



Version 6.1 Software

User's Guide



Revision 2.0

Digital Alert Systems, Inc.
100 Housel Ave • PO Box 535 • Lyndonville, NY 14098
www.digitalalertsistemas.com

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 © 2004-2026 Digital Alert Systems, Inc. All rights reserved.

Alert Agent™, DASDEC™, EAS-Net™, MultiPlayer™, MultiStation™, One-Net™, OmniLingual™, PureCAP™, PureCAP™ Plus, TDX™, HALO™, 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.

Unauthorized Third-Party Software/Firmware/Hardware

The DASDEC™/One-Net™ is a specialized appliance, not a general server product. Any modifications may cause issues with the proper functioning of the device, including disabling features, removal of security features, application instability, degradation of performance, and potential incompatibility with future software updates.

THE INSTALLATION OF ANY THIRD-PARTY PRODUCTS – HARDWARE OR SOFTWARE - OTHER THAN THOSE AUTHORIZED BY DIGITAL ALERT SYSTEMS (DAS) VOIDS ALL WARRANTIES.

Violating the warranty means DAS does not promise to support any repair, service, or replacement of a device having such third-party applications installed. DAS makes no warranty, implied or otherwise, regarding the performance or reliability of any third-party products (hardware or software).

The customer fully assumes all risks related to voiding equipment support, including any costs for repair and/or replacement, and non-compliance with any applicable regulatory rules should the third-party software interfere with the intended function and operation of the product.

Document Revision History

Date	Document Version	Content
2004 - 2023	Initial publication of the document to describe software version 5.1.	
2023	1.0	Software Version 5.2 with the following major changes: • Enhanced data security using encrypted file structure throughout the DASDEC system. • Changed 'NPT' label to 'Nationwide Test'. • Changed 'EAN' to 'National Emergency Message' • Text referencing a 'PEP' station is now 'United States Government' • Text referencing 'EAS' station is now 'EAS Participant' • Includes Text-to-Speech version 6.2.4. • Added pop-up Help on the Setup > Net Alerts > Stream MPEG page. • Matched the release with the most recent HALO package at 5.2.0.
2026	2.0	Software Version 6.1 with the following major changes: • The latest SSH security protocol and open SSL-based communication are not compatible with EAS-NET on DASDEC/ONE-NET units running V4.4 or lower. • Brand new 64-bit operating system (OS) with the latest security updates and ongoing support through 2032. • Support for the CAP Caribbean Barbados profile. • Direct access to the Amazon Web Services (AWS) S3 filesystem for MPEG-DASH alert data, enabling cloud service access to full-screen slides and audio. • Incorporated the Plus Package option for active Encoder devices. Upon installation of Version 6, if there is an active Encoder key, the Plus Package Option license will become 'VALID'. • Added audio-only option to DASH ISO-BMFF format • Improved audio monitoring when listening through the web interface.

Table of Contents

Introduction	1
Organization	1
Conventions.....	1
Chapter 1: Initial Setup.....	2
Making First Contact	2
Web Interface Login	3
Password Policy	4
Setting the IP Address.....	5
Chapter 2: Web Interface and Navigation	7
Input Elements	7
Action Buttons	7
Web Interface Layout	9
Web Interface Navigation	13
Chapter 3: Setup Tab.....	15
Main Setup	16
Network Setup.....	40
Time Setup.....	56
Users Setup.....	59
Email Setup.....	66
Audio Setup	70
Video/CG Setup	80
Alert Agent™ Setup	98
Station Setup	119
Demo/Practice Setup	130
Net Alerts Setup	133
GPIO Setup	167
Printer Setup.....	175
Alert Storage Setup	177
Chapter 4: Alert Events Tab	179
Auto-Refresh Timer	179
Decode Activity Table	180
Active	181
Incoming/Decoded	182
Forwarded Alerts	190
Originated/Forwarded Alerts	191
Originated Alerts	191
All Alerts	192
Backing Up EAS Event Logs.....	193
Chapter 5: Send Alerts Tab	195
General Alerts.....	196
One-Button Alert	208
Custom Message	211
Chapter 6: System Tab	222

Help	222
Status.....	224
Logs.....	225
Debug Logs	226
Appendix	I
The Emergency Alert System.....	I
Peripherals.....	II
EAS Protocol	IV
Terms and Definitions	VIII
Unauthorized Third Party Software/Firmware/Hardware	XII
Return to Factory Policy	XIII
End User License Agreement.....	XIV

Introduction

This manual describes the platform features, provides step-by-step instructions, and includes sample screenshots for quick reference.

Organization

Early chapters provide features and descriptions of the software for your Emergency Alert System (EAS) device. Setup tasks are presented in the order they should be completed, guiding a first-time user through basic setup in the most efficient way to configure the EAS device step-by-step. Advanced features are included later in the manual, including integrating with other software applications and hardware.

Hardware information and configuration details can be found in the Hardware/Installation Guide.

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 > Main > Upgrade** means you should select the **Setup** tab, then the **Main** navigation tab, and then the **Upgrade** sub-tab.
- Screen names/page titles are presented in **bold**.
- Buttons, pull-down menu labels, text box labels, check box descriptions, and radio button 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.

Tabs and Buttons are presented as seen on the screen. In many cases, these images will highlight a small portion of the complete screenshot, 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.

Chapter 1: Initial Setup

Making First Contact

The DASDEC/One-Net platform contains 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 Edge®, or Mozilla Firefox®. You will connect to the same network as the EAS device, launch a web browser, and input the device 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:

- A direct connection
- 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. See the Hardware/Installation Guide for 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:

- Turn on the EAS device by pressing and releasing the power switch on the upper right side of the back panel.
- The LCD screen will light during the power on.
- Allow the device time to boot.
- Refer to the Front Panel Display section in the Hardware/Installation Guide for a description of pages and lines.

Note: Information at rest is fully encrypted on the storage media. Enhanced data security using encrypted file structure has been integrated throughout the DASDEC system.

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.**

Web Interface Login

Launch a web browser application from a computer located on the same local area network (LAN) as the EAS device you intend to reach. Type the EAS device's 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 below.

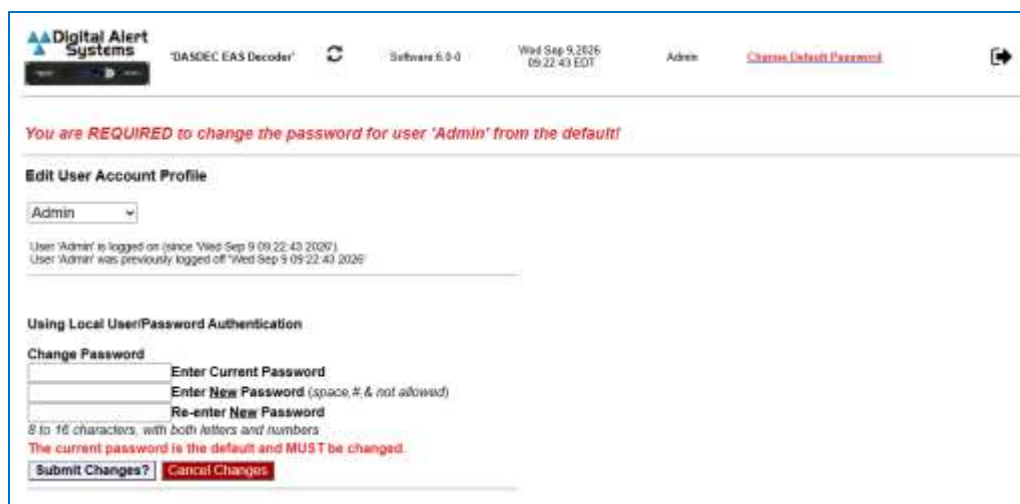
The image shows the login screen of the Digital Alert Systems DASDEC EAS Decoder. It features the company logo on the top left, the device name and serial number on the top right, and a login form with fields for Username and Password, followed by a 'Sign me in' button. A copyright notice is at the bottom.

