alerts Unacknowledged alerts can be forwarded and Demo Decoded alerts can be added from this screen. EAS alert logs can be printed and/or saved.
Forwarded Alerts	Displays the following: <ul style="list-style-type: none">• Status of Active Forwarded alerts• Expired Forwarded Alerts. EAS alert logs can be printed and/or saved.
Originated/Forwarded Alerts	Displays the following: <ul style="list-style-type: none">• A list of Scheduled Originated Alerts• Current Active Originated/Forwarded Alerts• Expired Originated/Forwarded Alerts EAS alert logs can be printed and/or saved.
Originated Alerts	Displays the following: <ul style="list-style-type: none">• A list of Scheduled Originated Alerts• Current Active Originated Alerts• Expired Originated Alerts EAS alert logs can be printed and/or saved.
All Alerts	Displays the following: <ul style="list-style-type: none">• A list of Scheduled Originated Alerts• Current Active Alerts• Expired Alerts EAS alert logs can be printed and/or saved.

Each radio button brings up status display screens of current and expired alerts. These screens show the active alerts and those that have expired or have been decoded, forwarded, and originated. These screens allow a precise audit of current and past EAS activity.

Auto-Refresh Timer

With a Plus Package license key, the web interface displays an **Auto-Refresh Timer** (just below and to the left of the page title in the header section) allowing the page to be re-displayed every 15, 30, or 60 seconds. Use this option to stay informed of the EAS device's decoding activity and decoded events status.



Decode Activity	WIHAML1>Main Left	WDVIR1>Main Right	NOAA(L2)-Aux 1 Left	IC-Aux 1 Right ID=4609 RWT HDR>
Station ID: WME Global Manual Forward Mode				

Decode Activity Table

Decode Activity Table

The Incoming Alerts, Incoming/Decoded Alerts, and Forwarded Alerts screens include the Decoder Activity Table which displays the input decoders for reference purposes. Each decoder channel has its own box in the table. When there is no incoming alert the channel is light blue. When there is an incoming decoding alert, the channel display box is red and displays the current state of the incoming decoding alert. In the screen shot below, event 4668, a Required Weekly test (RWT), is in process of being decoded, and the full header has been received (HDR>). The **Decode Activity** hyperlink takes users to the **Setup > Audio > Decoder Audio** screen.

Station ID and Global Forwarding Mode

Just below the **Decode Activity** table are hyperlinks for **Station ID** and **Global Forwarding Mode** (either Manual Forward Mode or Auto-Forward Mode). Both hyperlinks take users to the **Setup > Station > Global Options** screen.

- In Auto-Forward mode, alerts that match the auto-forwarding criteria are automatically forwarded (played).
- In Manual mode, no decoded alerts are forwarded. Active alerts have a button allowing manual forward.
 - With the Plus Package license key unlocked, if GPI input is properly programmed, an unforwarded active alert can be forwarded via GPI contact closure. The Plus Package license also allows Manual Forwarding to be blocked for specific alerts that do not match the Auto-Forwarding filter criteria.

View alert forwarding action table (uncheck to remove view).

Alert Forwarding Action Table (follow links to configure)								
Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1.2	Net Switch	Hub Ctrl	Analog Video	Audio
OFF	ON	ON	ON	N/A	OFF	ON	ON	Front Main
U:Unlicensed N/A:Unsupported								

Alert Forwarding Action Table

Alert Forwarding Action Table (Incoming Alerts & Incoming/Decoded Alerts)

Below Active Decoded Alerts is the optional Alert Forwarding Action Table. It displays current settings for actions associated with forwarding the alert. The serial protocol, the Net Alert protocols, and the Analog Audio/Video states are displayed to make it easy to know what peripheral devices is triggered by alert forwarding. Labels inside this table are hyperlinks directing the web interface to the correct Setup page for changing the configuration of the associated action.

Play audio alarm on browser when page has unacknowledged, active unforwarded alert. *Requires Flash plugin on host computer browser*

View Direct Event Storage Access

[Decoded Files](#) [Decoding Error Files](#) [EAS NET Decoded Files](#)
[CAP EAS Decoded Files](#) [CAP Files](#) [CAP Error Files](#)
[Forwarded Files](#) [Originated Files](#)

Generate Decoded Event Index File

L1 Last Post Decoded Alert Snapshot (Sun Jun 12 20:44:55 2016):
[L1_post_alert_snapshot.wav](#)
R1 Last Post Decoded Alert Snapshot (Sat May 14 08:50:10 2016):
[R1_post_alert_snapshot.wav](#)
L2 Last Post Decoded Alert Snapshot (Mon Jul 14 09:42:06 2014):
[L2_post_alert_snapshot.wav](#)
R2 Last Post Decoded Alert Snapshot (Tue Dec 8 10:03:02 2015):
[R2_post_alert_snapshot.wav](#)

Direct Event Storage Access Table

Direct Event Storage Access table *(applies to Incoming Alerts & Incoming/Decoded Alerts only)*

To the right of the Alert Forwarding Action Table is the Direct Event Storage Access Table with hyperlinks to Decoded Files, Decoding Error Files, EAS NET Decoded Files, CAP EAS Decoded Files, CAP Files and CAP Error Files. These hyperlinks navigate the web interface into the disk file storage area for decoded alerts; EAS NET decoded alerts, and errored alerts. Navigating one of the hyperlinks will place the web interface into a file view where all alert event files can be directly examined and downloaded. This is useful if an alert could not be decoded. The WAV file saved during the decode error can be downloaded and examined or sent to Digital Alert Systems/Monroe Electronics for analysis.

The Generate Decoded Event Index File can be toggled to generate a monthly index file of alerts received. Use it to automate queries of alert activity. Index files are stored in the Decoded Files storage area and are named "events_YYYY_M(M)".



Note
All options within the Alert Events tab are immediate and do not require the Accept Changes button to become active.

Incoming Alerts Screen

INCOMING ALERTS

This screen shows the status of Incoming and Currently Active Decoded Alerts. The **Incoming Alerts** screen monitors new and incoming EAS alert activity. Broadcasters who manually forward alerts should stay logged into the EAS device to view the **Incoming Alerts** screen with the auto-refresh option enabled.

The **Incoming Alerts** screen displays the status of all incoming alerts “received” by the EAS device. This screen contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Event Storage Access Table (described above)

Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Add Demo Decoded Alert
- Acknowledge Pending Alerts
- Forward Alerts
- Edit/Review Forwarding Text/Audio

This screen does not provide the interface for accessing expired alerts – this is found in the section: Incoming/Decoded Alerts.

All other interfaces on this web page are described in the Incoming/Decoded Alerts below.

INCOMING/DECODED ALERTS

Incoming/Decoded Alerts indicates the status of Incoming, Active and Expired Decoded Alerts. It is the primary interface for viewing current and past decoding activity. It displays the current forwarding mode (auto-forward or manual), current decoding activity (active alerts), the alert forwarding action table, event storage access table, active decoded EAS alerts, and expired decoded EAS alerts.

The **Incoming/Decoded Alerts** screen displays status of all incoming and decoded alerts “received” by the EAS device. This screen contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Event Storage Access Table (described above)
- Expired Decoded Alerts

Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Add Demo Decoded Alert
- Acknowledge Pending Alerts
- Forward Alerts
- Edit/Review Forwarding Text/Audio
- Review expired Incoming/Decoded EAS alerts
- Display, save, and print EAS message logs



Note

Under normal operation, disable the display of both of these tables to speed up the page load and refresh.

Incoming/Decoded Alerts Screen with Active Alert

Add Demo Decoded Alert

If the Demo Decode Alert mode is not enabled, go to **Setup > Demo/Practice** to enable it. This will make the **Add Demo Decoded Alert** button appear on the screen.

When Demo mode is enabled, simulate a newly decoded alert using the **Add Demo Decoded Alert** button shown below the Decode Activity Table. Pressing the button will generate an EAS DMO alert (Demo/Practice alert) and place it in the active decoded alert queue. This is a quick, convenient way to test the forwarding options. The Demo Alert is a real EAS alert and will have the same Manual Forwarding and Edit/Review button options as any other decoded alert. This is especially useful for practice and training of the Manual Forwarding options. Demo Alerts are set to a fixed duration of 15 minutes.

Configure Demo Decoded Alert hyperlink

This text to the right of the **Add Demo Decoded Alert** button is a hyperlink to the **Setup > Demo/Practice** screen. From this screen the user can enable the Add Demo Decoded Alert button/feature and configure the parameters of the DMO alert message (see [Chapter 5 - Demo/Practice](#)).

Currently Active Decoded Alerts

These alerts are below the Decode Activity Table and displays all decoded EAS alerts currently in progress between the start and end time for the alert. An active event remains on the active list until it reaches its expiration time, or until it is updated or canceled by another event of the same type and for the same area, which redefines the event times. Decoded alerts appear in the Currently Active Decoded Alerts list as long as they are current. Active events move to the expired alert list as each one reaches its end time.

Forwarded active events display the forwarding time as an active link label on the **Alert Events > Forwarded Alerts** status page.



Warning

Forwarding a DEMO alert will take it to AIR! BE CAREFUL: Examine if Auto-Forward Mode is enabled before use. Make sure your EAS broadcast system is off line during practice.

Active events that are not automatically forwarded present buttons to allow review and editing, acknowledgment, and manual forwarding / re-enable manual forwarding. These buttons are described below.

Acknowledge Pending Alert

The screen shot above shows an active, unacknowledged, unforwarded alert for the active Demo alert. Decoded alerts that have not been forwarded or acknowledged will be in an *unacknowledged* state. This state is indicated on the EAS device's front panel status LED with a blinking slowly/regularly red light and within the web interface active alert status display by a flashing button labeled **Acknowledge Pending Alert**. To end the unacknowledged state and stop the front panel red status LED from flashing, click the flashing **Acknowledge Pending Alert** button. You can also acknowledge an alert by pressing the front panel button once or a by a programmed GPIO closure. Any alert that remains unacknowledged or unforwarded will remain in this state until it expires.

Chnl/Orig	EAS Type	ID	Start Time	End Time	Location
DEMO from WME1 (EAS)	DMO <i>Node: DFLT</i>	586	Mon Jun 13 17:30:00 2016 MDT	Mon Jun 13 17:45:00 2016 MDT	Orleans, NY (036073) Genesee, NY (036037) Livingston, NY (036051)

Decoded as: A broadcast or cable system has issued A PRACTICE/DEMO WARNING for the following counties/areas: Orleans; Genesee; Livingston, NY; at 5:30 PM on JUN 13, 2016 Effective until 5:45 PM. Message from WME1.
Event Log: Practice/Demo Alert started Mon Jun 13 17:30:00 2016 MDT

Decoded EAS String:
ZGZC EAS-DMO-036073-036037-036051+0016-1652330 WME1-

Forwarding Alert Text Translation:(Length=432) Uses decoded alert text.
A broadcast or cable system has issued A PRACTICE/DEMO WARNING for the following counties/areas: Orleans; Genesee; Livingston, NY; at 5:30 PM on JUN 13, 2016 Effective until 5:45 PM. Message from WME1. Una estación emisora o un operador de cable emitió una Advertencia de Práctica/Demostración Para los siguientes condados: Orleans; Genesee; Livingston, NY; En 5:30 PM de JUN 13, 2016 Efectivo hasta 5:45 PM. Un mensaje de WME1.

This alert can have the broadcast translation edited prior to forwarding. Select one of the forwarding EAS and Custom text translation options:

- Primary and Secondary Langs EAS Text Translation
- Primary Lang EAS Text Translation + Custom + Secondary Lang EAS Text Translations
- Custom + Primary and Secondary Langs EAS Text Translations
- Custom Text Translation Only - No EAS Text Translation

Max translation size = 432

Original alert audio can be replaced. Make selection.
Original Audio
Canadian_Alerting_Attention_Signal_(8sec).wav

Optional Pre-Alert Audio Announcement (played before EAS Header audio)
No Audio

Optional Post-Alert Audio Announcement (played after EAS EOM audio)
No Audio

No audio message for this alert.

Record Audio File [Goto to -> Setup Audio Output Levels](#)

Total EAS FSK+Audio Duration: 11.49 seconds

OK Cancel

Upload Audio .WAV file to One-Net Server.
Choose File No file chosen
Upload .WAV file

Edit/Review Decoded Alert for Forwarding Screen

Edit/Review Forwarding Text/Audio

To review and edit the alert audio before forwarding, click the **Edit/Review Forwarding Text/Audio** button. This button displays the **Edit/Review Decoded Alert for Forwarding** screen. It allows you to:

- Play the original audio, select a new audio message from the local audio file list, upload or record new audio, add audio announcements to be played prior to or after alert play-out.
- If the Plus Package license key is unlocked, you can add text that will be displayed on the local CG during forwarding.



Note
If a decoded alert expires during edit/review, it cannot be forwarded after exiting the Edit/Review Decoded Alert for Forwarding screen.

The active decoded event is displayed as well as the translations that will be used when the alert is manually forwarded. Make changes as needed, and choose either the OK or Cancel buttons to return to previous alert status page.

Forward Alert button

The Forward Alert button will manually forward the alert. Once the alert is forwarded this button disappears from the active alert event display and is replaced by an **Enable Reforward** button, While an alert is actively being forwarded, a flashing indicator will display near the top of the page. A link labeled Forwarded followed by the time of forwarding, will also be displayed. Follow the link to the **Alert Events > Forwarded Alerts** page.

Add Demo Decoded Alert Configure Demo Decoded Alert					
Currently Active Decoded Alerts					
3 alert records displayed.					
Chnl/Orig	EAS Type	ID	Start Time	End Time	Location
DEMO from WME1 (EAS)	DMO Node: WWS Node:	598	Tue Jun 14 08:29:00 2016 MDT Forwarding blocked for this event.	Tue Jun 14 08:44:00 2016 MDT	Orleans, NY (036073)
Decoded as: A broadcast or cable system has issued A PRACTICE/DEMO WARNING for the following counties/areas: Orleans, NY, at 8:29 AM on JUN 14, 2016 Effective until 8:44 AM. Message from WME1. Total EAS FSK+Audio Duration: 18.94 seconds Event Log:Practice/Demo Alert started Tue Jun 14 08:29:00 2016 MDT					

Blocked Alert Example

Blocked Forwarding

Any alert to be blocked will be displayed in the **Currently Active Decoded Alerts** list. A hyperlink will appear in the Start Time column titled **Forwarding blocked for this event**. Clicking this hyperlink will take the user to the **Setup > Alert Agent™ > Manage Alert Nodes** screen where the Alert Node was configured to block the alert.

Enable Reforward

Use the **Enable Reforward** button to allow a previously forwarded alert to be manually forwarded again. After this button is pressed, the **Forward Alert** button will again be displayed.



Note
With a valid Plus Package, the **Setup > GPIO** screen allows the **Enable Reforward** button to be triggered from a GPIO input contact closure by selecting **Re-enable forwarded EAS alert**.

Select Expired Alert View
 View Expired Alerts View Expired Alerts Pending Deletion View Deleted Expired Alerts

Expired Alerts

301 Records from : 'Wed Mar 9 14:50:21 2016 MST' through 'Thu Feb 9 03:07:15 2017 MST'
 User defined range of alerts : **Expired Alerts Display Control**

Display FROM: 2016 Year Mar Month 10 Day TO: 2017 Year Feb Month 9 Day [Submit Dates](#)

[Click for text version.](#) Text version: Categorize alerts. Disabled.
 Alert records 1 to 150 of 299 displayed. [151-299](#)

Chnl/Orig	EAS Type	ID	Start Time	End Time	Location <small>(Limit)</small>
KSL (L1) from KSOPAMFM (EAS)	RWT <small>Node: 'DFLT'</small>	1372	Thu Feb 9 03:07:00 2017 MST Decoded Thu Feb 9 03:07:24 2017 MST	Thu Feb 9 04:07:00 2017 MST	Salt Lake, UT (049035)
<small>Decoded as: A broadcast or cable system has issued A REQUIRED WEEKLY TEST for the following counties or areas: Salt Lake, UT, at 3:07 AM on FEB 9, 2017 Effective until 4:07 AM. Message from KSOPAMFM.</small>					
Orig from WME TV (EAS)	RWT	1365	Mon Feb 6 15:27:00 2017 MST Originated To Station: 'WME TV 1' Mon Feb 6 15:27:00 2017 MST	Mon Feb 6 15:42:00 2017 MST	Orleans, NY (036073)
<small>A BROADCASTER has issued A REQUIRED WEEKLY TEST for the following counties or areas: Orleans, NY, at 3:27 PM on FEB 6, 2017 Effective until 3:42 PM. Message from WME TV.</small>					
Orig from WME TV (EAS)	RWT	1329	Thu Feb 2 05:01:00 2017 MST Originated To Station: 'WME TV 1' Thu Feb 2 05:01:00 2017 MST	Thu Feb 2 05:16:00 2017 MST	Orleans, NY (036073)
<small>A BROADCASTER has issued A REQUIRED WEEKLY TEST for the following counties or areas: Orleans, NY, at 5:01 AM on FEB 2, 2017 Effective until 5:16 AM. Message from WME TV.</small>					

Expired Alerts Section

View Expired Alerts

These check boxes enable the display of the following expired alerts:

- Expired Alerts (complete audio, text and aux data is stored on disk)
- Expired Alerts Pending Deletion (pending audio file deletion)
- Deleted Expired Alerts (expired alerts that have had audio data deleted)

Use these radio buttons to select the types of expired alerts to be viewed. Each of the listed alerts contain hyperlinks and a button that can be used to review the specific expired alert.

The deleted alerts viewer will only show events if Alert Storage management is enabled. Select **Setup > Alert Storage**, and choose a date range for alert records. The screen shot below shows the most commonly used option **View Expired Alerts**. The other two options present the same interface.

Expired Decoded Alerts list

The Expired event list shows past decoded alerts for any range of dates. Use the pull-down menu titled **Expired Alerts Display Control** to view a multitude of date range options. A user defined date range is available enabling custom start and end dates (year, month, day). The screen shot shows an example of the expired alerts list for a selected range of dates.

Select Expired Alert View
 View Expired Alerts View Expired Alerts Pending Deletion View Deleted Expired Alerts

Expired Decoded Alerts

61 Records from : 'Tue Dec 8 08:38:53 2015 MST' through 'Tue Jun 14 07:29:57 2016 MDT'
 User defined range of alerts : **Expired Alerts Display Control**

Display FROM: 2016 Year May Month 3 Day TO: 2016 Year Jun Month 14 Day

[Click for text version.](#) Text version: Categorize alerts. Disabled.
 41 alert records displayed.

Chnl/Orig	EAS Type	ID	Start Time	End Time	Location <small>(Limit)</small>
WHAM (L1) from KSL(A/F) (WXR)	SVR <small>Node: 'DFLT'</small>	581	Mon Jun 13 17:45:00 2016 MDT Decoded Mon Jun 13 17:54:05 2016 MDT	Mon Jun 13 18:15:00 2016 MDT	Tooele, UT (049045) Box Elder, UT (049003) Davis, UT (049011) Weber, UT (049057)
<small>Decoded as: The National Weather Service has issued A SEVERE THUNDERSTORM WARNING for the following counties/areas: Tooele; Box Elder; Davis; Weber, UT, at 5:45 PM on JUN 13, 2016 Effective until 6:15 PM. Message from KSL(A/F).</small>					
<small>Audio Portion : Play -> Front Panel Listen on Browser Duration: 118.577 seconds</small>					

Expired Alerts Section – Custom Date Range

Set the Date Range

Whatever Expired Alert View is selected, the number of expired alert records and the earliest to latest dates for these expired alerts is displayed. Control the expired alerts display date range by entering a from/to date. All expired alerts between and including these dates will be displayed in order.

To select a date range, select **User defined range of alerts** from the **Expired Alerts Display Control** pull-down menu. Next, choose a Year, Month, and Day for the FROM and TO dates. Make sure to click the **Submit Dates** button when finished entering the date range. All data for each expired alert decoded within the selected time period will display. Decoded headers are stored on the EAS device. This information is an accurate reflection of what was received. The EAS device can archive an enormous number of expired events and will automatically remove the oldest event descriptions as needed to reserve enough space for new alerts, however storage capacity is in the thousands so do not worry about losing important archived information.

A text version is available. Select the option **Click for text version**. This will display a text file copy of the current range of expired alerts in the browser. To categorize this text version by EAS codes, use the **Text version: Categorize alerts** check box. Otherwise the text version will be organized by date of alert.

If a printer is enabled, a **Print** button will display to the right of the link **Click for text version**. This will print the text version of the displayed alerts. You may print the event status page to compile FCC paper documents for EAS test accounting.

Expired Alerts Display

Details about the alert is displayed in a table:

- The time the alert was decoded
- The time the alert was forwarded, and if it was forwarded

Forwarded alerts are displayed on the **Forwarded Alerts** or **Originated/Forwarded Alerts** screen.

Audio Portion

An alert with an audio message, can be played through the EAS device front panel internal speaker by clicking **Play->Front Panel** button inside the online alert entry area. You can also play the audio file on your host computer by clicking on **Listen on Browser** hyperlink. To listen to the audio, the host computer must have a WAV file player. Alerts without an audio message will not display either the **Play->Front Panel** button or **Listen on Browser** hyperlink.

TDX portion

If the alert has TDX details data, information is appended to the text translation for the alert. Also, links to any TDX-provided URL information is displayed. These links can be followed to go to web pages with more detailed information relevant to the alert. TDX details must originate from the alert source.

Play audio alarm on browser

On the right side of the page, under the Active Decoded alert table, is the **Play audio alarm on browser when page has unacknowledged, active unforwarded alert** check box to control an audible browser announcement for active, decoded alerts that have not yet been acknowledged or forwarded. Enabling this option on a speaker-equipped computer, along with an auto-refresh, can audibly notify control room staff that an alert has been decoded. Every time the browser page



Note

The text file display is outside of the standard EAS device web interface. If selected, use the web browser **BACK** button to return to the EAS device web interface.

refreshes while a decoded alert remains unacknowledged and unforwarded, an audio recording of the three burst EAS end-of-message “noise” will play over the host computer’s speakers. The audio notification will stop once the alert is forwarded or acknowledged. An alert can be acknowledged using the **Acknowledge Pending Alert** button on the active alert status display, by pressing the EAS device’s Front Panel button, or a programmed GPIO input closure.



Note
Adobe Flash Player must be installed for the audio notification to work.

Incoming & Incoming/Decoded Alerts: Multistation Mode

The active decoded alerts display supports MultiStation mode. You can view the active (enabled) stations on the right side of the page above the active decoded alerts table. Within the active decoded alert status, a target station ID and a **Forward Alert** button is displayed for each enabled station. Alerts can be forwarded to any station by pressing the appropriate **Forward Alert** button. The screen shot below shows one active, unacknowledged decoded alert, with two available enabled station targets and thus, two **Forward Alert** buttons, one per station. A single **Acknowledge Pending Alert** and **Edit/Review Forwarding Text/Audio** button is provided to cover MultiStation mode.

Chnl/Orig	EAS Type	ID	Start Time	End Time	Location
DEMO from WME2 (EAS)	DMO Node: "NWS Node"	605	Tue Jun 14 10:30:00 2016 MDT	Tue Jun 14 10:45:00 2016 MDT	Orleans, NY (036073)

Station	Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1,2	Net Switch	Hub Ctrl	Analog Video	Audio
Station 1	OFF	OFF	OFF	OFF	N/A	OFF	OFF	OFF	Main Front
Station 2	OFF	OFF	OFF	OFF	N/A	OFF	OFF	ON	Front Main

Active Decoded Alerts – MultiStation Mode

A severe EAS alert may need to be forwarded faster than to each enabled station in sequence. In that case, a separate button, labeled **Forward Alert Once for All Stations**, is available and can be pressed to forward the alert to the Main station configuration. If this button is used, all stations will forward immediately.



Note
In MultiStation mode, to customize the alert audio/text translation, you must run the Edit/Review process separately before station forwarding.

Alert Forwarding Action Table

Below the active alerts, the Alert Forwarding Action Table supports multiple station status by displaying the enabled and disabled actions per station. They may be changed at any time prior to forwarding in order to affect the outcome of actions when an alert is forwarded to a specific station. Follow the station name links to the **Setup > Station** (and appropriate station sub-tab) to change the desired settings for station alert forwarding.

View alert forwarding action table (uncheck to remove view).

Alert Forwarding Action Table (follow links to configure)									
Station	Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1.2	Net Switch	NET GPIO	Analog Video	Audio
WME TV 1	VIDEOSTAMP	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front
WME TV 2	CODI	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front
WME TV 3	CODI	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front

U:Unlicensed N/A:Unsupported

Alert Forwarding Action Table

After an alert is forwarded to a station, the **Forward Alert** button is replaced by the **Enable Rereward** button with a message showing the time of forwarding to the station name. This message is an active link to the **Alert Events > Forwarded Alerts** screen. Follow that link to view the status of the forwarded alert. The image below shows the display for an active decoded alert after forwarding to the second station.

Currently Active Decoded Alerts					
1 alert records displayed.					
Chnl/Orig	Code	ID	Start Time	End Time	Location
DEMO from WKDQ.FM (EAS)	DMO	9	Tue Jun 19 13:42:00 2012 EDT	Tue Jun 19 13:57:00 2012 EDT	Orleans, NY (036073) Genesee, NY (036037) Monroe, NY (036055) Niagara, NY (036063) New York (036000)
			Station: 'Station 1' *Retranslates alert text	Forward Alert	
			Forwarded to Station: 'Station 2' Tue Jun 19 13:44:49 2012 EDT	Enable Rereward	
			Station: 'Station 3' *Uses decoded alert text	Forward Alert	
			Forward Alert Once for All Stations	*Uses decoded alert text	
			Edit/Review Forwarding Text/Audio		
Decoded as: THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A PRACTICE/DEMO WARNING FOR THE FOLLOWING COUNTIES/AREAS: Orleans; Genesee; Monroe; Niagara, NY; New York; AT 1:42 PM ON JUN 19, 2012 EFFECTIVE UNTIL 1:57 PM. MESSAGE FROM WKDQ.FM.					
Audio Portion : Play->Front Panel Listen on Browser Duration: 11.699 seconds					
Total EAS FSK-Audio Duration: 34.43 seconds					
Event Log: Practice/Demo Alert started Tue Jun 19 13:42:14 2012 EDT					

Active Decoded Alerts – MultiStation Mode w/ Enable Rereward button

Below is an example of the changes to the alert display after using the other **Forward Alert** buttons. The screen shot shows the active decoded alert status after forwarding to the first, second, and third enabled station, and after forwarding to all stations once (using the **Forward Alert Once to All Stations** button for forwarding to all stations simultaneously). This screen also shows the **Enable Reforward** buttons which can be pressed to once again enable the Forward Alert button per station (or for all stations).

Currently Active Decoded Alerts					
1 alert records displayed.					
Chnl/Orig	Code	ID	Start Time	End Time	Location
DEMO from WKDQ FM (EAS)	DMO	9	Tue Jun 19 13:42:00 2012 EDT	Tue Jun 19 13:57:00 2012 EDT	<i>Orleans, NY (036073)</i> <i>Genesee, NY (036037)</i> <i>Monroe, NY (036055)</i> <i>Niagara, NY (036063)</i> <i>New York (036000)</i>
			Forwarded to Station: 'Station 1' Tue Jun 19 13:45:47 2012 EDT <input type="button" value="Enable Reforward"/>		
			Forwarded to Station: 'Station 2' Tue Jun 19 13:44:49 2012 EDT <input type="button" value="Enable Reforward"/>		
			Forwarded to Station: 'Station 3' Tue Jun 19 13:45:53 2012 EDT <input type="button" value="Enable Reforward"/>		
			Forwarded Tue Jun 19 13:46:04 2012 EDT <input type="button" value="Enable Reforward Once for All Stations"/>		
<i>Decoded as:</i> THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A PRACTICE DEMO WARNING FOR THE FOLLOWING COUNTIES/AREAS: Orleans; Genesee; Monroe; Niagara, NY; New York; AT 1:42 PM ON JUN 19, 2012 EFFECTIVE UNTIL 1:57 PM. MESSAGE FROM WKDQ FM. <i>Audio Portion :</i> Play->Front Panel Listen on Browser <i>Duration:</i> 11.699 seconds <i>Total EAS FSK+Audio Duration:</i> 34.43 seconds <i>Event Log:</i> Practice Demo Alert started Tue Jun 19 13:42:14 2012 EDT					

FORWARDED ALERTS

Forwarded Alerts contain the same detailed alert information about Forwarded Alerts as previously discussed in the Alert Events section. They are organized alike, without the options for the Forwarding Action table, Play audio alarm, and the Event Storage Access Table.

The **Forwarded Alerts** screen displays the status of all forwarded alerts and contains the following sections:

- Currently Active Forwarded Alerts
- Expired Forwarded Alerts

Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Review expired Forwarded EAS alerts
- Display, save, and print EAS message logs

Forwarded Alerts: MultiStation Mode

The **Forwarded Alerts** screen indicates which alerts have been forwarded to MultiStation mode enabled stations. They display the station ID in the Event Status Table for each forwarded alert. The bottom two DMO alerts below show that one Demo alert has been forwarded sequentially to two different enabled stations.

This screen shot also shows the active Forwarded Alerts display after the same decoded alert was forwarded to all stations using the **Forward Alert Once to All Stations** button (top DMO alert). It replaces the two active alerts forwarded earlier to the individual stations. The active alerts for the two stations are updated by this new forwarded alert and thus have expired.

The screenshot shows a software interface with a header bar containing several tabs: 'Decode Activity', 'KSL-AM(1)-Main Left', 'WQV(F1)-Main Right', 'NOAA(L2)-Aux 1 Left', and 'R2-Aux 1 Right'. Below the header, there are two active stations listed: '2 Active Stations : 2 Visible' and 'Global Manual Forward Mode'. The main content area is titled 'CURRENTLY Sending Alert:DMO' and 'Currently Active Forwarded Alerts'. It displays '3 alert records displayed.' and a table with the following columns: 'Chnl/Orig', 'EAS Type', 'ID', 'Start Time', 'End Time', and 'Location'. The table contains three rows of alert records, each with detailed information including the station of origin, the alert type (DMO), the ID (606), the start and end times, and the location (Orleans, NY (036073)). Each record also includes a description of the alert and links for audio playback.

Chnl/Orig	EAS Type	ID	Start Time	End Time	Location
DEMO from WME (EAS)	DMO	606	Tue Jun 14 11:01:00 2016 MDT Forwarded To Station: 'Override' Tue Jun 14 11:04:02 2016 MDT	Tue Jun 14 11:16:00 2016 MDT	Orleans, NY (036073)
DEMO from STATION2 (EAS)	DMO	606	Tue Jun 14 11:01:00 2016 MDT Forwarded To Station: 'Station 2' Tue Jun 14 11:03:14 2016 MDT	Tue Jun 14 11:16:00 2016 MDT	Orleans, NY (036073)
DEMO from STATION1 (EAS)	DMO	606	Tue Jun 14 11:01:00 2016 MDT Forwarded To Station: 'Station 1' Tue Jun 14 11:02:25 2016 MDT	Tue Jun 14 11:16:00 2016 MDT	Orleans, NY (036073)

ORIGINATED/FORWARDED ALERTS

The **Originated/Forwarded Alerts** screen displays the status of all alerts “sent” from the EAS device. Three sections display the following:

- Scheduled Originated Alerts
- Currently Active Originated/Forwarded Alerts
- Expired Originated/Forwarded Alerts.

Users may perform the following actions from this screen:

- Review expired Originated and Forwarded EAS alerts
- Display, save, and print EAS message logs

Scheduled Originated Alerts

This section lists scheduled alerts. Typically, it is populated with the next Required Weekly Test when Automatic Random Required Weekly Test Generation is turned on (see [Chapter 5 - Station > Main](#)).

Currently Active Originated/Forwarded Alerts

This section lists originated and forwarded currently active alerts.

Expired Alert View

As with the other event status views, you may choose View Expired Alerts, View Expired Alerts Pending Deletion, or View Deleted Expired Alerts. (See the [Incoming/Decoded Alerts section](#) for more information about the options in this section.)

Expired Originated/Forwarded Alerts

This section displays the total number of expired and currently active originated and forwarded alerts, and offers the same expired alert event viewer as the other event viewers.

The **Date Range** field sets a date range to display alerts.

ORIGINATED ALERTS

The **Originated Alerts** screen displays the status of all originated alerts “sent” from the EAS device. Three sections display the following:

- Scheduled Originated Alerts
- Currently Active Originated Alerts
- Expired Originated Alerts

Users may perform the following actions from this screen:

- Review expired Originated EAS alerts
- Display, save, and print EAS message logs

This screen operates in the same way as other **Alert Events** screens but only displays Originated Alerts.

ALL ALERTS

The **All Alerts** screen is typically used to view or print all activity for a selected date range. This screen displays the following sections:

- Scheduled Alerts
- Currently Active Alerts
- Expired Alerts

Users may perform the following actions from this screen:

- Review all expired EAS alerts
- Display, save, and print EAS message logs

This screen functions in the same way as other Alert Events screens.

Scheduled Alerts

This section lists scheduled alerts.

Currently Active Alerts

This section lists all currently active alerts.

Expired Alert View

As with the other event status views, you may choose to view Expired Alerts, Expired Alerts Pending Deletion, or Deleted Expired Alerts.

Expired Alerts

This section lists all EAS device expired alerts. Decoded, Forwarded and Originated (labeled Encoded) alerts are clearly labeled in order to distinguish between them.

Use the **Date Range** field to set a date range to display alerts.

BACKING UP EAS EVENT LOGS

The following provides step-by-step instructions on how to back-up EAS event logs. On those occasions when manually backing-up EAS events is desirable, these steps will assist in exporting the selected logs to a local computer.

1. Log into the DASDEC/One-Net.
2. Go to **Alert Events**



Note
Establishing an **EAS Event Report by EMail** is the preferred method of exporting EAS event logs. The EMail method sends regular (weekly/monthly) and automated e-mail messages to the configured address(es). These e-mails may be used for FCC filings.

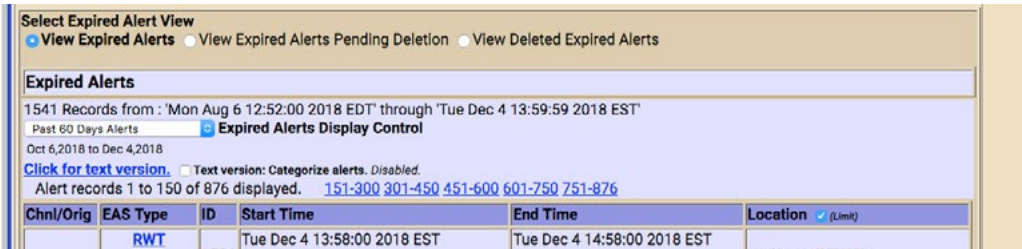
Alert Events Screen

3. Depending the types of logs desired use the radio button to select one of the following:
 - Incoming / Decoded Alerts
 - Forwarded Alerts
 - Originated / Forwarded Alerts (*This is the typical selection for FCC logging purposes*)
 - Originated Alerts
 - All Alerts
4. Scroll down and find **Select Expired Alert View** and make sure the radio button **View Expired Alerts** is selected

Select Expired Alert View Section of Alert Events Screen

5. The blue area reflects the EAS logs that have been processed within the above selections.

- The total number of records is shown (above the 'Expired Alerts Display Control' pull-down) along with the date range. These EAS records are sorted from earliest (at top of list) to latest dates.