Web Interface Login Screen

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

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

Click the **Sign me in** button. If the username or password is incorrect, a **** Login failed. **** message will display above the **Sign me in** button, indicating the problem.

The image shows the 'Edit User Account Profile' screen. It includes a header with the system name, version, date, and user name. A red message states that the user is required to change their password. Below this, there's a section for 'Using Local User/Password Authentication' with a 'Change Password' form containing fields for current, new, and re-enter new passwords, along with a 'Submit Changes?' button.

Edit User Account Profile Screen

Upon initial user login, the **Edit User Account Profile** screen is displayed. 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 > Network > Configuration** screen (below). Near the top of this screen are 14 tabs, with the **Network** tab underlined in blue.
4. The Network Configuration Screen will be displayed (see below). This is the screen where the network settings are modified.



Setup > Network > Configuration Tab View

Note: After five failed login attempts, the system will display “Account Temporarily Suspended.” Contact your system administrator for assistance.

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 and a maximum of 16 characters.
- Passwords must contain both letters and numbers.
- Commonly used (and blacklisted) passwords are not allowed.
- The following text strings are forbidden in any password. These are not case sensitive, and any combination of upper and lower case are not allowed.
 - password
 - 12345678
 - qwerty
 - dasdec
 - onenet
- The EAS Device will visually alert users with passwords older than 180 days

Setting the IP Address

A new unit has a default IP address of 192.168.0.200 and must be changed to an unused IP address that matches the scheme of the network it will operate in.

To assign an IP address to the EAS device, navigate using the tabs at the top of the webpage labeled **Setup > Network > Configuration**.

Setup > Network > Configuration Sub-tab

- Set the **Network Type** to **Static (Manually Configure)** (*outlined in red*).
- Set the IP address of your network's internet gateway in **IP Address of Gateway** (*outlined in black*).
- Set the desired IP address for the EAS device, along with the proper subnet mask in **Manual Config Options** (*outlined in purple*).
- Double-check that your information is correct and click the **Accept Changes/Restart Network** button at the bottom of the page. The following screen will appear:



Changing Network Address/Restarting Web Server Screen

Note: The IP address assigned to the DASDEC/One-Net cannot match the IP address of any other device on your network, or it will create a conflict. If necessary, verify with your network administrator what IP address to set the EAS device.

The EAS device can now be connected to your network. Once the device is connected to your switch/router, launch a browser on a PC on the same network as the EAS device. Access the login page by typing the newly programmed IP into the browser's address bar.

Log in and navigate to the **Setup > Network > Configuration** page. Check the 'Use DNS?' box to add a DNS IP address.

The screenshot shows a web-based network configuration interface with a green background. At the top, it says "Network is 'Enabled'" and "Current IP : 192.0.0.214". Below this is a "Network Speed" section with a dropdown menu set to "Auto (recommended)". The "Network Type" section has two radio buttons: "Static (Manually Configure)" which is selected, and "Automatic (via DHCP)". Under "Manual Config Options", there are input fields for "IP Address" (192.0.0.214) and "IP Netmask" (255.255.255.0). The "Use DNS?" checkbox is checked. Below it are input fields for "Timeout (1-5 secs)" (3) and "Tries (1-2)" (2). Further down are input fields for "IP Address of Primary Nameserver" (8.8.8.8) and "IP Address of Second Nameserver" (8.8.4.4). There are also optional fields for "DNS Domain name" and "DNS Search name". At the bottom, there is a "Test Name" field with "www.example.com" and a "Test DNS" button.

Network Configuration Interface

Additional dialog boxes to input the network's primary and secondary nameservers are provided. Once entered, click the **Accept Changes/Restart Network** button. If you do not know or have DNS IP addresses, you can use a public DNS server such as 8.8.8.8 and 8.8.4.4 as an alternative.

Chapter 2: Web Interface and Navigation

Input Elements

Graphical elements, Navigation Tabs, Sub-Tabs, Hyperlinks, Pull-Downs, Check Boxes, Radio Buttons, and Text Fields are employed throughout the web interface, enabling 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. Once a Navigation Tab is selected, the Sub-Tabs contained within it will be displayed.



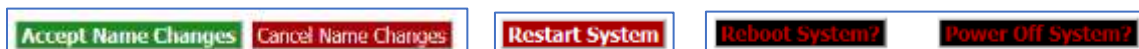
Example Navigation Tabs and Sub-Tabs

Sub-Tabs

Used to navigate the web interface within the currently selected Navigation Tab. When active, the Sub-Tab's background color will be lighter than the other Sub-Tabs.

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, accessing a pull-down menu, and many other functions.



Example Action Buttons

Pull-Down Menus

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.

Add New User Account

Enter unused login name

View Only Level Set permission level

View Only Level Enter account comment

Basic Operation Level Authentication Type

Operation Level

Operation/Control Level

Administration Level

Min 8 characters, with both letters and numbers

Example Pull-Down Menu

Check Boxes

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.

☐ Block Origination and Manual Forwarding during in progress alert announcement

☐ Use separate EAS Station IDs for Origination and Forwarding

Alert Origination

Set One-Button Required Weekly Test (RWT) Duration: 0 Hours 15 Mins

☒ Forwarded alerts halt creation of random Required Weekly Tests (RWT)

☒ Automatically Manage random Weekly Test removal upon firing of alerts

☐ Allow Required Weekly Test to include audio

☒ Front Panel Button generates Required Weekly Test (RWT)

☐ Tagged Alert Origination

Example Check Boxes

Text Fields

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, to input user credentials, and configuration settings as well. Text fields typically allow the entry of any alphanumeric text. In some instances, the text may be limited to just numbers, just letters, or may prohibit specific characters.

Current Access NIC Host: 192.0.0.208

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)

☐ 3rd Network Interface (if selected remember to enable 3rd network)

☐ 4th Network Interface (if selected remember to enable 4th network)

192.0.0.1 IP Address of Gateway

Example Text Fields and Radio Buttons

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 found on interface pages.

Hyperlinks

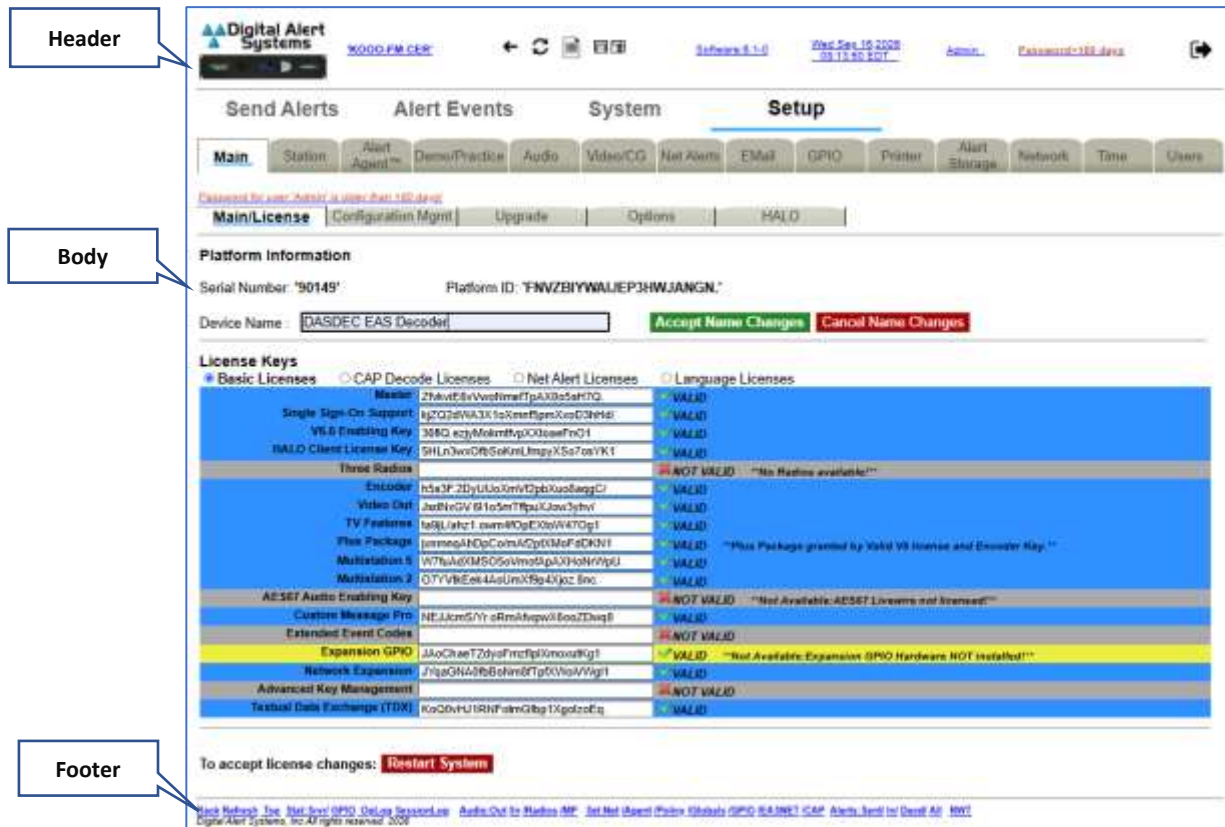
Text elements that are highlighted in blue and underlined link to another location within the web interface or to the World Wide Web. Hyperlinks assist in navigating the many menus found in the web interface. Click on a hyperlink to navigate to the indicated location.



Example Hyperlink

Web Interface Layout

The web interface contains dozens of unique screens that are organized with a system of tabs and sub-tabs. The main sections located across the top of the header are: **Send Alerts**, **Alert Events**, **System**, and **Setup**. Within each section, sub-sections are organized by navigation tabs and sub-tabs located directly below the tabs.



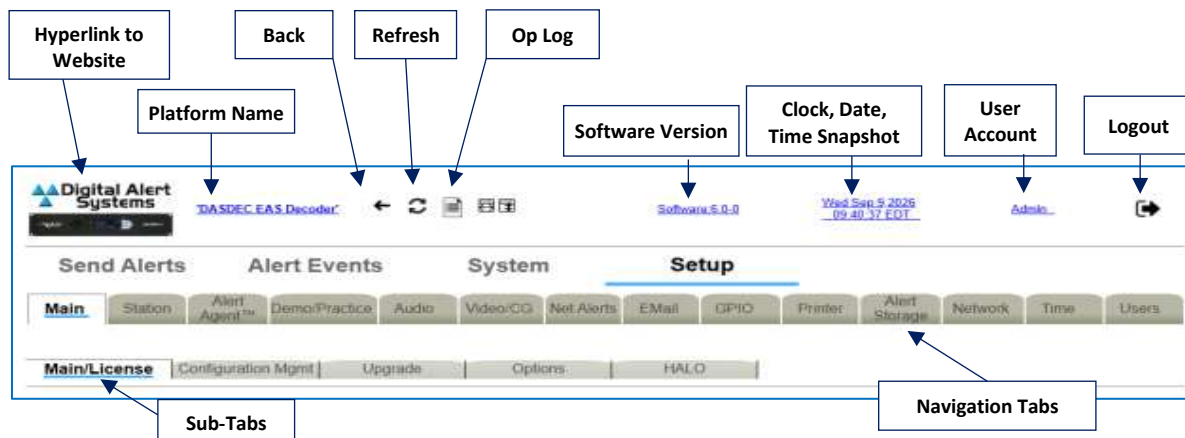
Web Interface Sections

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

The Header displays relevant information about the software and the path used to arrive at that screen.



Web Interface - Header Section

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

- **Link to DAS Website:** Click here to be directed to Digital Alert Systems' website.
- **Platform Name:** The Platform/Device Name, located near the top, left 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 device name, follow the hyperlink or navigate to **Setup > Main > Main/License**.
- **Back:** The preferred means of navigating back to the previously viewed web interface screen.
- **Refresh:** The preferred method to refresh the web interface.
- **OpLog:** A link to navigate to the **System > Logs > Operation Log** screen.
- **Software Version:** The installed software version is listed as a hyperlink (blue, underlined text); clicking the link will take you to the **System > Help > About DASDEC** page, where you can find additional information about the installed software.
- **Clock, 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.
- **User Account:** The current user is noted in the hyperlink. In instances where multiple users are logged in to the same device, the Username 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 in to 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.
- **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

Note: Using the back/refresh buttons on your web browser can provide out-of-date server information and may result in unintended actions being performed. Use the **Back** and **Refresh** navigation buttons in the web interface instead.

Navigation Tabs and Sub-Tabs

This section describes the sections of the screen.

Body

The **Body** is the main portion of the web interface, which allows for configuring settings, sending alerts, viewing alerts, and monitoring system parameters.

Platform Information

Serial Number: 'G31000' Platform ID: '2XHUKM8BJOS.OAVHEZL/7I'

Device Name: Accept Name Changes Cancel Name Changes

License Keys

☒ Basic Licenses ☐ CAP Decode Licenses ☐ Net Alert Licenses ☐ Language Licenses

License Key	Key	Status	Notes
Master	dcblgpeMced1gs7FocUREVTkd	VALID	
Single Sign-On Support	dbfkgWencsdXNBtBStnS8grHf5Q0	VALID	
VELO Enabling Key	d b f q g e 4 c d s Y C A X C M F t o x r 1	VALID	
HALO Client License Key	dbdq1eNcBdS7tqLFIEHvyDePie	VALID	
Three Radios	debtgleAcndPoncAAN.aVtL7LQA0	VALID	
Encoder	d4btqWetUc2syNAmcwoa57CIASjd	VALID	
Video Out	adbqgNeJcYdc2DdNgv1rdZj470	VALID	
TV Features	db3qnenclmVGAseF1fKPQWMBu0	VALID	
Plus Package	dubtqzevcRdUSszqQn.LP14LKq1	VALID	"Plus Package granted by Valid V6 license and Encoder Key."
Multistation 5	d2btq9eicFdmWUKNqazZzJLohv	VALID	
Multistation 2	dJbtqMeGcdDvlyokFKNytZvnu7 x	NOT VALID	
AESE7 Audio Enabling Key	abtmqEeBcdv2UzhZIGRK77C7Fk1	VALID	
Custom Message Pro	dcbTqdekKdGHdyTWmtp4Jmzhb31	VALID	
Extended Event Codes		NOT VALID	
Expansion GPIO	drbEqVeBxdn8KHjvYvY0V54fW1	VALID	"Expansion GPIO Hardware installed."
Network Expansion	dbwq9e4cNdpjg.PWY7logSQf	VALID	
Advanced Key Management		NOT VALID	
Textual Data Exchange (TDX)	dCbdqRegchK24NopnA3uh1rmhdc1	VALID	

To accept license changes: Restart System Reboot System Power Off System

Web Interface - Body Section

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

Footer

The **Footer** is a row of commonly used links at the bottom of the screen.