Select Expired Alert View Section of Alert Events Screen

- Use the **Expired Alerts Display Control** pull-down menu to further refine the records displayed.
- Once the desired list is displayed, clicking the **Click for text version** hyperlink will produce a text-only web-page representation of the selected data.
 - Standard web-page print functions will allow these logs to be printed.

```

Expired originated/received/forwarded alerts:
-----
Summary: "DASDEC-18 EAS" # 132,148 : 15
DASDEC-18 EAS Report at "Tue Dec 4 13:58:00 2018 EST"
From "Sat Oct 6 00:00:00 2018 EDT" to "Wed Dec 5 00:00:00 2018 EDT"
-----
225699: XWT RECEIVED WEEKLY TEST 'CAP' (PANSWCAP) ORG-CIV
  "Sat Oct 6 04:00:00 2018 EDT" to "Sat Oct 6 04:10:00 2018 EDT"
  Originated: "Sat Oct 6 04:07:33 2018 EDT"
  (EASID: CA124893)
-----
225699: XWT RECEIVED WEEKLY TEST 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 14 19:00:00 2018 EDT" to "Sun Oct 14 20:00:00 2018 EDT"
  Decoded: "Sun Oct 14 19:00:00 2018 EDT"
  Comp(SM6203) Northern Mariana Islands(165000)
  Event Log:VERIFIED Digital Signature UNTESTED/decoded CA certificate.. update CAP decoder CA file!!
-----
225699: XWT FIRE WARNING 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 15 09:37:00 2018 EDT" to "Sun Oct 15 09:52:00 2018 EDT"
  Decoded: "Sun Oct 15 09:37:00 2018 EDT"
  (EASID: CA124893)
  Event Log:Digital Signature VERIFICATION ERROR: Signer UNTESTED: Check for correct CAP decoder CA file..
-----
225701: XWT SHELTER IN PLACE WARNING 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 15 09:37:00 2018 EDT" to "Sun Oct 15 09:52:00 2018 EDT"
  Decoded: "Sun Oct 15 09:37:00 2018 EDT"
  (EASID: CA124893)
  Event Log:Digital Signature VERIFICATION ERROR: Signer UNTESTED: Check for correct CAP decoder CA file..
-----
225701: XWT RECEIVED WEEKLY TEST 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 15 09:00:00 2018 EDT" to "Sun Oct 15 10:00:00 2018 EDT"
  Decoded: "Sun Oct 15 09:00:00 2018 EDT"
  (EASID: CA124893)
  Event Log:VERIFIED Digital Signature (NOT)emulped CA certificate.. update CAP decoder CA file!!
-----
225701: XWT RECEIVED WEEKLY TEST 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 15 09:00:00 2018 EDT" to "Sun Oct 15 10:00:00 2018 EDT"
  Decoded: "Sun Oct 15 09:00:00 2018 EDT"
  (EASID: CA124893)
  Event Log:VERIFIED Digital Signature (NOT)emulped CA certificate.. update CAP decoder CA file!!
-----
225703: XWT RECEIVED WEEKLY TEST 'CAP' (PANSWCAP) ORG-CIV
  "Sun Oct 15 09:00:00 2018 EDT" to "Sun Oct 15 10:00:00 2018 EDT"
  Decoded: "Sun Oct 15 09:00:00 2018 EDT"
  (EASID: CA124893)
  Event Log:VERIFIED Digital Signature (NOT)emulped CA certificate.. update CAP decoder CA file!!
-----

```

Text Version of EAS Event Logs

- OPTIONAL: Many web browsers also include a 'Save Page As...' option in the File menu. Use this feature to download the selected EAS log data to your local computer.

Chapter 7: Send Alerts Tab

The **Send Alerts** tab is for originating different types of EAS alert messages. Only an EAS device configured with a valid Encoder license key will display the **Send Alerts** tab. Within this tab, there are up to three radio buttons.

Radio Button	Description
General Alerts	Originate (create and send) general EAS alert messages. Store and recall EAS message templates. Requires a valid Encoder license key.
One-Button Alert	Send Required Weekly Test. Provides hyperlinks to test setup screens. Requires a valid Encoder license key.
Custom Message	Originate custom EAS (CEM, ADR, and CAE) and non-EAS alert messages. Requires a valid Encoder and Custom Messaging license keys.

Use the **Send Alerts** screens to originate EAS alerts (when an EAS alert is first issued from an EAS encoder/decoder platform). EAS alert encoding is when the digital codes and alert audio tones and message defined by the EAS protocol are assembled and played over a broadcast medium for which EAS decoders might be listening. EAS alerts can be constructed and issued from these web interface screens. This differs from forwarding - when a decoded EAS alert is re-encoded and relayed.

Due to the need for immediate action during origination, Send EAS pages do NOT have any **Accept Changes** buttons. Changes to check boxes, pull-down menus, radio buttons, and action buttons are immediate.

Before originating any alert messages, make sure the Available FIPS and EAS codes have been configured within the **Setup > Alert Agent™ > FIPS Groups** and **EAS Code Groups** screens. The **Configured Available Encoder FIPS Locations** and **Configured Available Encoder EAS Codes** establish which codes are available for origination.

An EAS alert comprises a specific set of data values for encoding as Frequency Shift Keyed (FSK) digital audio data into an audio header - creating the characteristic EAS “squawk” sound that is repeated three times at the start of an EAS alert message. The data placed into an EAS message is:

- the origination code
- the EAS code type
- FIPS codes
- alert duration
- start time
- station ID

A decoded EAS header shows these values following a standard 4 letter sequence ZCZC.

Example: a 15-minute Required Monthly Test for Genesee and Orleans, NY starting on June 14 at 5:18PM from a station named WME would be encoded to or decoded as:

ZCZC-EAS-RMT-036037-036073+0015-1662318-WME.

This information can be interpreted by an EAS decoder into a human readable form, referred to as the “Standard Translation.” The Standard Translation of the above alert string is:

A BROADCASTER has issued A REQUIRED MONTHLY TEST for the following counties or areas: Genesee; Orleans, NY; at 5:18 PM on JUN 14, 2016 Effective until 5:33 PM. Message from WME.

The text translation is used for video and sign displays driven from the EAS device when an alert is originated or when a decoded alert is forwarded. The translation is also prominent in the EAS device event status displays and the operation log. All interfaces that originate and forward the alert display the translation.

A valid Plus Package license key provides options to customize the alert translation. Custom translation allows video displays driven by the EAS device to better describe an alert and provide more details than what is actually transmitted within the EAS protocol. The custom translation only affects the video displays. Unless TDX is used, these added text details are not sent out within the encoded EAS alert audio. A translation can be set to substitute a user-written string for the ORIG code and well as to prepend or append text to the standard translation or even fully substitute the translation for custom text.

GENERAL ALERTS

The **General Alert** web interface screen provides an easy-to-use interface for setting the EAS data elements.

To make and send an EAS alert, review and set items on the **General Alert** page corresponding to the described EAS protocol and to the generation of local video displayed text information.

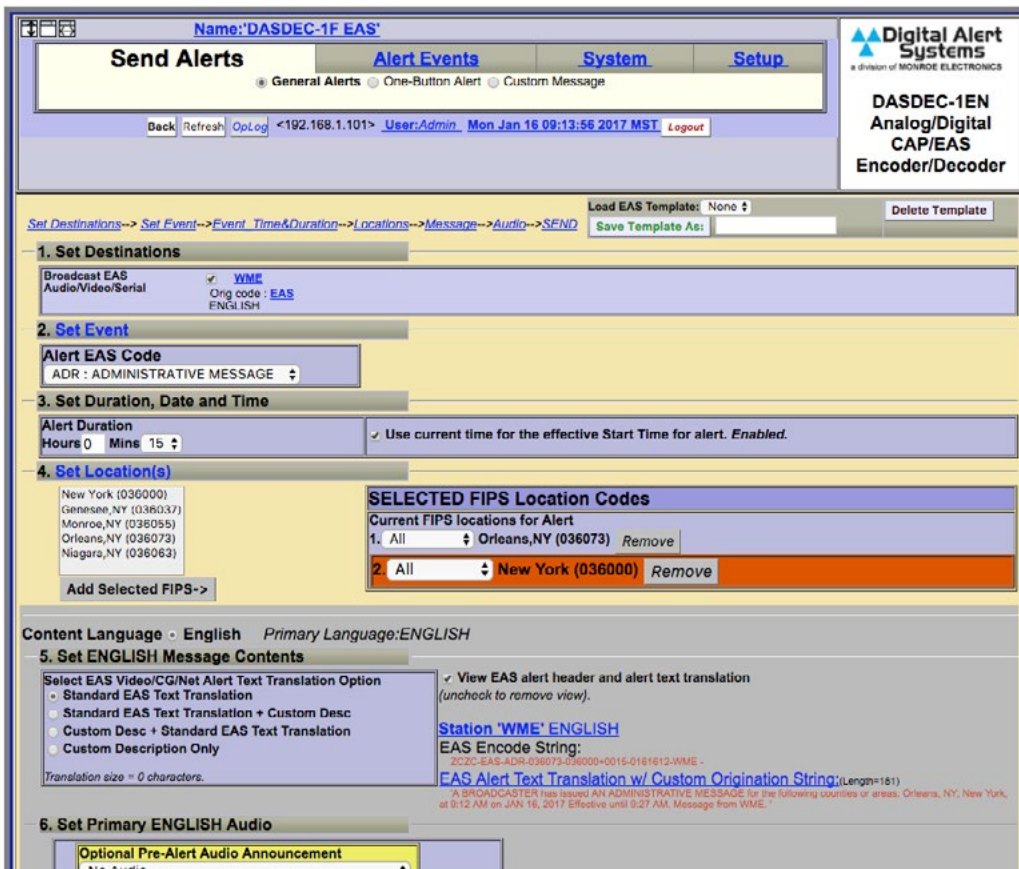
- Station ID
- EAS alert code
- Alert duration
- Starting time (effective time)
- FIPS Location Code(s)
- Message contents
- Pre-alert audio announcement (optional)
- Alert audio message (if any)
- Post-alert audio announcement (optional)
- Optional text translation modifications (required valid Plus Package license key)

The General Alerts screen is composed of seven numbered sections along with several useful hyperlinks, an EAS Template Management (save/load/delete section), and an alert action table. This screen has been updated to include the addition of EAS templates.



Note

Some browsers will not accept the text field change until the mouse is clicked outside of the field entry box. Other browsers simply will accept the change when the Enter key is touched. Make sure to click outside the text field to insure text entry.



General Alerts Screen



Note
The screen captures within this chapter may look different based on the licensed options on your system.

Template Management

Message templates may be saved, recalled, and deleted using the following controls:

Load EAS Template

This pull-down menu enables users quick and easy access to pre-configured (or saved) EAS templates. A saved EAS Template will recall all configuration settings saved within the gray message composition area of this interface. Click this pull-down menu text once to view the available options, then select/click the desired option.

Loaded EAS Templates can be modified prior to being sent. Recall the saved template, make the desired changes, and send the Alert.

Delete Template Button

The process of deleting EAS Templates is a three step process. First, load the desired template from the **Load Custom MSG Template** pull-down menu. Second, click the Delete Template button next to the pull-down menu. This will change the screen to a confirmation page where the user may perform the third and final step - choosing to continue to delete the template or cancel the delete process. To delete the template, click the **Yes, delete template** button and return to the General Alerts screen. Click the **No, cancel** button to abort the deletion process and return to the Custom Messaging Pro screen.



NOTE
Selecting **None** from the **Load EAS Template** pull-down menu will clear all the text fields and reset all the controls to their default configuration settings.

Save Template As:

EAS templates may be saved for later recall. Once the user has composed the desired message – including destinations, Alert EAS Code, duration, locations, language/message contents, and alert audio content – type a name for the EAS template into the text box adjacent to this button and click the **Save Template As:** button. The template will be saved and available in the **Load Custom MSG Template:** pull-down menu.

Set Destinations

These settings are only displayed on devices with a valid EAS-NET™ license key. The frame below the Set Destinations heading displays Station ID, Origination Code, Alert Language settings, and a check box that enables audio, video, and triggering serial communication for that station. The **Station ID** value is taken from the **Origination EAS Station ID** setting found within the Origination Settings of the **Setup > Station > Main** screen. The **Origination (ORG) Code** and **Alert Language** (Primary and Extended) settings are also found in the same screen. These settings will generally not need to be changed. If the Station ID, Origination Code, or Alert Language needs to be changed, the **Station ID** and **Orig Code** labels are hyperlinks to the above mentioned screen. Edit as needed and then use the Back button to return to the Send Alerts > General Alerts screen.



General Alerts - Set Destinations Section - MultiStation Mode

When in MultiStation mode, this frame will display the 'Override' channel information along with any enabled stations. Each station will have the same displayed information (Station ID, ORG Code, Alert Language(s)) and a check box. To disable the audio, video, and serial communication for any of these channels, uncheck the associated check box.

Set Event

Select the desired EAS code from the pull-down menu. Codes shown in this menu are the ones added to the **Configured Available Encoder EAS Codes** list found on the **Setup > Alert Agent™ > EAS Code Groups** screen. If the list needs to be corrected, click the **Set Event** hyperlink, make the desired modifications, and return the **Send Alerts > General Alerts** screen.

Set Duration, Date and Time

The default duration is 15 minutes and corresponds with the minimum allowed duration. Change the alert duration as needed, based on the alert being issued. The FCC allows alerts under an hour to be set in 15 minute increments. Alerts of an hour or more are set in 30 minute increments. The EAS device interface enforces this FCC compliance.

Use current time for the effective Start Time for alert

When checked, the EAS alert message will contain the current date and time (month, day, and year followed by the current time). Users can manually set the effective (starting) date and time for the alert by unchecking this box and manually entering the desired information.



Note

Only specially configured EAS devices allow origination of National Alerts – Emergency Action Notification and National Periodic Test (EAN & NPT).

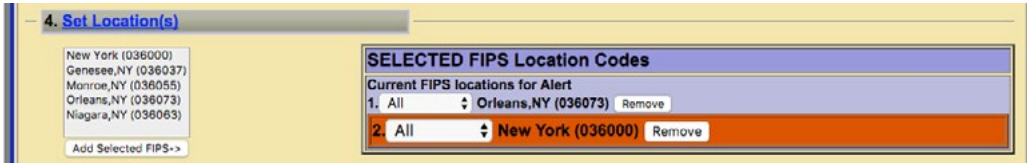


Note

Make sure to enable the **Weekly Test Audio** check box found in the **Setup > Station > Global Options / Global Origination Settings** when creating Required Weekly Tests from the General Alerts interface. This will allow the user to select a locally stored WAV file for the **EAS Broadcast Audio Content**.

Set Location(s)

An EAS alert must be issued for specific locations. Until FIPS location codes are entered, the EAS device will not display a **Send Alert** button. Instead, a message box will show on the right side of the screen stating, ****Need to Add FIPS Codes****. Two additional red message boxes will appear (one in the Set [Content Language] Message Contents section and the other in the Send Alert section) stating **Alert NOT Ready to send::Specify FIPS Codes**.



General Alerts – Set Location(s) Section

To set the FIPS location(s) for the alert code, select from the list of **Available FIPS Code**. The codes shown are the ones that were added on the **Setup > Alert Agent™ > FIPS Groups** screen. *(To correct the list, click on **Set Location(s)** hyperlink. Add FIPS codes to the Configured Available Encoder FIPS Location list. Use the Back button to return to the Send Alerts > General Alerts screen to continue constructing the alert.)*

For each location, select one or more FIPS, and click **Add Selected FIPS->** button. Up to 31 FIPS location codes may be added using the FIPS selection table.

As you build the list of current FIPS locations for the alert, locations will display on the right in the **SELECTED FIPS Location Codes** frame. The sub-region of the FIPS location can be edited for every chosen location. If a different sub-region is desired, select one of the choices presented in the pull-down menu displayed to the left of the FIPS code.

If a FIPS location needs to be removed, click the corresponding **Remove** button.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but not very common.

After selecting the FIPS location(s), the “Alert NOT Ready...” message changes to a **Send Alert** button. The alert can be sent immediately if no audio message or language settings are needed. However, often the alert should have Pre-Alert Audio Announcement or an Alert Audio Message file.

Content Language

These radio buttons dictate the language-related settings for Message Contents and Audio within this gray'd section. When using both Primary and Extended languages, these radio buttons allow the user to select individual configuration settings for each language.

English and Spanish languages are standard within each EAS device. Users can choose a Primary Alert Language and one or more Extended Alert Language from the Setup > Station > Main screen (use the Station ... hyperlink under the View EAS alert header and alert text translation check box for quick access). These settings will encode a primary and extended languages into the EAS alert message. By selecting the same language for both the Primary and Extended Alert Language setting, only one language will be enclosed in the EAS alert message. Selecting two different languages will enable both languages (Primary followed by the Extended Alert Language).



Note
Additional languages (beyond English and Spanish) are available with a valid OmniLingual™ license key.

Set [Content Language] Message Contents

A valid Plus Package and EAS NET™ license keys will display the **Select EAS Video/CG/Net Alert Text Translation Option** frame. Use radio buttons to select one of four combinations of Standard Translation and Custom Translation. For selections with custom translations, a text entry field displays where the text can be entered is displayed.

The alert text translation is used for the local video details, serial and net-attached CGs, and EAS NET™ devices. This alert text can be augmented or replaced with the provided options. Options are provided to add a custom message in front of, after, or completely replace the standard translation. The default is the Standard Text Translation selection. Custom descriptions are outside the scope of EAS alert messages and will not be contained within the EAS alert message. They will be transmitted to local video output details page, serial and network-attached CG's, and EAS NET™ devices. The available radio button selections are:

- Standard Text Translation
- Standard Text Translation + Custom Description
- Custom Description + Standard Text Translation
- Custom Description Only

View EAS Alert header and alert text translation

Enable this check box to view the alert header EAS Encode String and the EAS Alert Test Translation for the currently constructed alert. When enabled, the actual EAS encode string (or EAS header) is displayed. Below this is the current translation. The label above the translation will state if the translation is the basic standard translation or one with a Custom Origination String (see [Origination Settings](#) within the **Setup > Station > Main** screen). Both these labels are hyperlinks to this setup screen allowing you to make changes as needed.

The screenshot shows a software interface for configuring EAS alerts. At the top, it indicates the content language is set to English. Section 5, 'Set ENGLISH Message Contents', includes a radio button selection for 'Standard EAS Text Translation' and a checked box for 'View EAS alert header and alert text translation'. Below this, the 'EAS Encode String' is shown as 'ZCZC-EAS-DMO-036073#0015-3581719-WME'. Section 6, 'Set ENGLISH Audio', features dropdown menus for 'Optional Pre-Alert Audio Announcement' (WME_AlertTone_Audio.wav) and 'Optional Post-Alert Audio Announcement' (No Audio). It also includes settings for 'EAS Broadcast Audio Content (optional)' and 'Select Alert Audio Message' (WME_Alert_Message.wav), along with playback controls.

General Alerts – Language & Audio Selection Section

Set [Content Language] Audio

Use this frame to attach pre-recorded audio voice messages to the EAS alert. Each interface permits selection of no audio file or of an audio WAV file that has been recorded or uploaded onto the EAS device. Add audio files to these lists list in two ways.

- Upload WAV files using the **Upload Audio File** button
- Directly record audio files into the EAS device by using the **Record Audio File** button

Optional Pre-Alert Audio Announcement

Use the pull-down menu to select a pre-recorded audio file to precede the actual alert announcement.