[Back Refresh](#) [Top Bot](#) [Stat:Srvr/](#) [GPIO](#) [OpLog](#) [SessionLog](#) [Audio:Out /In /Radios /MP](#) [Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP](#) [Alerts:Sent/ In/ Decd/ All](#) [RWT](#)
 Digital Alert Systems, Inc. All rights reserved. 2026

Web Screen - Footer Section

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

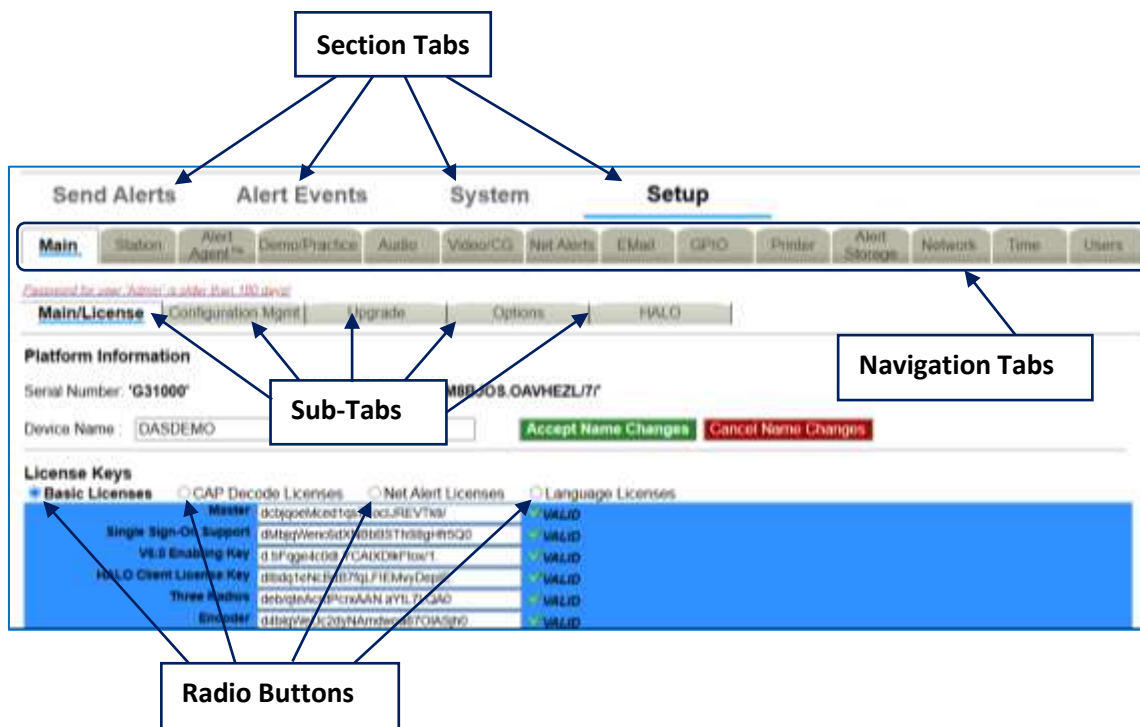
Navigation:

- **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.
- **Status**
 - **Stat:Srvr/** 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**
 - **Audio:Out** navigates to the **Setup > Audio > Audio Outputs** screen.
 - **/In** navigates to the **Setup > Audio > Audio Inputs** screen.
 - **/Radios** navigates to the **Setup > Audio > Audio Inputs** screen.
- **Set:**
 - **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 > Main GPIO** screen.
 - **/EASNET** navigates to the **Setup > Net Alerts > EAS NET** screen.
 - **/CAP** navigates to the **Setup > Net Alerts > CAP Decode** screen.
- **Alerts:**
 - **Alerts:Sent/** navigates to the **Alert Events > Originated Alerts** screen.
 - **In/** navigates to the **Alert Events > Active** 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 of, and monitor all activity. Radio buttons, check boxes, text fields, pull-down menus, and hyperlinks are found throughout the document.

The web interface uses a hierarchical organizational structure to navigate dozens of screens. The levels utilize section tabs, followed by navigation tabs, sub-tabs, and radio buttons where applicable.



Web Interface Navigation

The example shown is **Setup > Main > Main/License > Basic Licenses**.

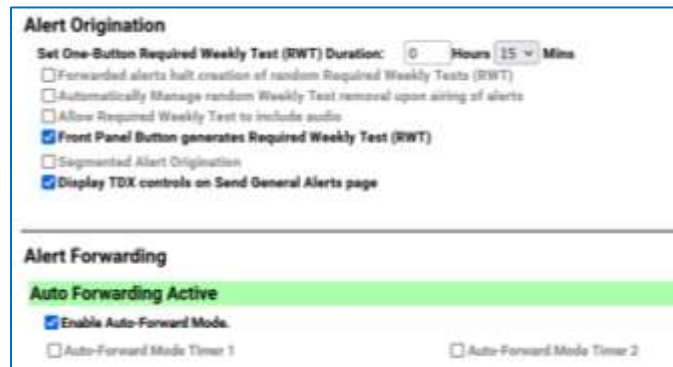
Throughout this manual there are references to menu structures, such as **Section Tabs > Navigation Tab > Sub-Tab > Radio Button** (for example, **Setup > Main > Main/License > Basic Licenses**).

To navigate:

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

Changes and Updates

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



Example Enabled/Disabled Check Boxes

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.

Accept Changes **Cancel Changes**

Pages with Accept Changes/Cancel Changes Buttons

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

Chapter 3: Setup Tab

The majority of all configuration settings are found in the Setup section. There are 14 sub-categories, accessed by clicking their individual navigation tabs.

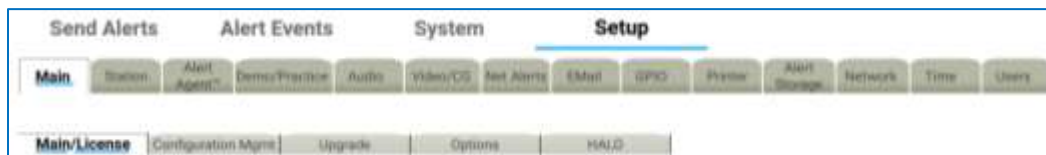


Setup Section Navigation Tabs

The categories are as follows:

Navigation Tab	Description
Main	License keys, saving/recalling configuration settings, upgrades, general system options, and HALO.
Station	Global and main 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 inputs/output levels/tests, optional radio tuner settings
Video/CG	Internal CG settings and serial port configuration
Net Alerts	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

Main Setup



Setup > Main Sub-Tabs

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

Sub-Tabs	Description
Main/License	Provides platform information.
Configuration Mgmt	Used to store, manage, and recall configuration backup files.
Upgrade	Used to quickly and conveniently upgrade software.
Options	Used 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.
HALO	Only visible with a HALO license key. HALO is an enterprise-level EAS management system developed by Digital Alert Systems to consolidate the monitoring and management of multiple EAS devices into a single user interface

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

There are two main sections on this screen: Platform Information and License Keys. Use this screen to set the Device Name and enable licensed features.