When an audio file is selected, its duration appears along with its sample rate. A **Listen on Browser** hyperlink is available to listen to the audio file within the web interface.

If the audio file does not match the configured **Audio Output Sample Rate** found in the **Setup > Audio > Audio Output Levels/Tests** screen, the text “NOTE:Resample to output rate (*configured output sample rate*) to avoid play out slowdown!” and a **Resample File** button will appear. This process will maintain a constant sample rate for all audio output files and prevent slow-downs when playing differing audio files.

EAS Broadcast Audio Content (optional)

This setting enables users to select where audio content is sourced. This pull-down has the following three options:

- **Local audio content** – Allows users to select and play locally stored WAV files. When this option is selected, a **Select Alert Audio Message** pull-down menu will be present below. Users can choose **No Audio** to play during the alert or a pre-recorded audio message from the list in the drop-down menu.

6. Set Primary ENGLISH Audio

Optional Pre-Alert Audio Announcement
No Audio

EAS Broadcast Audio Content (optional)
Local audio content

Select Alert Audio Message
WME_Alert_Message.wav

Duration: 22.101 seconds Rate:32000 samples/sec Mono
[Listen on Browser](#)

Play->Front Panel Play->Main Play->Preview Out

Record Audio File Upload Audio File Delete Selected

Optional Post-Alert Audio Announcement
No Audio

The audio file duration (in seconds) and sample rate is displayed below the selection. There might also be a **Resample File** button – as described above.



Attention

This manual is organized in a sequential fashion to assist first-time users in the step-by-step configuration of the EAS device. For best results, first-time users should follow the instructions in the order in which they are presented.

If the TDX option is licensed and enabled (**Setup > Station > Global Options**), then to the right of the alert audio selection are three radio buttons: No TDX; TDX Text; TDX URL. These control the addition of TDX alert details.

Audio Playback Options:

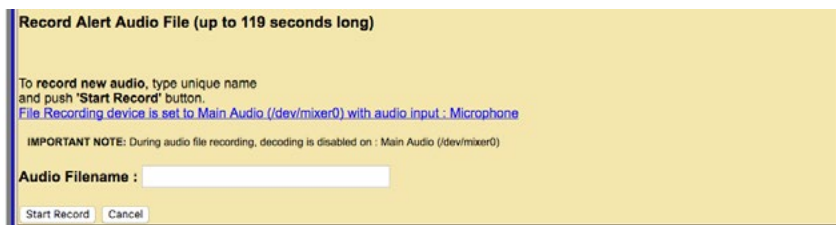
Numerous playback options are added to the interface once an audio file is selected. These include:

- **Play->Front Panel** – plays the audio file out the internal front panel speaker
- **Play->Main** – plays the audio file out the Main Audio output
- **Play->Preview Out** – plays the audio file out the configured Audio Preview Devices (see [Setup > Audio > Audio Output Levels/Tests / Direct Audio Output Levels and Tests](#))

Audio Management Options:

Included in this section are three buttons to assist with managing audio files within the EAS device:

- **Record Audio File** – clicking this button displays a new **Record Alert Audio File** screen. This screen enables users to record audio files with a microphone or from the line input. The active input source is noted at the end of the hyperlink in the middle of this screen. In the example below, the input source **Microphone** is noted. Click the hyperlink to be directed to the **Select audio device for alert audio file recording:** section of the **Setup > Audio > Encoder Audio** to change the input source.



Enter a unique audio file name in the **Audio Filename** text field. (A unique file name is one not already used in the provided **Select Alert Audio Message** selection pull-down. If you use an existing name, the original file by that name will be overwritten.)

The duration of this file must be under two minutes (119 seconds) as the EAS device automatically cuts off recording at 2 minutes. Click the **Start Record** button and speak. A new screen will appear with a running countdown (from 2:00) clock. Click the **Stop Recording** button when finished. The web interface will return to the General Alerts sub-tab.

- **Upload Audio File** – An **Upload Audio .WAV file** interface appears when you click this button. The user is presented with the following buttons:
 - › **Choose File** – click this button to choose a file from the users' local workstation
 - › **Upload .WAV file** – once a .WAV file has been chosen, click this button to upload the file
 - › **Cancel** – click this button to cancel the upload process
- **Delete Selected** – available when an audio file is selected and will immediately delete the selected file.



Warning

Prior to clicking any of playback options, make sure the audio will not interrupt the stations on-air audio. These options are intended to allow users to preview the selected audio file.



Note

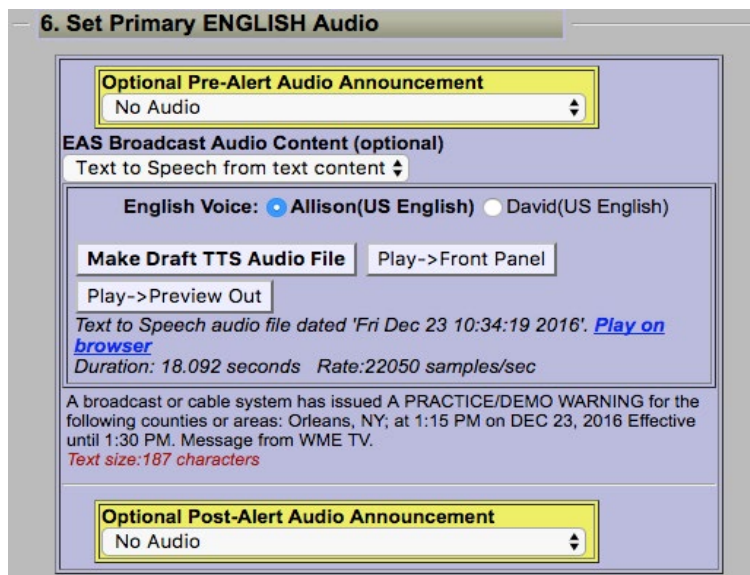
To change audio output levels, use the text link Goto --> **Setup Audio Output Levels** hyperlink to the **Setup > Audio > Audio Output Levels/Tests** screen. Return using the **Back** button.

- **Remote URI audio content** – Uniform Resource Identifier defines a network accessible audio file/location to play content from. This option is utilized to access remote content from a centralized, internet location.

Two pull-down menus and a text entry box will appear once this option is selected:



- **Audio Type:**
 - › **IPAWS MP3 audio file** (audio/x-ipaws-audio-mp3)
 - › **IPAWS MP3 streaming audio file** (audio/x-ipaws-streaming-audio-mp3)
 - › **WAV audio** (audio/wav)
 - › **MP3 audio** (audio/mpeg3)
 - **URI Type:**
 - › **http://** – HyperText Transfer Protocol
 - › **https://** – HyperText Transfer Protocol Secure
 - **URI Address Text Entry Field** – enter the URI address for the desired audio file
 - **Auto-download upon send** check box – will download the desired audio file for logging purposes.
- **Text to Speech from text content** – utilizes the internal text-to-speech engine. If there are licensed Premium TTS voices they will be listed here. Select the desired voice. Otherwise the generic TTS voice will be used.



There are three available buttons and a hyperlink available:

- **Make Draft TTS Audio File** – click this button to create an audio file based on the configured alert options. The audio file will be stored on the EAS device and can be previewed using the following playout options. A new TTS file will need to be created each time any of the alert settings are modified.
- **Play->Front Panel** – plays the audio file out the internal front panel speaker
- **Play->Preview Out** – plays the audio file out the configured Audio Preview Devices (see [Setup > Audio > Audio Output Levels/Tests / Direct Audio Output Levels and Tests](#))
- **Play on browser** hyperlink– will play the selected audio file within the web-browser

Optional Post-Alert Audio Announcement

Similar to the pre-alert announcement. Allows an audio message to be played after the end of an EAS alert.

Within the **Set [Content Language] Audio** section of this interface are buttons to **Record Audio File** and **Upload Audio File**.

Send EAS Alert/Alert NOT Ready to Send

When the alert is ready, the **Send Alert** button will appear. Click this button to send the alert. The EAS device will show a **Review of Prepared Alert** screen (confirmation) with a consolidated view of the alert details. If the alert is correct, click the **Yes, Send Alert!** button. If incorrect, click the **Cancel Send Alert** button. If the alert send is canceled, the EAS device will go back to the General Alerts screen. Edit the alert information before sending the alert again.

Review of Prepared Alert

Primary Language is 'ENGLISH'
Alert Language(s): 'ENGLISH'

AVW 'AVALANCHE WARNING'
from 'EAS-Broadcast Station/Cable System'
Alert effective 'Fri Dec 23 15:02:07 2016' for 0 hrs 15 mins
for the following areas:
Orleans, NY (036073)

EAS Encode String: 'ZCZC-EAS-AVW-036073+0015-3582202-WME TV -'

Complete Translation:
'A broadcast or cable system has issued AN AVALANCHE WARNING for the following counties or areas: Orleans, NY; at 3:02 PM on DEC 23, 2016 Effective until 3:17 PM. Message from WME TV.'

CAP UTF-8 Single Byte Mode
ENGLISH: Custom Text: 'THE FOLLOWING MESSAGE IS TRANSMITTED AT THE REQUEST OF THE WESTERN NEW YORK AVALANCHE CENTER. THIS AVALANCHE WARNING IS FOR THE MOUNTAINS AROUND HOLLEY AND CLAREDON. HEAVY SNOW AND STRONG WINDS OVERLOADED BURIED WEAK AREAS CREATING DANGEROUS AVALANCHE CONDITIONS AT UPPER ELEVATIONS. AVOID AND STAY OUT FROM UNDER OBVIOUS OR HISTORIC AVALANCHE PATHS. THIS WARNING WILL REMAIN IN EFFECT UNTIL DECEMBER 26, 2016. FOR MORE INFORMATION VISIT WWW.AVALANCHE.ORG OR CALL 888-999-4019'

Pre-alert audio announcement file : 'WME_AlertTone_Audio.wav'
ENGLISH:EAS Alert audio via Text to Speech Translation

Station ID is : 'WME TV'

Yes, Send Alert! Cancel Send Alert

Broadcast EAS FSK is Enabled
To Station ID : 'WME TV'

Review of Prepared Alert Screen

When you've clicked the **Yes, Send Alert!** button, the alert will be played out of the selected EAS device's audio output ports. The originated alert audio ports are selected from the **Setup > Audio > Encoder Audio** screen.

During the origination time, the front panel red LED will be lit, and the alert's audio will play from the built-in internal speaker. For the duration of the issued alert, the unit will periodically crawl the alert text across the front panel LCD. The LCD text for the alert will be preceded by the letter "O", indicating an originated alert. You can view details of the alert on the screen **Alert Events > Originated/Forwarded Alert** or **Originated Alert** screens.

During active alert sending, a red notice displays in the Send Alert interface. After the alert is sent, click the **Return** or **Refresh** button to return to the main Send Alerts screen.

Reset

The entire alert setup process can be restarted by clicking the **Reset** button – to the right of the red **Send Alert** button.

View Alert Action Table

When the alert action table check box is checked, you can see the Alert Origination Action Table. It contains active hyperlinks displaying the current status of the various peripheral interfaces that can be activated by an alert. The table displays which peripheral interfaces are available and which are enabled. The active links point to the associated page under **Setup**. Click the interface name to follow the hyperlink and change any specific peripheral used during alert origination.

Serial Protocol	EAS.NET	DVS644 (SCTE18)	Net.CG	Stream MP1.2	Net Switch	Hub Ctrl	Analog Video	Audio
VIDEOSTAMP	OFF	OFF	OFF	N/A	OFF	ON	ON	Front Main Aux1

U:Unlicensed N/A:Unsupported
 Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

Send Alert and View Alert Action Table Sections

Serial Interface Bypass

If a serial protocol has been selected, a Serial Interface Bypass check box is displayed. When the Serial Interface Bypass check box is checked, the currently selected serial protocol will not be used during the alert origination. A message in the Origination Table above changes to say the Serial Protocol is bypassed.

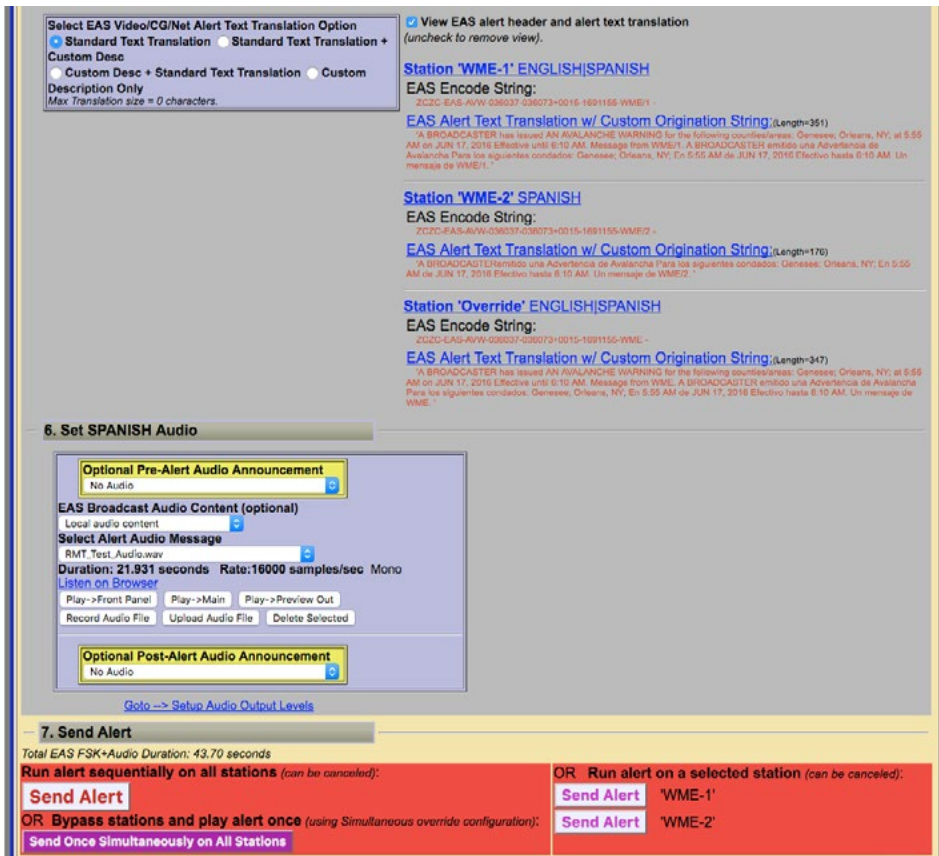
General EAS: MultiStation mode

When in MultiStation mode and at least one station is enabled, the General Alerts page displays added options to support alert origination to individual stations.

MultiStation operation allows EAS alerts to be originated using a specific subset of the hardware in order to play on a specific downstream station. In this way, up to five collocated broadcast stations or channels can use one EAS device for EAS alert origination.

The EAS protocol field for the Station ID can be programmed differently for each station as well. (see **Setup > Station > MultiStation**) This way the actual EAS alert header FSK audio (*which embeds the Station ID*) truly represents the station of alert origin.

Station configuration options can be found on the **Setup > Station >** (Station Sub-Tab).



Send Alerts > General Alerts with MultiStation options

There are different Send EAS Alert buttons provided for station support. They allow you to run the alert on each station in sequence, run on individual stations, and to run the alert once to all stations at the same time using the Main station configuration. As in non-MultiStation mode, when any of the Send Alert buttons are pressed, the actual send must be confirmed on the confirmation review page.

Another difference in MultiStation mode version of the **Send Alert > General Alerts** screen is the alert text translation display. The standard translation for each station is shown. Since each station can independently set the Station ID, the Origination code, and Origination code custom translation text – the translation text varies per station. The display shows exactly the text that is sent per station to video character generators.

All other interface components of the **Send Alert > General Alerts** screen are the same as in the non-MultiStation mode. Keep in mind that the settings on this screen apply to the alert (or alerts if sent to each station sequentially) at the time the **Send Alert** button is pressed.

Finally, the **Alert Origination Action** table is expanded in MultiStation mode to show the actions for each configured station. This table presents a quick view of the station by station configuration.

View alert action table (uncheck to remove view).

Station	Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1,2	Net Switch	Hub Ctrl	Analog Video	Audio
WME-1	OFF	OFF	OFF	OFF	N/A	OFF	ON	ON	Main Front
WME-2	OFF	OFF	OFF	OFF	N/A	OFF	OFF	ON	Front Main Aux1

U:Unlicensed N/A:Unsupported

Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

Alert Action Table – MultiStation Mode

If all of stations are disabled (from the **Setup > Station > (Station Sub-Tabs)** the alert origination reverts to using the Simultaneous Station Override configuration.

ONE-BUTTON ALERT

The EAS device supports configuration of a static set of Required Weekly Test parameters on the **Setup > Station > Main** screen. Once configured, the **Send Alerts > One-Button Alert** screen presents a single button (**Send Preconfigured Weekly Test!**) for issuing the weekly test alert. The Front Panel button will also trigger the test configured from this screen. This feature simplifies sending a weekly test alert.

Station ID: WME TV

CAREFUL: Run Weekly Test button IMMEDIATELY plays alert without confirmation!

Send Preconfigured Weekly Test!

View EAS alert header and alert text translation (uncheck to remove view).

Station 'WME TV' ENGLISH

EAS Encode String:
ZCZC-EAS-RWTT-036037-036073+0015-0031747-WME TV -

[EAS Standard Alert Text Translation](#) (Length=195)
A broadcast or cable system has issued A REQUIRED WEEKLY TEST for the following counties or areas: Genesee, Orleans, NY; at 10:47 AM on JAN 3, 2017 Effective until 11:02 AM. Message from WME TV.

One-Button Weekly Test is for the following locations:

Origination Codes

1. Genesee, NY (036037)
2. Orleans, NY (036073)

Effective Duration: 15 minutes.

Total EAS FSK+Audio Duration: 10.84 seconds

View alert action table (uncheck to remove view).

Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1,2	Net Switch	NET GPIO	Analog Video	Audio
CDDI	OFF	OFF	ON	N/A	OFF	ON	OFF	Front Main Aux1

U:Unlicensed N/A:Unsupported

Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

[Goto to -> Setup Audio Output Levels](#)
Wrong FIPS? Goto -> Setup - Station - Station - Origination Settings - Required Weekly Test
Front Panel Button Weekly Test Enabled. Goto -> Setup - Station - Global Options

One-Button Alert Screen

There are three ways to send reconfigured one button test alerts. In both cases, the alert is sent immediately with the current clock time as the effective alert start time. No confirmation dialog is presented.