Send Alerts		Alert Events		System		Setup																																																																
Main	Station	Alert Agent™	Demo/Practice	Audio	Video/CG	Net Alerts	EMail	GPIO	Printer	Alert Storage	Network	Time	Users																																																									
Main/License Configuration Mgmt Upgrade Options HALO																																																																						
Platform Information Serial Number: '90321' Platform ID: 'FNVZBIYWAIJEP3HWJANGN' Device Name : WCPO DASDEC EAS Accept Name Changes Cancel Name Changes																																																																						
License Keys ☒ Basic Licenses ☐ CAP Decode Licenses ☐ Net Alert Licenses ☐ Language Licenses																																																																						
<table border="1"> <thead> <tr> <th>License Key</th> <th>Status</th> <th>Notes</th> </tr> </thead> <tbody> <tr> <td>Master</td> <td>VALID</td> <td></td> </tr> <tr> <td>Single Sign-On Support</td> <td>VALID</td> <td></td> </tr> <tr> <td>V6.0 Enabling Key</td> <td>VALID</td> <td></td> </tr> <tr> <td>HALO Client License Key</td> <td>VALID</td> <td></td> </tr> <tr> <td>Three Radios</td> <td>NOT VALID</td> <td>**No Radios available!**</td> </tr> <tr> <td>Encoder</td> <td>VALID</td> <td></td> </tr> <tr> <td>Video Out</td> <td>VALID</td> <td></td> </tr> <tr> <td>TV Features</td> <td>VALID</td> <td></td> </tr> <tr> <td>Plus Package</td> <td>VALID</td> <td>**Plus Package granted by Valid V6 license and Encoder Key.**</td> </tr> <tr> <td>Multistation 5</td> <td>VALID</td> <td></td> </tr> <tr> <td>Multistation 2</td> <td>VALID</td> <td></td> </tr> <tr> <td>AES67 Audio Enabling Key</td> <td>VALID</td> <td>**Not Available: AES67 Livewire not licensed!**</td> </tr> <tr> <td>Custom Message Pro</td> <td>VALID</td> <td></td> </tr> <tr> <td>Extended Event Codes</td> <td>NOT VALID</td> <td></td> </tr> <tr> <td>Expansion GPIO</td> <td>VALID</td> <td>**Not Available: Expansion GPIO Hardware NOT installed!**</td> </tr> <tr> <td>Network Expansion</td> <td>VALID</td> <td></td> </tr> <tr> <td>Advanced Key Management</td> <td>NOT VALID</td> <td></td> </tr> <tr> <td>Textual Data Exchange (TDX)</td> <td>VALID</td> <td></td> </tr> </tbody> </table>														License Key	Status	Notes	Master	VALID		Single Sign-On Support	VALID		V6.0 Enabling Key	VALID		HALO Client License Key	VALID		Three Radios	NOT VALID	**No Radios available!**	Encoder	VALID		Video Out	VALID		TV Features	VALID		Plus Package	VALID	**Plus Package granted by Valid V6 license and Encoder Key.**	Multistation 5	VALID		Multistation 2	VALID		AES67 Audio Enabling Key	VALID	**Not Available: AES67 Livewire not licensed!**	Custom Message Pro	VALID		Extended Event Codes	NOT VALID		Expansion GPIO	VALID	**Not Available: Expansion GPIO Hardware NOT installed!**	Network Expansion	VALID		Advanced Key Management	NOT VALID		Textual Data Exchange (TDX)	VALID	
License Key	Status	Notes																																																																				
Master	VALID																																																																					
Single Sign-On Support	VALID																																																																					
V6.0 Enabling Key	VALID																																																																					
HALO Client License Key	VALID																																																																					
Three Radios	NOT VALID	**No Radios available!**																																																																				
Encoder	VALID																																																																					
Video Out	VALID																																																																					
TV Features	VALID																																																																					
Plus Package	VALID	**Plus Package granted by Valid V6 license and Encoder Key.**																																																																				
Multistation 5	VALID																																																																					
Multistation 2	VALID																																																																					
AES67 Audio Enabling Key	VALID	**Not Available: AES67 Livewire not licensed!**																																																																				
Custom Message Pro	VALID																																																																					
Extended Event Codes	NOT VALID																																																																					
Expansion GPIO	VALID	**Not Available: Expansion GPIO Hardware NOT installed!**																																																																				
Network Expansion	VALID																																																																					
Advanced Key Management	NOT VALID																																																																					
Textual Data Exchange (TDX)	VALID																																																																					
To accept license changes: Restart System Reboot System? Power Off System?																																																																						
Back Refresh Top Bot Stat: Srvr/ GPIO OpLog SessionLog Audio: Out / In / Radios / MP Set: Net / Agent / Policy / Globals / GPIO / EASNET / CAP Alerts: Sent / In / Decd / All RWT																																																																						

Main/License Screen

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 6 software is also enabled with a valid license key. Most EAS devices are delivered pre-configured from the factory, so this task may already be complete. If the device is being upgraded to Version 6.0, this is the location for inputting that license key.

Platform Information

Serial Number

Each physical chassis is identified by a unique 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 right side of the back panel is a label that notes this identifier, the unit model number, and a QR code that can be used to register the device.

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.

Device Name

The Device 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*, *WMMM*, or *DASDEC3*. The Device Name can have spaces and is limited to 70 characters.

To change the Device Name, click in the Device Name text field, highlighting the existing text. Type the desired Device Name, up to 70 characters, including spaces. When done, click the **Accept Name Changes** button. To cancel any entry and revert to the current Device Name, click the **Cancel Name Changes** button.

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

License Keys

Available features are enabled by using a license key interface. These license keys have been organized into four categories, with corresponding radio buttons: **Basic Licenses**, **CAP Decode Licenses**, **Net Alert Licenses**, and **Language Licenses**. Descriptions of each license key contained in each category are provided in the License Key tables that follow.

License Keys			
☒ Basic Licenses	☐ CAP Decode Licenses	☐ Net Alert Licenses	☐ Language Licenses
Master	ZfvkviE6vVwoNmeTtpAX0o5sH7Q	✓	VALID
Single Sign-On Support	kjZQ2dWA3X1oXmnf5pmXxoD3hHd/	✓	VALID
V6.0 Enabling Key	38fIQ_ezjyMokmtfpxXtoaeFnO1	✓	VALID
HALO Client License Key	5HLn3wxOfbSoKmlfmpyXSo7osYK1	✓	VALID
Three Radios		✗	NOT VALID **No Radios available!**
Encoder	h5s3F2DyUuXmVt2pbXuo8aagG/	✓	VALID
Video Out	JsdNxGV6l1o5mTffpuXJow3yhw/	✓	VALID
TV Features	ta9jL/ahz1_owm4fOpEXtoW47Og1	✓	VALID
Plus Package	jxnmngAhDpCo/mAl2ptXMoFdDKN1	✓	VALID **Plus Package granted by Valid V6 license and Encoder Key.**
Multistation 5	W7fuAdXMSQ5oVmoIApAXHoNrWpU.	✓	VALID
Multistation 2	O7YVikEek4AoUmXf9p4Xjoz_8nc	✓	VALID
AES67 Audio Enabling Key	ttFHvYlb1KWJoJmNfKpdX4oSvSA7	✓	VALID **Not Available: AES67 LiveWire not licensed!**
Custom Message Pro	NEJcmS/Yr oRmAfwpxX8ooZDwq0	✓	VALID
Extended Event Codes		✗	NOT VALID
Expansion GPIO	JAoChaeTZdyoFmztlpXmoxuIKg1	✓	VALID **Not Available: Expansion GPIO Hardware NOT installed!**
Network Expansion	JYqaGNA0fbBoNm8ITpXWoiVWgl1	✓	VALID
Advanced Key Management		✗	NOT VALID
Textual Data Exchange (TDX)	KoQ0vHJ1RNfotmGf8p1XgolzoEq	✓	VALID

License Keys Interface

Note: Addition of AES67/LiveWire

License keys have three different colored labels:

- **Blue license box:** When a feature is correctly licensed with a valid key in the associated key's text field on the right, the license key display is blue. The word VALID is shown to the right of the text field
- **Gray license box:** When the key's text field is incorrect or blank, the feature's box will be gray. The words NOT VALID are shown to the right of the text field
- **Yellow license box:** For options that also require specific hardware, the key display is yellow

when the license key entry is valid but the video frame buffer is unavailable or the hardware is not installed. The word VALID to the right of the text field indicates the key is OK. A message states what hardware is not yet installed.

Note: If the Video Out license key field is yellow, connect the dongle (included with the original package) to the VGA port on the back of the DASDEC-III, then reboot the system (full power cycle).

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.

New license keys are typically sent via email and are easily copied and pasted into the corresponding 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 by clicking the **Restart System** 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 blue background and a VALID label.

Restart System?

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

Reboot System?

Is a full system reboot. A confirmation screen will immediately appear with the options to **Yes, Reboot System** or **No, Cancel System 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 users to log in.

Power Off System?

Powers down the EAS device. A confirmation screen will immediately appear with the options to **Yes, Power Off System** or **No, Cancel System 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.

Basic Licenses

This grouping of license keys includes core functionality and general software and hardware options. The following list of license keys is included in the **Basic Licenses** radio button.

License Keys		
☒ Basic Licenses	☐ CAP Decode Licenses	☐ Net Alert Licenses
☐ Language Licenses		
Master	ZfvkviE6vVwoNmeffpAX0o5sH7Q.	✓ VALID
Single Sign-On Support	kgZQ2dWA3X1oXmnf5pmXxoD3hHd/	✓ VALID
V6.0 Enabling Key	36fIQ.ezyjMokmtfvpXXtoaeFnO1	✓ VALID
HALO Client License Key	5HLn3wxOfbSoKmlfmpyXSo7osYK1	✓ VALID
Three Radios		✗ NOT VALID **No Radios available!**
Encoder	h5s3F2DyUJoXmVf2pbXuo8aagC/	✓ VALID
Video Out	JsdNxGV8l1o5mTffpuXLow3yhw/	✓ VALID
TV Features	ta9jL/ahz1.owm4fOpEXtoW47Og1	✓ VALID
Plus Package	pxnmngAhDpCo/mA2ptXMoFdDKN1	✓ VALID **Plus Package granted by Valid V6 license and Encoder Key.**
Multistation 5	W7fuAdXlMSO5oVmotApAXHoNrWpU.	✓ VALID
Multistation 2	O7YVtkEek4AoUmXf9p4Xjoz.8nc.	✓ VALID
AES67 Audio Enabling Key	ttFhVYLb1KWojmNfKpdX4oSvSA7	✓ VALID **Not Available: AES67 Livewire not licensed!**
Custom Message Pro	NEJJcmS/Yr oRmAfwpwX6ooZDwq0	✓ VALID
Extended Event Codes		✗ NOT VALID
Expansion GPIO	JAoChaeTzdyoFmzfplXmoxutKg1	✓ VALID **Not Available: Expansion GPIO Hardware NOT installed!**
Network Expansion	JYqaGNA0fbBoNm8TpfxWoivWgl1	✓ VALID
Advanced Key Management		✗ NOT VALID
Textual Data Exchange (TDX)	KoQ0vHJ1RNFotmOfbp1XgolzoEq.	✓ VALID

License Keys / Basic License Screen

License Key	Description
Master	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 > Main menu is limited to the Main/License sub-tab, where the Server Name , Master license key, and V6.0 Enabling Key are the only available text fields.
Single Sign-On Support	SSO. Provides device login access via a TACACS+ authentication server and OpenID Connect.
V6.0 Enabling Key	Necessary to operate the version 6 software and is preconfigured for each new device. A valid V6.0 Enabling key enables users to operate, configure, and access the permissions allowed by their user credentials. Without a valid V6.0 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.
HALO™ Client License Key	An enterprise-level EAS management system enabling users to monitor and manage multiple EAS devices within a single user interface. The HALO Client License Key (or HALO-CLK) is necessary for each EAS device to communicate and exchange files with the central HALO server.

Radio Enabling Key (Three Radios)	DASDEC-III Dual Tri-band 2-Radio receiver license. This option upgrades any DAS3-EL by enabling the two (2) internal radios. DASDEC-III Triple Tri-band 3-Radio receiver license. This option upgrades any DAS3-EX by enabling the three (3) internal radios. Each receiver allows any combination of AM, FM, or WX (NOAA) frequencies with band selection, tuning, and level controlled via the browser interface.
Encoder	Controls 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: • Plus Package • Custom Messaging • CAP Canada NAAD Decode • All EAS NET options • DVS644 (SCTE18) • MultiStation 5 • TDX • CAP Caribbean Decode • DVS168 Single Client • Streaming MPEG 1/2 & 1/2/4
DAS3-HDMIOUT (Video Out)	Enables the HDMI port for displaying emergency message details as HDMI video with embedded EAS audio when the necessary hardware is installed. Standard on the DAS3-GX model. Consult factory for more information.
TV Features	Unlocks support for television specific features, including specific serial port protocols, to support several external video display devices. Standard on all DASDEC-III models.
Plus Package	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. • Support for multiple serial port control using an external USB/4RS232 serial port expander. • FIPS/EAS filtering for selective serial port and GPIO's control under MultiStation option • Allows Auto-Forward Filters optional block Manual Forwarding. • Front panel audible announcement of decoded alerts. • Automatic browser refresh and instant display of incoming alerts on Alert Events page. • Custom text modification for ORG codes and CGs. • Custom message modification allows both text and audio message editing. • Allows Auto-Forward Filters to optionally block Manual Forwarding. • 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), Simple Chyron Intelligent IF, Compix™ NewsScroll, and Compix AutoCast character generators. • MP3 and OGG/Vorbis streaming audio of audio sources. • Supports Fox Splicer™ (Cisco DCM™) • Customizable hourly station ID/ Message display for R194 or XBOB4

	character generators
MultiStation™- 2 MultiStation™- 5	When the Plus Package license is enabled, an option is available for licensing the MultiStation mode. 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. FIPS/EAS filtering allows for selective serial port and GPIOs control. GPIOs can be set for each stream according to Station ID, FIPS, and/or Event Code. Provides sequential or simultaneous station payout and staggered payout with optional MultiPlayer™.
AES67/LiveWire Audio Enabling Key	Invokes livewire compatible devices to switch to and from the DASDEC digital audio stream during and after alerts, respectively.
Custom Message Pro™	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. Not recommended for use with MultiStation feature due to restricted functionality.
Extended Event Codes	Adds several non-EAS SAME codes.
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.
Network Expansion	Enables the Dual Port Gigabit Ethernet Expansion hardware option (DAS3-EX and DAS3-GX ONLY), creating controls for 3 unique Ethernet 10/100/1G network links.
TDX	Unlocks the EAS Textual Data Exchange (TDX) option, a Digital Alert Systems 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.