1. Click the button **Send Preconfigured Weekly Test!** on the One-Button Alert screen
2. Press the front panel button once, wait a second, press it again
3. Initiating a contact closure on a configured GPIO Input

This screen contains numerous hyperlinks throughout to aide in making configuration changes if needed. Some of the more useful hyperlinks are found in the lower right corner of the screen: Audio Output Levels, FIPS codes, and Front Panel Button enable.

The **View alert header and alert translation** check box and the **Alert Origination Action** table operates the same as on the **General Alerts** screen.

One-Button Alert: MultiStation mode

When in MultiStation mode and at least one station is enabled, the One-Button Alert screen displays added options to support individual station origination. See the screen shot below.

One-Button Alert – MultiStation Mode

One-Button MultiStation operation allows EAS Required Weekly Tests to be originated using a specific subset of controlled hardware in order to play on a specific downstream station. In this way, up to five collocated broadcast stations or channels can use one unit for EAS Weekly Test origination.

Individual station configuration settings are located at **Setup > Station > (Station Sub-Tabs)** with **Simultaneous Station Override** sub-tab used for any un-configured station.

The screen shot demonstrates the different **Run Weekly Test** buttons provided for station support:

- **Run Weekly Test sequentially on all stations**
- **Run Weekly Test once simultaneously on all stations**
- **Run Weekly Test on Station ‘insert station name’** (one for each station)

As in non-MultiStation mode, when any of the **Run Weekly Test** buttons are pressed, the test is done immediately without confirmation.

If all of the stations are disabled the alert origination reverts to using the settings configured within the Simultaneous Station Override sub-tab.

CUSTOM MESSAGE PRO

The EAS device supports a licensed feature called **Custom Messaging** for playing out Child Abduction Emergency (CAE), Civil Emergency Alert (CEM), and Administrative (ADR) EAS alert messages as well as non-EAS audio/video messages. Using Custom Messaging, the unit can be used to:

- broadcast custom text messages
- play audio messages multiple times
- use automatic text to speech conversion
- play Pre-Alert and Post-Alert audio files
- assign local audio files or use text-to-speech for Alert Audio messages
- create, save, recall, and delete custom message templates
- create, save, recall, and delete custom text message files
- upload audio (.wav) files
- generate FSK headers tones for EAS messages
- assign custom messages to GPI inputs

Custom Messaging Pro can originate both EAS and non-EAS messages, which means the EAS device can be used as a custom warning or information system as well as an EAS message originator.



Note
Custom Messaging is not available when the MultiStation feature is active with enabled stations.

Custom Message Pro Screen

The Custom Messaging Pro screen is divided into three functional sections. At the top of the interface screen is where Custom Message templates are loaded, deleted, saved, and sent (Template Management). The center (gray) section is used to compose the message and includes the Message Type Control, Message Display Control, Message Duration, Custom Text Message, and Audio Messages selections. The bottom most section contains the Upload Audio .WAV file controls.

Template Management

This first section of this screen allows for quick and easy access to stored message templates. The following controls are available:

Load Custom MSG Template:

This pull-down menu enables users quick and easy access to saved (or pre-configured) Custom Messages. A saved Custom Message will recall all saved configuration settings within the gray message composition area of this interface.



Load Custom MSG Template Pull-Down Menu

To load a Custom Message Template, click once on the pull-down menu and select the desired template by clicking on that menu item. The template will immediately populate the message composition section with the pre-configured (saved) settings.

Loaded Custom Message Templates can be sent as-is, or they can be modified just prior to being sent. For example, a Civil Emergency Alert (CEM) template may be stored advising the residents of six counties to boil water due to concerns of water contamination. A similar emergency may arise, however, this time it only affects three out of the six counties within the EAS devices' service area. Simply recall the original CEM, remove the unaffected counties, and send the CEM Alert.

Delete Template Button

The process of deleting Custom Message Templates is a three step process. First, load the desired template from the **Load Custom MSG Template** pull-down menu. Second, click the Delete Template button next to the pull-down menu. This will change the screen to a confirmation page where the user may perform the third and final step - choosing to continue to delete the template or cancel the delete process. To delete the template, click the **Yes, delete template** button and return to the Custom Messaging Pro screen. Click the **No, cancel** button to abort the deletion process and return to the Custom Messaging Pro screen.

Save Template As:

Custom Messages templates may be saved for later recall. All of the configuration settings found in the (gray) message composition area can be stored and easily recalled.

Once the user has composed the desired message – including Custom Text, Message Type, Display Controls, Custom Text, and audio settings – type a name for the Custom Message template into the text box adjacent to this button and click the **Save Template As:** button. The template will be saved and available in the **Load Custom MSG Template:** pull-down menu.



NOTE

Selecting **None** from the **Load Custom MSG Template** pull-down menu will clear all the text fields and reset all the controls to their default configuration settings.

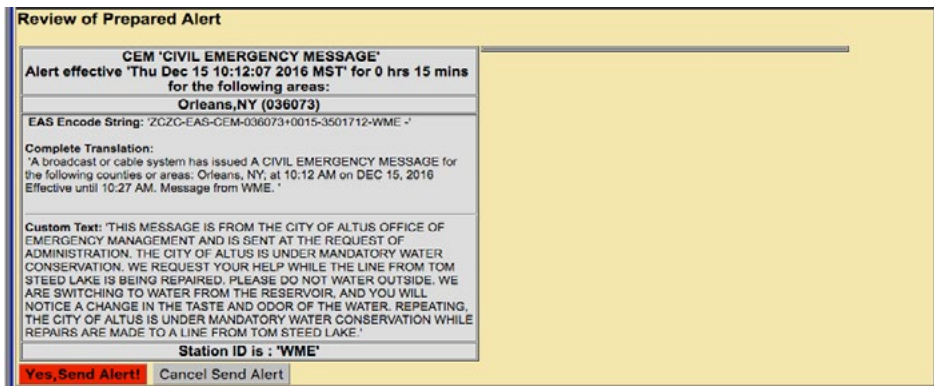


Note

Use a descriptive and short template name. Avoid special characters such as <, >, |, \, ;, (,), &, ;, and quote marks – as well as wildcard such as ? and *.

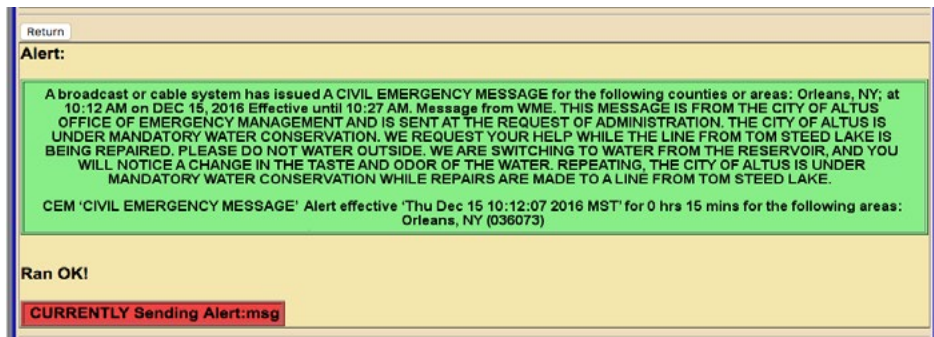
Send Custom Message/Send Alert Button

This white button with red text / border is used to initiate the origination of either a Custom Message or EAS Alert. The button will change depending on which type of message is configured to send. When sending a Custom Message, the button will read Send Custom Message and when sending a CEM, ADR, or CAE, it will read Send Alert. This is a quick and visual way to determine an EAS or non-EAS message is being sent.



Review of Prepared Alert Screen

Once a Custom Message or EAS Alert has been configured (see below to configure both EAS and non-EAS messages/alerts) or loaded, the user may click the Send Custom Message/Send Alert button. The interface will change to a review screen where the user can review the message details. The interface displays two options to the user: start the message or cancel the message. If for any reason the message is not configured properly, use the Cancel Send Message button, make the necessary changes and begin the send message/alert process again. Otherwise, click the Yes, Start Message! button to send the configured message/alert.



Confirmation Screen

A confirmation screen will then appear showing the status of the active message/alert for a few seconds before returning to the main Custom Message screen.

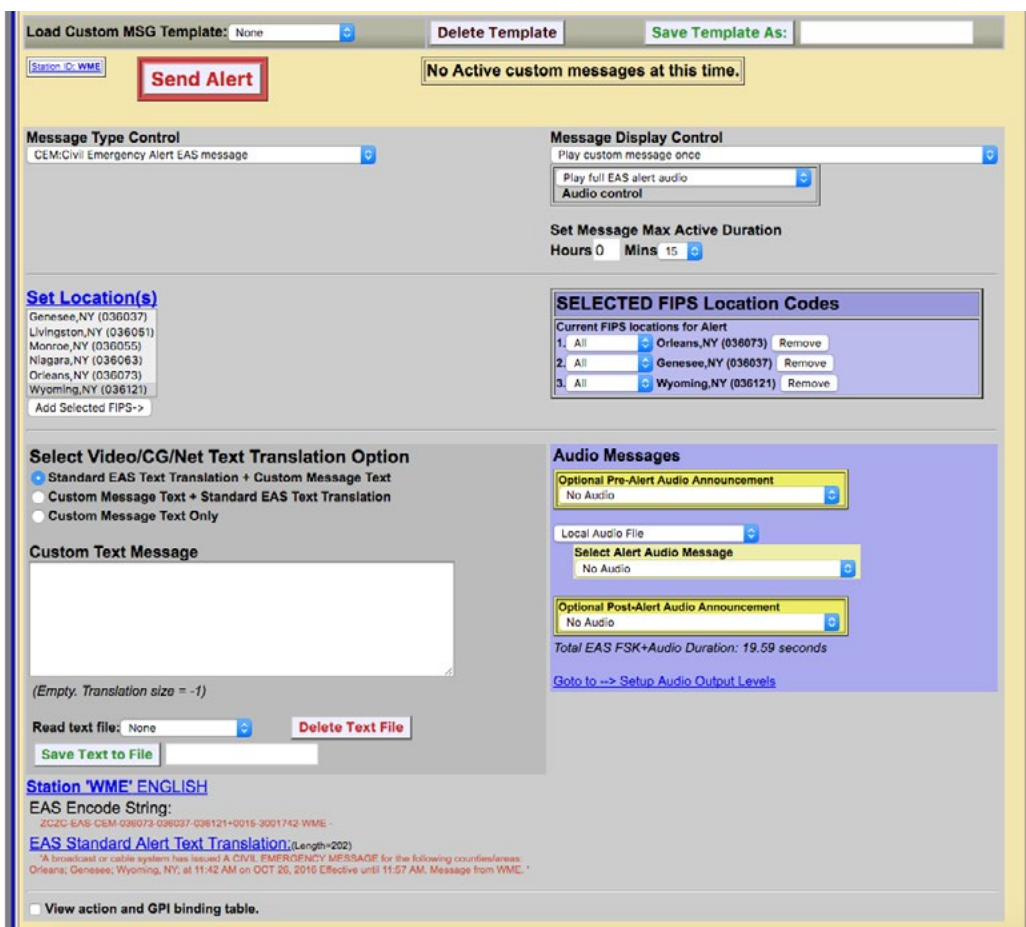


Custom Message Screen with Active Message/Alert

The Custom Message interface shows the current status of the custom messaging operation. While a custom message is being broadcast, the interface will display the message play-out status along with a **STOP Active Message** button. This button can be pressed throughout the duration of the message/alert to force an early end to the message broadcast.

When a custom message is active, the **Alert Events > Originated/Forwarded Alerts** and **Originated Alerts** event status screens display the message as an active originated event. The display includes the same force **Stop Active Message** button.

Below the **Send Custom Message/Send Alert** button is a gray-background section for composing message/alerts. This section has numerous configuration settings. Several settings are universal to both Custom Messages and EAS Alerts. EAS Alerts have additional settings, such as FIPS codes and EAS Text Translation, are added to the interface when CEM, ADR, and CAE message types are selected. When composing EAS Alerts, the bottom of this section will display the EAS Encode String and the EAS Standard Alert Text Translation.



Custom Messaging Pro Screen – EAS Alert

Message Type Control

The interface allows selection of a message type, which can be a fully custom message or one of three EAS-specific alerts. This pull-down menu is used to select the type of custom message being sent. The menu contains the following four selections:

Message Type	Description
Non-EAS Custom Message	Custom messages that do not include EAS specific information – including FIPS location codes and the generation of FSK tones. These messages are usually intended for closed systems, such as corporate campuses and educational institutions to broadcast both audio and visual emergency alert information.
CEM: Civil Emergency Alert EAS Message	An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. For example, a CEM could be used to alert the public to a public water contamination issue and provide guidance to boil tap water or where to obtain clean water.
ADR: Administrative EAS Message	A non-emergency message that provides updated information about an event in progress, an event that has expired or concluded early, pre-event preparation or mitigation activities, post-event recovery operations, or other administrative matters pertaining to the Emergency Alert System. The ADR is to be used for all follow-up messages pertaining to an original warning.
CAE: Child Abduction Emergency (Amber Alert) EAS Message	An emergency message regarding a specific Child Abduction Emergency. Alerts usually contain a description of the child, the likely abductor, and specific information about the abductors vehicle. To avoid false alarms, the criteria for issuing an alert are rather strict. Each state's or province's AMBER alert plan sets its own criteria for activation. The U.S. Department of Justice issues the following "guidance", which most states are said to "adhere closely to" (in the U.S.): <ol style="list-style-type: none">1. Law enforcement must confirm that an abduction has taken place2. The child must be at risk of serious injury or death3. There must be sufficient descriptive information of child, captor, or captor's vehicle to issue an alert4. The child must be under 18 years of age



NOTE

Many law enforcement agencies have replaced CAE #2 criterion with 'The child's whereabouts is unknown of is assumed to be at risk of serious injury or death'.

Select the desired **Message Type** by clicking the menu once and selecting the desired type by clicking again one that selection.

Message Display Control

There are many options available for the playout of both video and audio content during the active alert duration (see **Set Message Max Active Duration** below). The five available options may be selected through this pull-down menu. These options are quite descriptive and are as follows:

- Play custom message once
- Repeat custom message playout for the defined max duration (or until stopped)
- Repeat custom message playout until stopped
- Repeat custom message playout for a specific duration (or until stopped)
- Repeat custom message playout for a fixed number of times (or until stopped)

Select the desired **Message Display Control** by clicking the menu once and selecting the desired type by clicking again one that selection.

The **Message Display Control** and **Audio Control** interfaces will change depending on the chosen selection. For example, when selecting **Repeat custom message playout for a fixed number of times**, the interface will automatically add a **Number of repetitions**: text entry box. These interface changes are self-explanatory.

Audio Control

Due to the tight relationship between video and audio, the **Audio Control** pull-down menu is located directly below the **Message Display Control** pull-down menu. This setting enables the user to select one of the following three options:

- Do not play any alert audio
- Play full EAS alert audio
- Play just alert voice audio message portion

It is important to understand what components are contained within the *'full EAS alert audio'*. The *'full EAS alert audio'* contains the header tones, attention signal, alert voice audio, and the End of Message (EOM) tones. All these components are required to send a valid EAS alert.

When originating an EAS message, the EAS device may use a pre-recorded Alert Audio Message file or utilize text-to-speech of the **Custom Text Message** for the *'alert voice audio'*.

Selecting any of the repeating options in the **Message Display Control** pull-down menu will change the options available within the **Audio Control** pull-down menu:

- Do not play any alert audio
- Play full EAS alert audio with every display repetition
- Play full EAS alert audio just during the first display
- Play full EAS alert audio once and alert voice audio message portion during repetitions
- Play just alert voice audio message portion with every display repetition
- Play just alert voice audio message portion during the first display



Link

Refer to the [EAS Protocol section](#) this manual for additional information about the structure of EAS messages.

Set Message Max Active Duration

Every message/alert contains an active duration. This time is useful for several reasons:

- Used to calculate the 'Effective until...' time displayed in an EAS alert
- When selecting Repeat custom message payout for the defined max duration, the message/alert will remain active in the EAS device for the defined duration

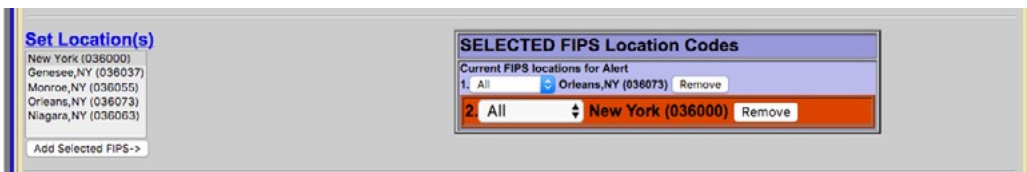
The **Message Max Active Duration** does not always mean the message/alert will be active within the EAS device for the entire configured duration. For example, a CEM alert is configured to inform the public of contaminated water and advise them to boil tap water for 24 hours. Setting the **Message Max Active Duration** to **24 Hours** and **0 Mins** will add 24 hours to the date and time the alert is sent and display that as the 'Effective until...' time within the EAS alert:

'A broadcast or cable system has issued A CIVIL EMERGENCY MESSAGE for the following counties or areas: Orleans; Genesee; Wyoming, NY; at 8:41 PM on OCT 26, 2016 Effective until 8:41 PM OCT 27, 2016. Message from WME.'

This CEM alert may only be broadcast once. In this case the alert is only active in the EAS device for the time of that broadcast.

Set Location(s) [EAS Specific Setting]

Just below the **Set Location(s)** hyperlink is a text box with a list of counties and FIPS location codes. This list represents all the available FIPS codes that can be used in the origination of an EAS alert message.



Set Location(s) Section - EAS Alert

To modify this list, follow the **Set Location(s)** hyperlink to the **Setup > Alert Agent™ > FIPS Groups** screen. At the bottom of this page is the **Configure Available FIPS for Encoder Alert Origination** section.

Returning to the Custom Messaging screen, configure the FIPS location codes by clicking the desired county/FIPS code and then click the **Add Selected FIPS->** button at the bottom of the list. Repeat this process until all the desired FIPS codes are listed in the purple **Current FIPS locations for Alert** list. Multiple FIPS codes can be added by holding either the Ctrl or Alt key while selecting. Only the FIPS codes in the purple area will be used in the origination of the EAS alert message. FIPS subdivisions may be configured for each FIPS code by using the pull-down menu next to each FIPS code. The **Remove** button adjacent to each FIPS code will remove that code from the **Current FIPS locations for Alert** list.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but not very common.



Note

The FCC has defined the minimum EAS duration as 15 minutes. As such, the smallest duration available in this interface is 15 minutes.



Note

The EAS device does not sort Pre-Alert, Alert, or Post-Alert audio files separately. All audio files will be displayed in each of these pull-down menus.

Select Video/CG/Net Text Translation Option *[EAS Specific Setting]*

The EAS device will send text information to either internal or external video devices. These radio buttons configure the information sent to those devices:

- Standard EAS Text Translation + Custom Message Text
- Custom Message Text + Standard EAS Text Translation
- Custom Message Text Only

Custom Text Message

This text entry field is used to augment a standard EAS alert message or provide text for a custom message. Information contained in this field will be sent to internal or external character generators for visual alerting. It may also be used for text-to-speech (TTS) generation within the EAS device.

Just below this text entry field is a count of the number of characters found within the Custom Text Message. The screen requires a refresh in order to provide an accurate count.

Custom text messages can be loaded, deleted, and saved – similar to Custom MSG Templates. The next three items discuss how to perform these functions.

Read text file:

Text files may be recalled by clicking this pull-down menu and selecting the desired file. Once a text file has been selected, the Custom Text Message field is cleared and populated with the selected file.

Delete Text File Button

To delete an existing text file, follow the process above to read the desired text file and click the **Delete Text File** button. The text file is immediately deleted without additional confirmation.

Save Text to File Button / Text Entry Field

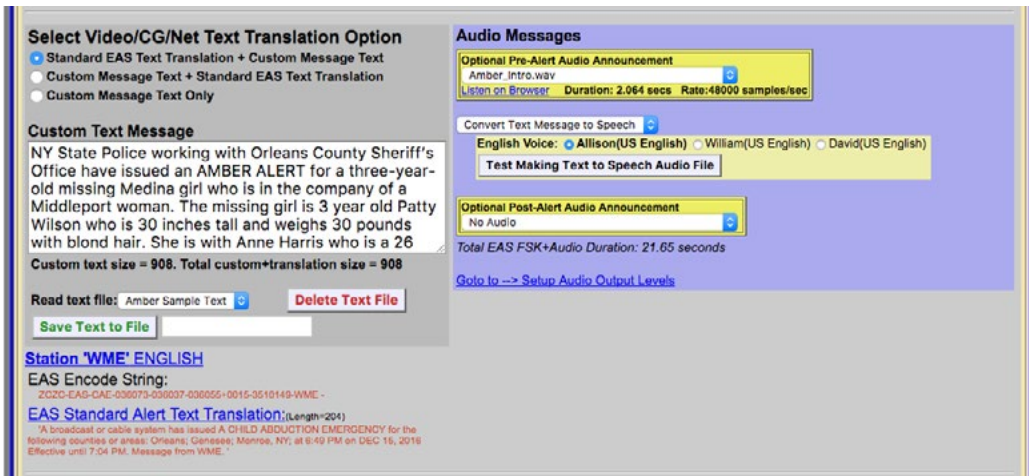
Saving text files is a useful feature when wanting to quickly and reliably recall Custom Text Messages. In many instances it is easier to modify existing/recalled text than completely re-type it.

Type the custom text in the **Custom Text Message** field. Move down to the text field directly to the right of the **Save Text to File** button and enter a file name for this text file. Click the **Save Text to File** button and the text file will be saved. To double check the file is available to recall, click the **Read text file:** pull-down menu and make sure the new text file is in the list.

Audio Messages

There are three main pull-down settings within the purple Audio Messages sections of the interface. These settings determine what audio, if any, will be utilized during the Pre-Alert, Alert, and Post-Alert segments of the message/alert. Both the Pre-Alert and Post-Alert are optional settings and are not required during an EAS or Non-EAS message, but may also be useful in enhancing the total message/alert. For example, a pre-alert audio file might contain alert tones since they are not standard for non-EAS messages. Another example might utilize a personalized station ID audio file as pre-alert audio when sending an EAS message. These are just a few examples of how pre and post alert audio may be used. With valid premium Language Licenses, TTS may be generated for Alert Audio to streamline the creation of message/alerts.

Audio files may be uploaded to the EAS device via the **Upload Audio .WAV file** section at the bottom of this screen. (see below for more detailed information on loading audio .wav files)



Audio Messages Section (TTS Enabled)

Optional Pre-Alert Audio Announcement

Pre-Alert Audio is played prior to the Header tones in an EAS alert and prior to the alert audio in a non-EAS message. These audio files are selected by clicking once on the **Optional Pre-Alert Audio Announcement** pull-down menu and selecting the desired item from that list with a second click.

When an audio file is selected, additional text will appear below the pull-down menu. The **Listen on Browser** hyperlink text will play the selected audio file through the local computers speakers. It may be useful to access the EAS device from a quieter office rather than a noisy equipment room. The selected audio file's duration (in seconds) and sample rate are also displayed here.

Select Alert Audio Message

This audio selection is the audio used within both an EAS and non-EAS message/alert. This interface allows for the playout of pre-recorded audio files or the generation of TTS (of the **Custom Text Message**) to be used for the Alert Audio Message. The pull-down menu contains the following options:

- Local Audio File
- Convert Text Message to Speech

With **Local Audio File** selected, the interface displays a pull-down menu titled Select Alert Audio Message. From that pull-down menu, users can select a pre-recorded audio file for playout.

When **Convert Text Message to Speech** is selected, the interface displays selections for available premium voices. Select the desired voice by clicking the radio button to the left of listed voice. There is also a **Test Making Text to Speech Audio File** button for creating the TTS audio file. Click either the **Play->Front Panel** button or **Play on browser** hyperlink to listen to this audio file. This section of the interface also displays the audio files' creation date/time, duration, and sample rate information.

Optional Post-Alert Audio Announcement

Audio played after the Alert Audio in non-EAS applications or following the EOM tones of an EAS alert is considered Post-Alert Audio. The pull-down menu located in this section of the interface will display all the available audio files. These audio files are selected by clicking once on the **Optional Post-Alert Audio Announcement** pull-down menu and selecting the desired item from that list with a second click.



Note

Multiple GPI's may be configured to trigger the same Custom Message Template. The GPI Binding Table will display all the configured GPI's assigned to trigger the selected Custom Message Template. However, a single GPI may not be assigned to multiple templates.

When configuring EAS alerts, the total duration of the EAS alert is displayed just below this pull-down menu – labeled **Total EAS FSK+Audio Duration**:

The interface also contains a hyperlink to the **Setup Audio Output Levels** for easy access to audio output levels.

EAS Encode String and EAS Standard Alert Text Translation [EAS Specific]

It is useful, when configuring an EAS alert message, to view the outgoing text information for accuracy. The ZC string will be sent out to encode the Header information. Based on the information contained in the ZC string, the EAS device generates the Standard Alert Text Translation. This is a good place to review the outgoing EAS alert, prior to clicking the **Send Alert** button.

View action and GPI binding table

This check box allows the user to view the Alert Origination Action Table. It contains active hyperlinks displaying the current status of the various peripheral interfaces that can be activated by a custom message/alert. The table displays which peripheral interfaces are available and which are enabled. The active links point to the associated page under **Setup**. Click the interface name to follow the hyperlink and change any specific peripheral used during alert origination.



Alert Origination Action & GPI Binding Tables

The GPI Binding Table (to the right of the Alert Origination Action Table) displays the GPI(s) configured to trigger the selected **Custom Message Template**. A Custom Message Template must be selected (at the top of the screen) in order to see what GPI(s) are configured to trigger that specific Custom Message Template, otherwise the table will display **Message template not selected above**. Load each Custom Message Template to view what GPI's are assigned to that template.

The hyperlink text within the GPI Binding Table will direct the user to the **Setup > GPIO** screen for assigning GPI to Custom Message Templates. (see **Assigning GPI Triggers To Custom Message Templates** (below) for more detailed information)

Upload Audio .WAV file

The interface at the bottom of this screen allows .wav and .mp3 audio files to be uploaded into the EAS device for payout from the EAS device.



Upload Audio .WAV file Section

- Click the **Browse** button to locate the file on the local computer
- Click the **Upload .WAV file** button. MP3 files are automatically converted into a WAV files.

Uploaded audio files are available for tests as well as for encoding and manual forwarding.

ASSIGNING GPI TRIGGERS TO CUSTOM MESSAGE TEMPLATES

Custom Message Templates may be triggered by GPIs. This process is performed from the **Setup > GPIO** screen. A hyperlink is available in the GPI Binding Table at the bottom of the Custom Message Pro interface screen or simply navigate using the tab/radio buttons at the top of the user interface.

Any GPI may be assigned to a template – including internal and external/networked GPI's. More than one GPI may be assigned to a single template. However, a single GPI may not be assigned to multiple templates.



GPI Setup Screen

At the top of the GPI Setup screen is the GPIO Table. In the above screen capture, the table displays **GPI Input 1** as being assigned to the **GenPlatformAlarm** custom message template. To configure this relationship:

- Locate the GPI Input 1 pull-down menu on the left side of the interface
- Click the pull-down menu to view the available options
- Select **Run Custom Message** at the bottom of the pull-down menu
- Another pull-down menu will appear titled **Custom MSG:**
- Click on this pull-down menu and select the desired Custom Message Template

Repeat this process for each, individual GPI requiring configuration.

The various GPIO Tables will be updated with these GPI/template assignments. They will also be visible within the GPI Binding Table for each Custom Message Template.

Chapter 8: System Tab

The **System** tab presents system, system status, and log information for the EAS device along with useful Emergency Alert System information. There are no configuration settings contained in these screens. Some display features and hyperlinks to different parts of the web interface are available. The **System** tab has the following radio buttons:

Radio Button	Description
Help	Useful information about the EAS device, End User License agreement, and general information about EAS.
Status	Displays the current status of components such a decoders, GPIOs, network(s), Operating Systems, USB, CPU, PCI, IO devices, and e-mail.
Logs	The EAS device keeps extensive logs on web sessions, operation, OS, security, boot, and e-mail.
Debuglogs	When enabled, displays detailed logs for the decoder, main server, serial ports, audio, video, network(s), and web server. Only use this feature when needed.

HELP

The **System > Help** menu displays basic information about the One-Net R189 or DASDEC II-1EN, End User License, About EAS EAS Message Protocol, and EAS Codes.

Sub-Tab	Description
About DASDEC-1EN / One-Net R189	Displays basic system information about the EAS device, OS version, software version, installation date, software build date, and description of the EAS device.
End User License	Shows a copy of the End User License Agreement
About EAS	Provides a description of the Emergency Alert System
EAS Message Protocol	Illustrates the EAS Message Protocol
EAS Codes	Displays a list of current EAS Codes

Help Screen

About DASDEC II-1EN / One-Net R189

Presents information about the installed operating system, software version, install date and build date. This screen additionally displays information about Digital Alert Systems/Monroe Electronics and the EAS device. The software version indicator in the box on the top right side of each screen is a hyperlink to the **Setup > Server > Upgrade** screen.

End User License

A copy of the Digital Alert Systems/Monroe Electronics End User License Agreement is displayed on this sub-tab.

About EAS

Emergency Alert System information: purpose, operation, management, your responsibilities as a broadcaster, and the future of EAS and DASDEC/One-Net.

EAS Message Protocol

Displays EAS message protocol information from the FCC. This text discusses audio FSK, EAS message protocol content and the different elements that comprise an EAS alert message.

EAS Codes

A list of current National, State and Local EAS Event Codes along with a description and severity for each code. This list coincides with available EAS Codes throughout the web interface.

STATUS

The **Status** radio button menu screen has several sub-tab options. Each sub-tab displays a different set of information. The following is a list of sub-tabs and a description of the status information displayed:

Sub-Tab	Description
Main	Displays Platform ID, Server Name, Uptime, Decoder Setting, GPIO, Alert Forwarding and Alert Origination Action Tables along with Printer, Disk Usage and TTS information
GPIO	Presents the current state of GPIO closures
Network	Presents Links, Routes, Net Status Dump, Firewall information along with scripts info for Master and any installed network ports. The SSH Public Encryption Key and Authorized Remote SSH Public Encryption Keys are displayed.
Operating System	Information about the OS including Hostname, Kernel, Uptime, Memory, Temperatures, Disk Usage, Kernel Modules and Sound System are displayed.
USB	A list of Universal Serial Bus (USB) Serial Devices, Basic USB Devices, and a Detailed USB Device List is presented
CPU	Detailed information about the CPU and Run Status
PCI	A detailed list of Peripheral Component Interconnect (PCI) components
IO	A detailed list of Input/Output (IO) device port mapping and memory
Email	Displays the Email Configuration settings

One-Net R189 Platform ID : 'PYGK8C6NRHWSRQUCFHBO/' Server Name : OneNet-1F EAS

System Uptime : 12:29:19 up 49 days, 1:53, 0 users, load average: 0.28, 0.18, 0.11

Decoder and Other Server Status

Decoder Name	Active	Input Level	Level Status	Mixer	Output Name	Output Level	Mixer	Orig Aud	Fwd Aud	3 Radio Tuner's
L1	Yes	55	OK	/dev/mixer0	Front Panel Speaker	70	/dev/mixer0	ON	ON	1. AM 1160 KHz (63%)
R1	Yes	32	LOW	/dev/mixer0	Main Audio	70	/dev/mixer0	ON	ON	2. NOAA 162.550 MHz (15%)
L2	Yes	55	ZERO	/dev/mixer2	Aux 1 Audio	L:75 R:75	/dev/mixer2	ON	OFF	3. FM 98.9 MHz (8%)
R2	Yes	75	ZERO	/dev/mixer2						

Number of active decoders: 4 of 4

Decode Activity: KSL-AM(L1)-Main Left | WDIV(R1)-Main Right | NOAA(L2)-Aux 1 Left | R2-Aux 1 Right

Encoder Station ID: Forwarding Station ID:

Station ID: WML | Station ID: WML | Global Manual Forward Mode

One-Net Server GPIO Table

Front Panel Button Press Current Status:Open (OFF)	GPI Input 1: Forward Active pending Decoded EAS Alert once to all Current Status:Open (OFF)	GPI Input 2: Reenable forwarding of active EAS once to all Current Status:Open (OFF)
GPI Output 1 : Closed during EAS Audio Current Status:Open (OFF)	GPI Output 2 : Closed during unforwarded, active, decoded EAS alert Current Status:Open (OFF)	Main audio passthrough Enabled: Internal audio OFF.

Main Status Screen

LOGS

The **Logs** screen has six sub-page options: Web Session Log, Operation Log, Operating System Log, Security Log, Boot Log, and Email Log.

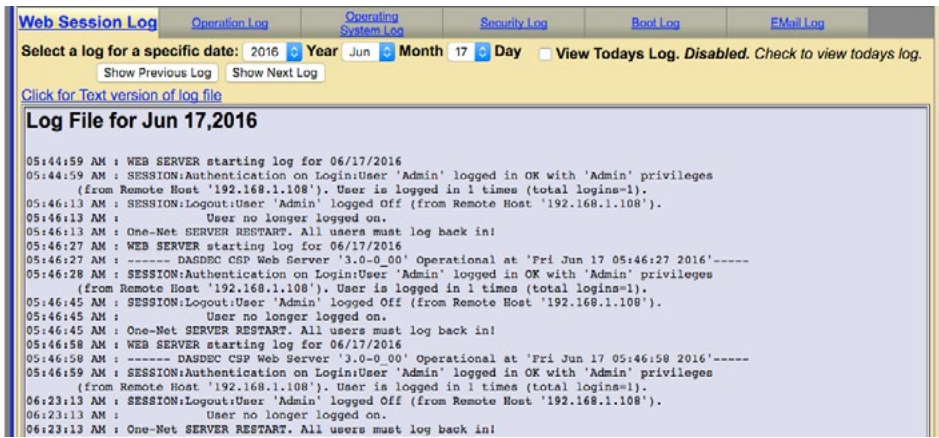
Sub-Tab	Description
Web Session Log	Displays user access to the EAS device
Operation Log	Shows EAS device operation log including EAS event information
Operating System Log	Presents the last 500 lines of current and previous backup log
Security Log	Presents the last 500 lines of security log
Boot Log	Presents the last 500 lines of boot log
Email Log	Presents the last 500 lines of Email log

Web Session Log

Presents time stamped information about user access to the unit. It shows exactly who and when users logged on or attempted to log on the unit. The Web Session Log is an important part of the security auditing for the unit and should be reviewed often if security is an issue with your installation. Two settings are available.

- Check the **View Today's Log** check box to show the Web session log for the current day.
- Uncheck the box to view archived web session log files. Then select a log for a specific date. You can then show the log for the previous or the next day.

Log files a day old or more old can be deleted using the delete button. The page can be refreshed by a button at the bottom of the page to show new information.



Web Session Log Screen

View a text version of a log page by clicking on the provided **Click for Text Version of log file** hyperlink.

Operation Log

Presents time stamped information about the EAS devices' operation. This interface works the same as the one for the Web Session Log. Important EAS events will be shown here. At the top of every page is an **OpLog** button that navigates to this page.

View a text version of a log page by clicking on the provided link **["Click for Text Version of log file"](#)**.

Operating System Log

Presents the last 500 lines of the current and previous backup of the Linux System Log.

Security Log

Presents the last 500 lines of the Linux System Security Log.

Boot Log

Presents the last 500 lines of the Linux System Boot Log.

Email Log

Presents the last 500 lines of the Linux System Email Log. Also, has list of the Email Submission Queue and the Email Send Queue.

DEBUG LOGS

The Server Debug logs screen is only available when the **Server Debug Log Interface** check box is enabled within the **Setup > Server > Options** screen. These logs provide customer service engineers a better view of what is happening within the EAS device. For each of these sub-tabs categories, a pull-down menu enables users to set Basic, Extra Debug Log Detail Level or None at all. These pull-down menus allow users to turn on specific debug logs for any of the above sub-tab categories. When debugging is no longer needed, make sure to uncheck the **Server Debug Log Interface** check box.



Note

The Server Debug Log Interface feature is typically used by and under the direction of a qualified customer service engineer. Do not turn this feature on unless directed by a Digital Alert Systems/Monroe Electronics customer service engineer.