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 is included in the **CAP Decode Licenses** radio button.

The screenshot shows the 'Main/License' configuration screen. At the top, there are tabs for 'Main', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. Below these are sub-tabs for 'Main/License', 'Configuration Mgmt', 'Upgrade', 'Options', and 'HALO'. The 'Platform Information' section displays 'Serial Number: '90321'' and 'Platform ID: 'FNVZBIYWAIJEP3HWJANGN.''. The 'Device Name' is 'WCPO DASDEC EAS', with 'Accept Name Changes' and 'Cancel Name Changes' buttons. The 'License Keys' section has radio buttons for 'Basic Licenses', 'CAP Decode Licenses' (selected), 'Net Alert Licenses', and 'Language Licenses'. A table lists the following license keys:

License Key	Key	Status	Notes
CAP Standard	rD2tEQ/7P.JoUmItrp2XeoZpB9R.	VALID	**CAP Standard Decode granted by Valid CAP Plus key.**
CAP Plus	7aagw7BaRjcoQmjfUpqXaotaa9o/	VALID	
CAP Canada NAAD Decode	YbCymSiilj.o5mjfwpcXSo6Nbih0	VALID	
CAP Caribbean Decode	72zcBTS.7rLoXm7fJphXKowzv/VQ/	VALID	
Triveni Skyscraper	rINpPROBihuoKmBfdpaXgoHr9GW.	VALID	**Skyscraper Software is not installed!**
CAP IPAWS Server Emulation	UZ17iMz3Yuto.mWfNpqXtomWSed1	VALID	

License Keys / CAP Decode Screen

License Key	Description
CAP Standard	CAP software option for directly handling CAP v1.2 messages to ensure compliance with FEMA/ Integrated Public Alert & Warning System (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	Allows users to decode National Alert Aggregation & Dissemination System (NAAD System) alerts in Canada. Provides support for using https for CAP decode file download.
CAP Caribbean Decode	Processes CAP messages using profiles for national alerting systems of Anguilla, Montserrat, Sint Maarten, Barbados and subdivision alerts, and Aruba (English only).
Triveni™ Skyscraper	Datacast CAP receiver 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-III 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™, DVS168, DVS644, and MPEG streaming options.

License Keys		
☐ Basic Licenses	☐ CAP Decode Licenses	☒ Net Alert Licenses
EAS-NET™ (includes DVS168)	3-NwXoFguaXtZgTA6Y5KTLyxb1	VALID
EAS-NET™/CAP Send	v7f0d7oZgbay1GjW6WjJF9kFt	VALID
EAS-NET™/CAP Send to IPAWS Open	vcNtd1oigfaLPUAvmFaWqJAg	VALID
EAS-NET™/CAP Send PureCAP™	QGfudPolgzaifgseVHVEb2s2Fm6	VALID
EAS-NET™/CAP Send OmniLingual™	yT2dSo3ga5C0uBtBafHfKkQJ1	VALID ***Not Available: Requires Valid Multi Language key.**
EAS-NET™ Mediaroom	azf0dGonghLRVkaDy645ZIEo0	VALID
EAS-NET™ Minerva	rgfBdloUg1aYf2boc1NcPNA03H	VALID
EAS-NET™ Automation	m0Fv0Oomg4axem7qcJmD38Zm70	VALID
EAS-NET™ AEA	S-fedCovgpalh7JF8aqipQpOQ0	VALID
EAS-NET™ AEA+	DDfcdZooq1aCzrU56fzz0V6gR	VALID
DVS168 Single Client	qFwJd0wgRa6kSLKSp2zyVtux	VALID ***Multiclient EAS-NET version generated by Valid EAS-NET key.**
DVS644 (SCTE18)	V5f6dZooq2aefMtpwzVukbGgmKI	VALID
MPEG-DASH	vXf5dldodgaHfR1qozGzuGimbiV	VALID ***Not Available: No video out!***
Stream MPEG 1/2	F0fudNozga3f0gJVVU8aQUpCtZ x	NOT VALID ***Not Available: No video out!***
MPEG-DSD	k7Gdt0rg6aUqnaucE7fZ Q pz	VALID ***MPV 0. Software streaming***

License Keys / Net Alert Licenses Screen

The following list of Net Alert License keys is included in the Net Alert Licenses radio button.

License Key	Description
EAS NET™ (Includes DVS168)	A 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	Allows origination of CAP alert messages. This 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	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™ 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™	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	Unlocks EAS alert network forwarding via the Minerva EAS LAN protocol. This license key is a bundle that includes EAS-Net.
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. 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	Interface which 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. Works with models with DASENCS only.
DVS644 (SCTE 18)	Enables sending EAS data as an MPEG-2 Transport Stream over a TCP/IP network to up to sixty-four (64) DVS644(SCTE18) compatible platforms. Works with models 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 2 streaming video/audio. A license key is provided when special MPEG 2 encoder software is purchased.
MPEG-D2D	This license key option unlocks the D2D interface enabling specialized interfacing with D2D Technologies products. Must be secured through D2D at 904-323-4777 (DASDEC-IIIs only).

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 the license keys available for licensing, with a number of additional premium TTS voices available. Please contact Digital Alert Systems for a list of all available premium TTS voices.

License Keys
☐ Basic Licenses ☐ CAP Decode Licenses ☐ Net Alert Licenses ☒ **Language Licenses**

OmniLingual™ Enable Key PeKolJd5RuJovmofZpZXjoTGUAf1 VALID

Voice	Licensed Name	Licensed Company	License Key
William (US English)			
David (US English)			

To accept license changes: Restart System Reboot System? Power Off System?

License Keys / Language Licenses Screen

License Key	Description
OmniLingual™ Enable Key	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.
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.
Millie	Premium Text-To-Speech Millie (UK English-Female) license key.
Miguel	Premium Text-To-Speech Miguel (Americas Spanish – Male) license key.
Charlie-Hmong	Premium Text-To-Speech (TTS) Charlie (Hmong – Male) license key.
Dallas-Somali	Premium Text-To-Speech (TTS) Dallas (Somalis – Male) license key.

Editing Premium Text-To-Speech Voices

Premium Text-To-Speech Voice License Keys are found within the **Language Licenses** radio button. When a Premium Voice is purchased and properly licensed, that license key's box will turn blue 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, as well as 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 “wind” 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.

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 as well. 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.

New Word Definition 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 field and enter the desired **Pronunciation** into the corresponding text field. 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.

Show Phoneme Rules Chart Check Box

This list of phonemes are the only letter combinations the TTS engine will recognize. Notice all vowel phonemes are immediately followed by 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.

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. 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.

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.

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.

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 to 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.

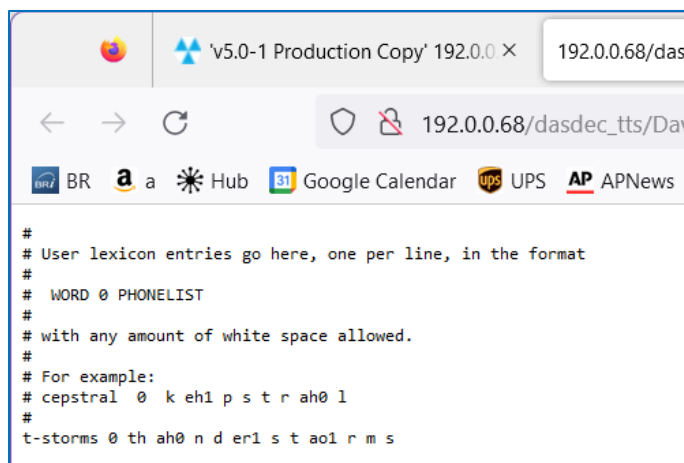
[Make TTS Sample](#)

Tue Oct 29 17:37:26 2013: [View/Download the current saved lexicon file for Allison.](#)

Upload a Lexicon file at the bottom of this page.