HARDWARE AND SOFTWARE SPECIFICATIONS

An Emergency Alert System Analog/Digital Encoder/Decoder Platform

The One-Net and DASDEC II are State-of-the-Art Emergency Alert Systems (EAS) Analog/Digital Encoder/Decoder platforms. First introduced in 2005, this system is being deployed around the United States in a wide variety of Cable, Broadcast, IPTV, and Emergency Operation facilities. The EAS device is built with the latest digital PC computer technology along with software based encoding/decoding technology and is built upon the Linux OS. The core hardware is a standard PC motherboard and digital audio sound cards. The EAS device is easy to upgrade, not requiring custom ROMS. The EAS device also exploits the benefits of modern network technology. It is fully operable over a LAN using secure network protocols. In addition, it supports existing methods of device control using a serial port. This platform is representative of the continuing advancement of PC hardware into technological areas that only a few years ago required custom hardware.

Hardware Specs

- ▶ 2x20 backlit LCD display for monitoring unit and decoder status
- ▶ Operational status LED
- ▶ Alert decoding/output LED
- ▶ Cool running, low power CPU
- ▶ Add operating temp here
- ▶ Ethernet port for network access
- ▶ Base unit has one 3.5mm mini-jack audio input port that supports Scanning/decoding EAS on two radio channels
- ▶ Hard drive or flash drive options
- ▶ 3.5mm mini-jack stereo audio output port
- ▶ 3.5mm mini-jack microphone input
- ▶ 1 RS-232 Serial port supports a variety of serial control protocols, including industry standards like TFF Standard and Sage Generic.
- ▶ 1 parallel port will support a variety of printers
- ▶ 2 USB ports - will support a 2nd Ethernet port, extra serial ports, printers, modems, wireless Ethernet, flash drives, etc.
- ▶ VGA out for console or desktop GUI interface
- ▶ One NTSC video output
- ▶ Standard PS/2 keyboard/mouse ports
- ▶ Supports two PCI expansion cards, use with audio card for scanning two more Audio inputs (total of up to six EAS audio sources)
- ▶ Internal speaker for monitoring
- ▶ Can be safely powered off/on without disk damage
- ▶ Optional 3 internal radio receivers, GPI input/output and balanced audio output module.
- ▶ Optional MPEG2 and MPEG4 video/audio encoding card

General Software Features/Specs

- ▶ Linux version 2.6.32 operating system / CentOS release 6.9 (Final)
- ▶ Built in multi-user, password protected Web interface for control/status/monitoring of all activity.
- ▶ Web interface supports 128-bit encrypted Secure Socket Layer (SSL).
- ▶ Email for decoded/forwarded/originated/error alerts & system status
- ▶ Supports 2nd network interface via USB
- ▶ Supports a variety of printers via USB/Parallel
- ▶ Operational status indication via LED and LCD
- ▶ Web interface for easy software update
- ▶ Programmable GPI input to trigger actions and GPI output relays during alerts.
- ▶ English and English/Spanish EAS text translations. Editable EAS translations.
- ▶ Configurable audio output port selection for alert origination and forwarding.
- ▶ Audio level input/output controls via Web Interface.
- ▶ Audio file upload.
- ▶ Configurations file download/upload.

Decoder/Forwarding Features

- ▶ Decodes FCC EAS codes and NOAA SAME codes from radio transmissions or other analog audio input.
- ▶ Automatic audio level correction for reliable operation. Advanced error detection, correction, and logging for noisy EAS transmissions and troubleshooting quality of service problems.
- ▶ Supports fully unattended operation.
- ▶ Supports manual and user configurable filtered automatic alert auto-forwarding. Easy to use web interface for configuration of auto-forwarding locations and codes.
- ▶ Web interface makes it easy to review and print logs of active and expired decoded/forwarded alerts.
- ▶ Automatic alert storage management.
- ▶ Manages and displays multiple unique simultaneous active decoded alerts.
- ▶ Decoding status displayed on unit LCD and LED & Web interface.
- ▶ Stores each audio section of EAS alerts into digital files.
- ▶ Supports TFT-911 serial protocol for alert audio playback and alert translation data transfer from devices requiring TFT. Supports a variety of other serial protocols for operating CGs.
- ▶ Will support scanning up to six decoder input channels (depends on hardware expansion)
- ▶ Optional support for a variety of network forwarding protocols: EAS NET (with DVS-168), DVS-644(SCTE-18), and streaming MPEG2 and MPEG4 output digital interfaces.

Encoder/Origination Features

- ▶ Easy to use Web interface for creating and sending FCC EAS alerts.
- ▶ Web interface makes it easy to configure commonly used locations and alert types.

- ▶ Web interface makes it easy to review and print logs of active and expired originated alerts.
- ▶ All audio sections of encoded alerts are stored into separate digital audio files.
- ▶ Automatic originated alert storage management.
- ▶ Supports multiple unique simultaneous active originated alerts.
- ▶ Automatic randomized weekly test generation within user configurable calendar time spans.
- ▶ Web interface upload feature for digital audio files makes it easy to encode the audio portion of EAS alerts.
- ▶ Supports direct recording of EAS alert audio into digital files.
- ▶ GPI input controlled alert audio dubbing.
- ▶ Optional support for a variety of network origination protocols: EAS NET (with DVS-168), DVS-644(SCTE-18), and streaming MPEG2 and MPEG4 output digital interfaces

THE EMERGENCY ALERT SYSTEM

Purpose

According to the FCC, “The EAS is designed to provide the President with a means to address the American people in the event of a national emergency. Through the EAS, the President would have access to thousands of broadcast stations, cable systems and participating satellite programmers to transmit a message to the public. The EAS and its predecessors, CONELRAD and the Emergency Broadcast System (EBS), have never been activated for this purpose. But beginning in 1963, the President permitted state and local level emergency information to be transmitted using the EBS.”

However, the EAS system is used for much more than to support a method of communication that has never been (and hopefully never will be) used. The EAS system provides state and local officials with a method to quickly send out important local emergency information targeted to a specific area. This includes weather alerts as well as local emergency alerts such as child abductions and disasters. The EAS system also runs test alerts on a weekly and monthly basis in order to insure operability.

Operation

The EAS system digitally encodes data into audible audio in order to distribute messages. This information can be sent out through a broadcast station and cable system. The EAS digital signal uses the same encoding employed by the National Weather Service (NWS) for weather alerts broadcast over NOAA Weather Radio (NWR). Broadcasters and cable operators can decode NWR alerts and then retransmit NWS weather warning messages almost immediately to their audiences. With the proper equipment and setup, EAS alerts can be handled automatically, making EAS information useful for unattended stations. Other specially equipped consumer products, built into some televisions, radios, pagers and other devices, can decode user selectable EAS messages.

The device is designed to facilitate the management side of encoding and decoding EAS alerts within cable and broadcast facilities. It is especially easy to use since it is IP addressable and accessible over a LAN.

Management

The FCC designed the EAS system, working in cooperation with the broadcast, cable, emergency management, alerting equipment industry, the National Weather Service (NWS) and the Federal Emergency Management Administration (FEMA).

The FCC provides information to broadcasters, cable system operators, and other participants in the EAS regarding the requirements of this emergency system. Additionally, the FCC ensures that EAS state and local plans developed by industry conform to the FCC EAS rules and regulations and enhance the national level EAS structure.

NWS provides emergency weather information used to alert the public of dangerous conditions. Over seventy percent of all EAS and EBS activations were a result of natural disasters and were weather related. Linking NOAA Weather Radio digital signaling with the EAS digital signaling will help NWS save lives by reaching more people with timely, site-specific weather warnings.

FEMA provides direction for state and local emergency planning officials to plan and implement their roles in the EAS.

What you need to do as a Broadcaster

The encoder/decoder allows your facility to decode EAS alerts originated from alert sources in your area. These sources can be radio, TV, and cable TV stations. These stations can be forwarding alerts received from a web of broadcasters, or originating alerts if designated as a primary source. **To meet minimum requirements of the FCC, you must send randomized weekly tests, forward monthly tests, and forward National alerts.** Your state and local EAS plan may also impose other requirements.

A good source of information is the EAS website at <https://www.fcc.gov/general/emergency-alert-system-eas>. The FCC provides handbooks in Adobe PDF format for AM and FM radio, for TV and for Cable TV.

PERIPHERALS

The DASDEC/One-Net supports many peripheral devices, from character generators to printers. As of this release, the EAS device can replace most commercial EAS encoder/decoder units, depending upon the peripheral hardware to which they have been connected.

Monroe Electronics Cable Envoy and CEMS 500/1000

The EAS device directly supports Monroe Electronics Cable Envoy multi-channel analog video CG and the CEMS 0500/1000 single channel analog video crawl overlay keyer. The Cable Envoy interacts with and acts as a controller for the EAS device. For instance, it controls running audio from the EAS device. The CEMS unit is a basic CG to which the EAS device can send text crawl commands. Both Monroe units require a straight through RS-232 cable. The Monroe CEMS requires a valid TV license key. See EAS equipment at www.monroe-electronics.com.

Keywest VDS-830/840/Starmu/Star-8

The EAS device directly supports the single channel analog Keywest Technology VDS-830 and 840 character generator units. These units require a NULL modem RS-232 cable. The EAS device can crawl alert text on the VDS as well as provide severity color coded backgrounds. The VDS-830 cannot key the crawl over a video background. It will

utilize a full page with a gray background. The VDS-840 can key the crawling text over live video. The EAS device also has modes to support the Starmu and Star-8 CG's. This option requires a valid TV license key. See www.keywesttechnology.com.

Chyron CODI

The EAS device can replace systems that operate Chyron CODI character generators. The EAS device supports both the analog CODI as well as the Digibox CODI. The EAS device can crawl alert text overlaid on live video on these units. The Digibox CODI provides SDI digital video input and output. The EAS device also supports simultaneous network based control of multiple CODI Digibox units that provide a built-in LAN port. This valid TV and Plus Package license keys. See www.chyron.com.

Evertz Keyers

Evertz Logo Inserters, Media Keyers, and other digital and analog Evertz character generators are supported by the EAS device using the SAGE generic CG protocol. The Evertz unit must support an EAS option and be pre-programmed to recognize EAS communication on the specific COM port being used. For digital operation the EAS device must be equipped with an optional AES audio output or the EAS device Analog audio needs to be encoded into AES digital audio with an A to D converter. The GPI EAS Audio output of the EAS device is used as an input to trigger voice-over activation on the Evertz unit. The Evertz units handle all switching between normal program video/audio to EAS play-out. The EAS device offers manual alert forwarding notification with GPI output relay indication of pending alerts. This allows EAS to be forwarded when appropriate, either manually by an operator or by automation. See the diagram below.

The directions provided by Evertz for the SAGE generic protocol has been tested by Evertz and will work with the EAS device. See www.evertz.com.

XBOB CG

The EAS device can generate a crawl on a single video channel that is passed through an XBOB. This option requires a valid TV license key.

BetaBrite LED sign

The EAS device supports driving the wide range of BetaBrite LED signs from a EAS device serial port. A special cable is usually needed to connect the EAS device RS-232 serial ports to a BetaBrite. The Betabrite protocol on the EAS device supports running EAS alert text crawls immediately upon decoding as well as during alert origination and forwarding.

Other Character Generators

Any character generator or turnkey system that can operate the standard TFT 911 EAS serial control protocol or supports the SAGE Generic protocol can interface to a EAS device. A Null modem cable from the CG serial port must be connected to the EAS device serial port for TFT emulation. The serial cable required for units using the SAGE Generic CG protocol depends on the unit.

Character generators that can be run from the SAGE generic CG protocol include Evertz Keyers and Miranda ImageStore units.

Utah Scientific SqueezeMax

Interfacing to a TV system with Utah Scientific SqueezeMax HD system with Utah Scientific 2020 switcher, downstream mode.

The EAS device can interface to multiple SqueezeMax units using the LAN based EAS NET protocol, but the alert must be played on all SqueezeMax units at the same time. EAS NET sends alert text to each interfaced SqueezeMax unit and then goes into a pending alert play-out state. The text alert sent to the SqueezeMax places it into a pending EAS play-out mode. The EAS crawl can then be triggered manually on the SqueezeMax via 2020 Master Control switcher when desired (within a few minutes). Master Control supports this action via a custom macro, associated with a panel button, which triggers the SqueezeMax EAS preset, switches audio output to the EAS device input, and produces a GPI contact closure for triggering alert play-out on the EAS device. The EAS device goes out of pending alert mode and plays the alert audio until finished. When the alert is finished, SqueezeMax is taken out of EAS display and Master Control returns audio back to normal program audio.

The EAS device can also be directly connected to a single SqueezeMax using a serial connection.

Interfacing to a TV system with Utah Scientific SqueezeMax SD system with Utah Scientific 2020 switcher, upstream mode.

Refer to the description above for the SqueezeMax. An EAS device can interface to mixed SD and HD SqueezeMax units, but as described above, the alert must be played on all units at the same time.

For additional information refer to the Digital Alert Systems website's application notes. (http://www.digitalalertsystems.com/resources_application_notes.htm#)

EAS PROTOCOL

The EAS device encodes the EAS messages per FCC rules for the EAS protocol. The EAS protocol from the FCC is described as follows (printed directly from the FCC ruling).

The EAS uses a four-part message for an emergency activation of the EAS. The four parts are; Preamble and EAS Header Codes, audio Attention Signal, message, and, Preamble and EAS End Of Message Codes.

The Preamble and EAS Codes must use Audio Frequency Shift Keying at a rate of 520.83 bits per second to transmit the codes. Mark frequency is 2083.3 Hz and space frequency is 1562.5 Hz. Mark and space time must be 1.92 milliseconds. Characters are ASCII seven bit characters as defined in ANSI X3.4-1977 ending with an eighth null bit (either 1 or 0) to constitute a full eight-bit byte.

The Attention Signal must be made up of the fundamental frequencies of 853 and 960 Hz. The two tones must be transmitted simultaneously. The Attention Signal must be transmitted after the EAS header codes.

The message may be audio, video or text.

The ASCII dash and plus symbols are required and may not be used for any other purpose. Unused characters must be ASCII space characters. FM or TV call signs must use a slash ASCII character number 47 (/) in lieu of a dash.

The EAS protocol, including any codes, must not be amended, extended or abridged without FCC authorization. The EAS protocol and message format are specified in the following representation. Examples are provided in FCC Public Notices.

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJHHMM-LLLLLLLL-
(one second pause)

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJHHMM-LLLLLLLL-
(one second pause)

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJHHMM-LLLLLLLL-
(At least a one second pause)

(Transmission of 8 to 25 seconds of Attention Signal)

(Transmission of audio, video or text messages)

(at least a one second pause)

[PREAMBLE]NNNN

(One second pause) **[PREAMBLE]NNNN**

(One second pause) **[PREAMBLE]NNNN**

(At least one second pause)

[PREAMBLE] This is a consecutive string of bits (sixteen bytes of AB hexadecimal [8 bit byte 10101011]) sent to clear the system, set AGC and set asynchronous decoder clocking cycles. The preamble must be transmitted before each header and End Of Message code.

ZCZC- This is the identifier, sent as ASCII characters ZCZC to indicate the start of ASCII code.

ORG- This is the Originator code and indicates who originally initiated the activation of the EAS. These codes are specified in paragraph (d) of this section.

EEE- This is the Event code and indicates the nature of the EAS activation. The codes are specified in paragraph (e) of this section. The Event codes must be compatible with the codes used by the NWS Weather Radio Specific Area Message Encoder (WRSAME).

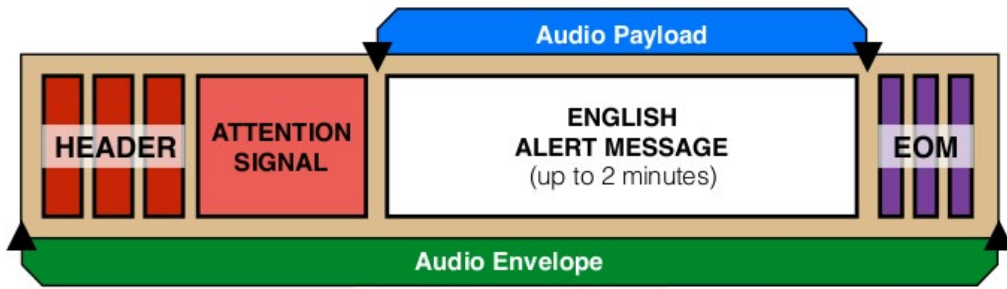
PSSCCC- This is the Location code and indicates the geographic area affected by the EAS alert. There may be 31 Location codes in an EAS alert. The Location code uses the Federal Information Processing Standard (FIPS) numbers as described by the U.S. Department of Commerce in National Institute of Standards and Technology publication FIPS PUB 6-4. Each state is assigned an SS number as specified in paragraph (f) of this section. Each county and some cities are assigned a CCC number. A CCC number of 000 refers to an entire State or Territory. P defines county subdivisions as follows: 0 = all or an unspecified portion of a county, 1 = Northwest, 2 = North, 3 = Northeast, 4 = West, 5 = Central, 6 = East, 7 = Southwest, 8 = South, 9 = Southeast. Other numbers may be designated later for special applications. The use of county subdivisions will probably be rare and generally for oddly shaped or unusually large counties. Any subdivisions must be defined and agreed to by the local officials prior to use.

+TTTT- This indicates the valid time period of a message in 15 minute segments up to one hour and then in 30 minute segments beyond one hour; i.e., +0015, +0030, +0045, +0100, +0430 and +0600.

JJHHMM- This is the day in Julian Calendar days (JJJ) of the year and the time in hours and minutes (HHMM) when the message was initially released by the originator using 24 hour Universal Coordinated Time (UTC).

LLLLLLLL- This is the identification of the broadcast station, cable system, MDS/MMDS/ITFS station, NWS office, etc., transmitting or retransmitting the message. These codes will be automatically affixed to all outgoing messages by the EAS encoder.

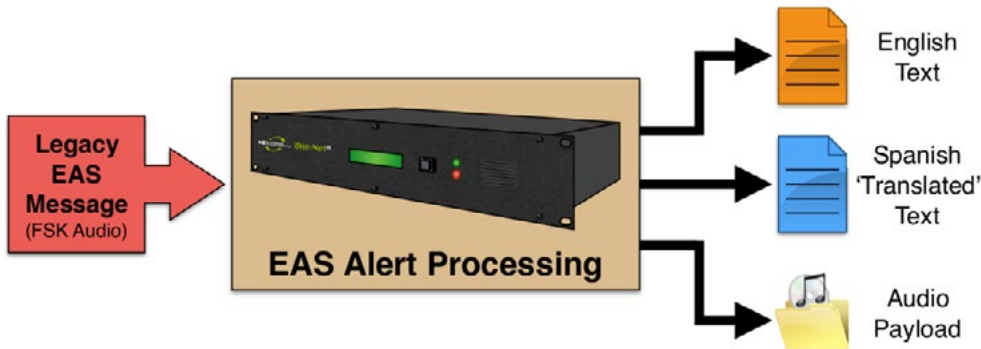
NNNN- This is the End of Message (EOM) code sent as a string of four ASCII N characters.



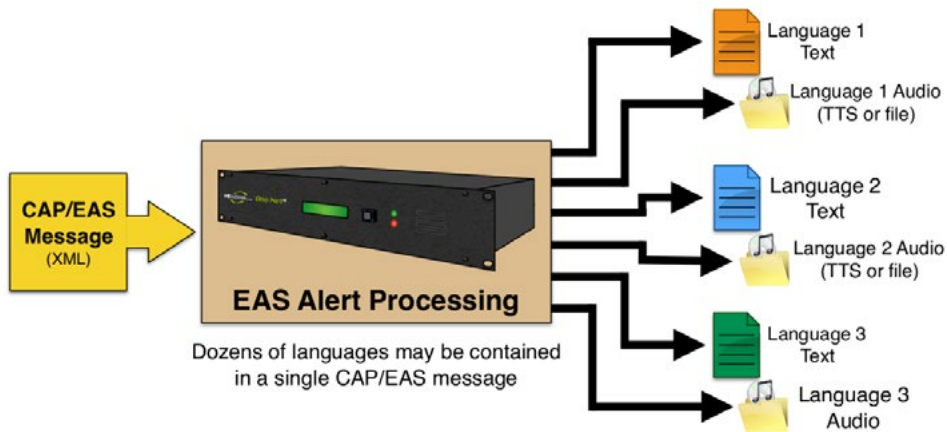
Incoming EAS Alert Message
(FSK Audio)



Originated/Forwarded EAS Alert Message
(with Pre-Alert, Post-Alert, & Ext. Alert Language Audio Options)



Legacy EAS Message Processing



CAP/EAS Message Processing
(XML)

The only originator codes are:

Originator Description	Originator Code
Code Broadcast station or cable system	EAS
Civil authorities	CIV
National Weather Service	WXR
Primary Entry Point System	PEP

The following Event (EEE) codes are presently authorized:

The following tables includes four columns describing EAS Codes: Nature of Action (description of Event Code), Event Code, Type, and maximum amount of time Delay allowed when forwarding the EAS alert.

National Codes (Required):

Nature of Action	Event Code	Type	Delay (:MM)
Emergency Action Notification	EAN (National only)	Emergency	:00
National Periodic Test	NPT (National only)	Test	:00
National Information Center	NIC (National only)	Advisory	:15
Required Monthly Test	RMT	Test	:60
Required Weekly Test	RWT	Test	:15

State and Local Codes (Optional):

Nature of Action	Event Code	Type	Delay (:mm)
Administrative Message	ADR	Advisory	:15
Avalanche Warning	AVW	Warning	:15
Avalanche Watch	AVA	Watch	:15
Blizzard Warning	BZW	Warning	:15
Blue Alert	BLU	Warning	:15
Child Abduction Emergency	CAE	Emergency	:15
Civil Danger Warning	CDW	Warning	:15
Civil Emergency Message	CEM	Emergency	:15
Coastal Flood Warning	CFW	Warning	:15
Coastal Flood Watch	CFA	Watch	:15
Demo / Practice Warning	DMO	Test	:15
Dust Storm Warning	DSW	Warning	:15
Earthquake Warning	EQW	Warning	:15
Extreme Wind Warning	EWW	Warning	:15
Evacuation Immediate	EVI	Emergency	:15
Fire Warning	FRW	Warning	:15
Flash Flood Warning	FFW	Warning	:15
Flash Flood Watch	FFA	Watch	:15
Flash Flood Statement	FFS	Advisory	:15



New Feature

The Blue Alert EAS event code (BLU) has been added to version 4.0 in compliance with the Federal Communications Commission's 47 CFR Part 11 final rule.

Nature of Action	Event Code	Type	Delay (:mm)
Flood Warning	FLW	Warning	:15
Flood Watch	FLA	Watch	:15
Flood Statement	FLS	Advisory	:15
Hazardous Materials Warning	HMW	Warning	:15
High Wind Warning	HWW	Warning	:15
High Wind Watch	HWA	Watch	:15
Hurricane Warning	HUW	Warning	:15
Hurricane Watch	HUA	Watch	:15
Hurricane Statement	HLS	Advisory	:15
Law Enforcement Warning	LEW	Warning	:15
Local Area Emergency	LAE	Emergency	:15
Network Message Notification	NMN	Advisory	:15
911 Telephone Outage Emergency	TOE	Emergency	:15
Nuclear Power Plant Warning	NUW	Warning	:15
Radiological Hazard Warning	RHW	Warning	:15
Severe Thunderstorm Warning	SVR	Warning	:15
Severe Thunderstorm Watch	SVA	Watch	:15
Severe Weather Statement	SVS	Advisory	:15
Shelter in Place Warning	SPW	Warning	:15
Special Marine Warning	SMW	Warning	:15
Special Weather Statement	SPS	Advisory	:15
Storm Surge Watch	SSA	Watch	:15
Storm Surge Warning	SSW	Warning	:15
Tornado Warning	TOR	Warning	:15
Tornado Watch	TOA	Watch	:15
Tropical Storm Warning	TRW	Warning	:15
Tropical Storm Watch	TRA	Watch	:15
Tsunami Warning	TSW	Warning	:15
Tsunami Watch	TSA	Watch	:15
Volcano Warning	VOW	Warning	:15
Winter Storm Watch	WSA	Watch	:15
Winter Storm Warning	WSW	Warning	:15

TERMS AND DEFINITIONS

Term	Definition
AEA	A key component of ATSC 3.0 - the next generation broadcasting standard. Advanced Emergency Alert (AEA) is still in the implementation phase, but promises to create enhanced value for viewers, broadcasters, electronics manufacturers, and emergency alerting authorities with on-screen, rich media emergency alerting information.
AES	Is a standard for the exchange of digital audio signals between professional audio devices. AES was jointly developed by the Audio Engineering Society (AES) and the European Broadcasting Union (EBU). Also known as AES3 or AES/EBU.
BNC	A round, quick connect/disconnect radio frequency connector used for coaxial cable. It features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. The connector was named the BNC (for Bayonet Neill–Concelman) after its bayonet mount locking mechanism and its inventors, Paul Neill and Carl Concelman.
CAP	The Common Alerting Protocol (CAP) is an XML-based data format for exchanging public warnings and emergencies between alerting technologies. CAP allows a warning message to be consistently disseminated simultaneously over many warning systems to many applications. CAP is an international standard that has been adapted by several countries to communicate emergency warnings including, Australia (CAP-AU-STD), Canada (CAP-CP/NPAS), Germany (MoWaS), and the United States (IPAWS-OPEN).
CAT-5 Cable	Category 5 cable (or CAT-5), is a twisted pair cable for carrying signals. This type of cable is used in structured cabling for computer networks such as Ethernet. The cable standard provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet). Category 5 was superseded by the category 5e (enhanced) specification, and later category 6 cable.
CG	A character generator (CG) is a device or software that produces static or animated text (such as crawls and credits rolls) for keying into a video stream.
EAS	The Emergency Alert System (EAS) is a national warning system in the United States put into place on January 1, 1997, when it replaced the Emergency Broadcast System (EBS), which in turn replaced the CONELRAD System. EAS is also designed to alert the public of local weather, law enforcement, and civil emergencies.
Ethernet	Ethernet is a family of computer networking technologies commonly used in local area networks (LANs). Frequently used wiring is CAT5/6 twisted pair cables with RJ-45 connectors (or 8P8C modular connectors).

Term	Definition
FCC	An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. The commission is the United States' primary authority for communications laws, regulation and technological innovation.
FIPS Codes	Geographic codes developed by the Federal Information Processing Standards (FIPS) that establish six digit numeric values for US states, counties, subdivision of counties and other predefined geographic boundaries.
FSK	Frequency-shift keying (FSK) is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal. FSK is used to transmit data within the EAS header.
GPIO	General-purpose input/output (GPIO) is a generic pin on an integrated circuit whose behavior—including whether it is an input or output pin—is controllable by the user at run time.
Hyperlink	A hyperlink is a reference to data the reader can directly follow either by clicking or hovering over. A hyperlink points to a whole document or to a specific element within a document. Hyperlinks are typically displayed in blue, underlined text: FIPS Groups .
IP Address	An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. Because of the growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed. IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6).
LED	A light-emitting diode (LED) is a two-lead semiconductor light source. When a suitable voltage is applied to the leads, electrons release energy in the form of photons – also called electroluminescence.
MPEG	The Moving Picture Experts Group (MPEG) is a working group of authorities that was formed by ISO and IEC to set standards for audio and video compression and transmission.

Term	Definition
NOAA	The National Oceanic and Atmospheric Administration (NOAA) is an American scientific agency within the United States Department of Commerce focused on the conditions of the oceans and the atmosphere. NOAA warns of dangerous weather, charts seas, guides the use and protection of ocean and coastal resources, and conducts research to improve understanding and stewardship of the environment.
NTP	Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).
PS/2	The PS/2 connector is a 6-pin mini-DIN connector used for connecting some keyboards and mice to a PC compatible computer system.
RCA Connector	Sometimes called a phono connector or Cinch connector, is a type of electrical connector commonly used to carry audio and video signals. The name "RCA" derives from the Radio Corporation of America, which introduced the design by the early 1940s for internal connection of the pickup to the chassis in home radio-phonograph consoles.
RJ45 Connector	The RJ45 connector (also known as 8 position 8 contact (8P8C)) is a modular connector commonly used to terminate twisted pair and multi-conductor flat cable. These connectors are commonly used for Ethernet over twisted pair.
RG6	RG-6 is a common type of coaxial cable and is generally used to refer to coaxial cables with an 18 AWG center conductor and 75 ohm characteristic impedance.
SCTE-18	A standard developed by the Society of Cable Telecommunication Engineers (SCTE) that defines an Emergency Alert signaling method for use by cable TV systems to signal emergencies to digital receiving devices that are offered for retail sale. Such devices include digital settop boxes that are sold to consumers at retail, digital TV receivers, and digital video recorders. Also referred to as DVS644.
Serial Port	A serial communication interface through which information transfers in or out one bit at a time. The term "serial port" identifies hardware compliant to the RS-232/422 standards, intended to interface with external CG's.

Term	Definition
TRS Connector	A three-contact phone connector (also known as phone jack, audio jack or jack plug) where T stands for “tip”, R stands for “ring” and S stands for “sleeve”. Is derived from a common family of connector typically used for analog audio signals. The outside diameter of the “sleeve” conductor is 1/4 inch (exactly 6.35 mm). The “mini” connector has a diameter of 3.5 mm (approx. 1/8 inch) and the “sub-mini” connector has a diameter of 2.5 mm (approx. 3/32 inch).
USB	Universal Serial Bus (USB) is an industry standard that defines the cables, connectors and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices.
VGA	Video Graphics Array (VGA) refers to the analog computer display standard found within the 15-pin D-subminiature VGA connector.
Web Browser	Commonly referred to as a browser - is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI/URL) and may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources. The major web browsers are Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Opera.
XLR Connector	The XLR connector is a style of electrical connector, primarily found on professional audio, video, and stage lighting equipment. The connectors are circular in design and have between 3 and 7 pins. They are most commonly associated with balanced audio, including AES3 digital audio.

END USER LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS ("Agreement") CAREFULLY. USE OF THE SOFTWARE defined below) PROVIDED BY DIGITAL ALERT SYSTEMS, INC. IS PERMITTED ONLY UNDER AND IN ACCORDANCE WITH THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, PLEASE DO NOT USE THIS SOFTWARE.

1. Grant of License. This Agreement permits you to have a limited, non-transferable, non-exclusive, license for use of the Software or the software included in this device ("Software"). For each software licensee, the program can be "in use" on, or in conjunction with the DASDEC™, DASDEC-II, DASEOC™, R189 One-Net™ and/or R189SE One-Net SE ("Device"). **IF YOU DO NOT AGREE TO BE LEGALLY BOUND TO BY THIS AGREEMENT IN ITS ENTIRETY, AND WITHOUT CHANGE TO ITS TERMS AND CONDITIONS, YOU DO NOT HAVE A LICENSE TO USE THIS SOFTWARE.**

2. License Restrictions. YOU MAY NOT RENT, LEASE, SUBLICENSE, SELL, ASSIGN, LOAN OR OTHERWISE TRANSFER THE SOFTWARE OR ANY OF YOUR RIGHTS AND OBLIGATIONS UNDER THIS AGREEMENT. You may not modify, translate, reverse assemble, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate or otherwise circumvent any software protection mechanisms in the Software, including without limitation any such mechanism used to restrict or control the functionality of the Software, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Software (except to the extent that such activities may not be prohibited under applicable law). However, you may transfer all your right to use the Software to another person or organization, provided that (a) the followings are also transferred with the Software, (i) this Agreement;(ii) other software if contained in the original package, and/or hardware that the Software is bundled;(iii) any original or updated version of the Software; (b) no copies including back-up and installed in your computer or other device are at your possession after the transfer, and (c) the recipient accepts all the terms of this Agreement. In no event shall you transfer the Software obtained as a trial, test version, or otherwise specified as not for resale. A special license permit from DIGITAL ALERT SYSTEMS is required if the program is going to be installed on a network server for the sole purpose of distribution to other computers.

3. Copyright. The Software or the Software contained in this package or device is protected by United States copyright laws, international treaty provisions, and all other applicable national laws. The Software must be treated like all other copyrighted materials (e.g. books and musical recordings). This license does not allow the Software to be rented or leased, and the written materials accompanying the Software (if any) may not be copied.

4. Ownership. Title, ownership rights, and all intellectual property rights in and to the Software and any accompanying documentation, and any copy of the foregoing, and any sample contents shall remain the sole and exclusive property of Digital Alert Systems and/or its third party licensors. You agree to abide by the copyright law and all other applicable laws. You acknowledge that the Software contains valuable confidential information and trade secrets of Digital Alert Systems and/or its third party licensors.

5. Warranty Disclaimer. THE SOFTWARE IS MADE AVAILABLE TO YOU ON “AS IS” BASIS. NO WARRANTIES, EITHER EXPRESS OR IMPLIED, ARE MADE WITH RESPECT TO THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES FOR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY, AND DIGITAL ALERT SYSTEMS EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED HEREIN. YOU ASSUME THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE. SHOULD THE SOFTWARE PROVE DEFECTIVE, YOU, AND NOT DIGITAL ALERT SYSTEMS OR AN AUTHORIZED RESELLER, ASSUME THE ENTIRE COST OF NECESSARY SERVICING, REPAIR, OR CORRECTION. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE. YOUR SOLE REMEDY AND THE ENTIRE LIABILITY OF DIGITAL ALERT SYSTEMS ARE SET FORTH ABOVE.

6. No Liability for Consequential Damages. YOU AGREE THAT IN NO EVENT SHALL DIGITAL ALERT SYSTEMS OR ITS AGENTS BE LIABLE FOR ANY LOSS OF ANTICIPATED PROFITS, LOSS OF DATA, LOSS OF USE, BUSINESS INTERRUPTION, COST OF COVER OR ANY OTHER INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE), EVEN IF DIGITAL ALERT SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL DIGITAL ALERT SYSTEMS BE LIABLE TO YOU FOR DAMAGES IN AN AMOUNT GREATER THAN THE FEES PAID FOR THE USE. THE FOREGOING LIMITATIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAWS IN YOUR JURISDICTION.

7. Export. You will not export or re-export the product incorporating the Software without the appropriate United States or foreign government licenses.

8. DISTRIBUTION TO THE U.S. GOVERNMENT: The Software and documentation qualify as “commercial items,” as that term is defined at Federal Acquisition Regulation (“FAR”) (48 C.F.R.) 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are “commercial computer software” and “commercial computer software documentation,” and constitutes acceptance of the rights and restrictions herein.

Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and/or the related documentation by the United States government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. Termination. THIS AGREEMENT SHALL BE EFFECTIVE UPON INSTALLATION OF THE SOFTWARE AND SHALL TERMINATE UPON THE EARLIER OF: (i) YOUR FAILURE TO COMPLY WITH ANY TERM OF THIS AGREEMENT; OR (ii) RETURN, DESTRUCTION OR DELETION OF THE DEVICE AND ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION. Digital Alert Systems’ rights and your obligations shall survive the termination of this Agreement.

10. High Risk Activities. The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, “High Risk Activities”). DIGITAL ALERT SYSTEMS EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

11. Governing Law and Jurisdiction. This Agreement will be governed by and construed under the laws of the State of New York and the United States as applied to agreements entered into and to be performed entirely within New York, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of the state and federal courts located in Orleans County, New York.

DASDEC AND ONE-NET CHASSIS CHART



One-Net SE Front Panel



Model: R189SE without radios



Model: R189SE with radios



DASDEC-II Front Panel



Model: DASDEC-II



Model: DASLPMR

Model: DASLPMF

Model: DASRADR

Model: DASRAD

Model: DASRADR/5

Model: DASDEC-IR



DASDEC-II Front Panel



Model: DASLPTV



Model: DASLPTVR

Model: DASTV

Model: DASLTVR

Model: DASTV/5

Model: DASTVR/5



DASDEC-LC Front Panel



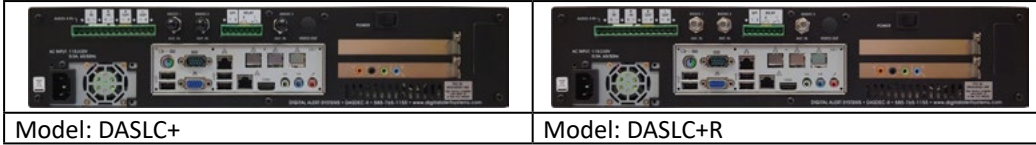
Model: DASLC



Model: DASLCR



DASDEC-LC Front Panel



Installed Options



Three additional NIC interfaces (triple port gigabit Ethernet option)



Expanded EAS Decoder Audio Inputs



Expanded GPIO Inputs and Outputs



MPEG 2 Card