View/Download the current saved lexicon file Hyperlink

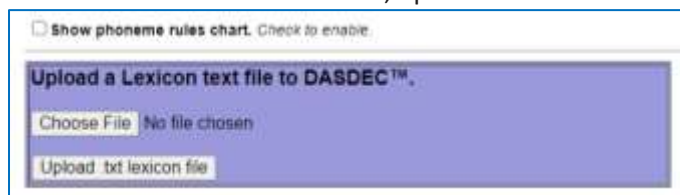
You will be presented with a .txt (text) file within the web browser. Use the **Save As...** or **Save Page As...** option found in the **File** pull-down menu of the web browser to save this file. Save the file to a local hard drive, not on the EAS device. The date to the left of the **View/Download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



Lexicon Table Text File

To upload a Lexicon Table text file:

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



Upload a Lexicon Text File Section

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.

Configuration Management

The **Setup > Main > 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 from this screen as well. 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, or license keys. Sound level, email recipients, and HALO settings are stored when a configuration backup file is created and are optionally restorable.

The screenshot shows the 'Configuration Mgmt' screen within the 'Setup' tab. At the top, there are navigation tabs: 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs: 'Main', 'System', 'Alert Events', 'Demo/Practice', 'Audio', 'Video/CG', 'Set Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. The 'Main' sub-tab is active, showing 'Configuration Mgmt' as the selected option. Below the navigation, there are buttons for 'Main/Content', 'Configuration Mgmt', 'Upgrade', 'Options', and 'HALO'. The main content area is titled 'Current and Previous Configuration' and includes a green 'Create Configuration Backup' button. It shows a 'Loaded configuration (Wed Sep 9 09:17:26 2026) : reinstalled a previous config' and a 'Previous configuration (Wed Sep 9 09:17:25 2026) : Restore Previous Configuration...' button with a warning icon. Below this, there is a 'Configurations' section with a 'Select Configuration' dropdown menu showing '2026_06_25_01_35_30_dasdecv6_config.zip', a 'Rename (no spaces)' text field with the same filename, and an 'Accept' button. There is also an 'Install Config' button with a warning icon and a checkbox for 'Force install'. An 'Include' section has checkboxes for 'Audio Levels/Input Sources', 'Email recipients', and 'HALO settings'. An 'Install Log' button is also present. At the bottom, there is an 'Upload DASDEC™ Server Configuration' section with a 'Choose File' button (showing 'No file chosen') and an 'Upload' button.

Configuration Management Screen

When the EAS device is configured for the first time, and before a backup configuration file is made, the page displays: ***Loaded configuration not available*** and ***No previous configuration***. Always 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 **Create Configuration Backup** button. After the first backup file is made, a pull-down list titled **Select Configuration** appears and the new file name appears in this list. All other standard configuration management options appear, such as a **Rename** text field and **Accept** button, a **Download** button, a **Delete File** button, an **Install Config** button and check boxes, and an **Install Log** button.

A ***Loaded configuration not available message*** is displayed on new devices when no configuration has been saved or uploaded.

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 restoring/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 is precautionary in the rare event that an upgrade corrupts an existing configuration. It can be used to attempt to restore settings to the pre-update state.

The **Restore 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 displayed.

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 return easily and quickly 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.

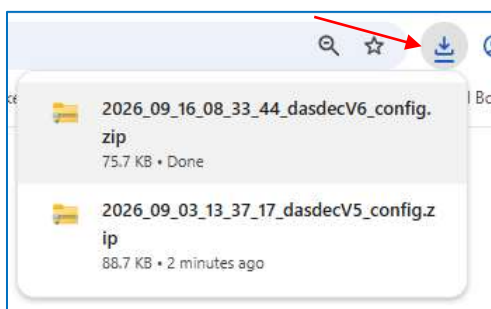
The **Select Configuration** pull-down menu displays the most recent backup configuration files. Use the pull-down menu to view and select a file. To add a file from a system, use the **Upload DASDEC Server Configuration** section found at the bottom of this screen.

To download a configuration file to the local host computer (not the EAS device), use the **Select Configuration** pull-down menu and select the appropriate file, which will display as a link. In the screenshot below, the file is **2026_09_03_13_37_17_dasdecV6_config.zip**. Each Configuration Backup File will default to a similar name, based on date/time. Click on the download icon to download the configuration back up.



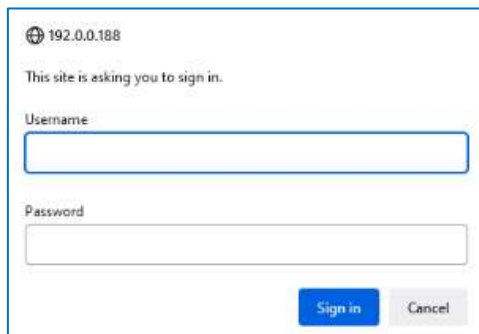
Configuration Mgmt - Configurations Screen

Once the download is complete, click on the download symbol on your browser and click in the file folder to save the file to your host computer. **Do not unzip the file.**



Save Downloaded Configuration 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.

A web-based authentication prompt dialog box. At the top, it shows a globe icon and the IP address '192.0.0.188'. Below this, it says 'This site is asking you to sign in.' There are two input fields: 'Username' and 'Password'. At the bottom right, there are two buttons: 'Sign in' (blue) and 'Cancel' (grey).

Authentication Prompt

Often the default configuration backup file name is not desirable. To rename the configuration file, type a new name in the **Rename (no spaces)** text field below the **Select Configuration** pull-down menu and click the **Accept** button. Do not use spaces or punctuation characters. Dashes, underscores, and dots are allowed.

The **Install Config** button installs the currently selected configuration file selected in the **Select Configuration** pull-down menu. The date of the selected file is displayed above the **Accept** button. Installation will restart the server software.

A screenshot of the 'Configurations' interface. It features a 'Select Configuration' dropdown menu showing '2026_09_03_13_37_17_dasdecv5_config.zip'. Below it is a 'Rename (no spaces):' text field with the same filename. To the right, the date 'Tue Sep 15 13:32:21 2026' is displayed above a green 'Accept' button. At the bottom left is an 'Install Config' button with a warning icon. In the center, there is an 'Include:' section with three checkboxes: 'Audio Levels/Input Sources', 'Email recipients', and 'HALO settings'. At the bottom right is an 'Install Log' button.

Configurations Interface Screen

A complete backup file includes all the audio settings, any email 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**

Email recipients (found on the **EMail** navigation tab screen) include:

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

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

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

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**.

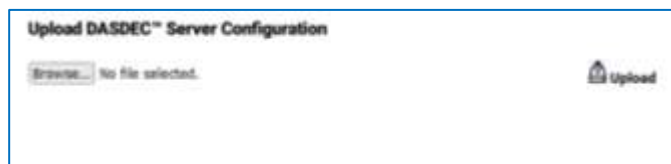


Install Configuration Confirmation Screen

Delete a selected configuration file found in the **Select Configuration** pull-down menu by clicking the **Delete** icon.

Note: There is NO confirmation opportunity and the deletion is instantaneous.

The **Upload DASDEC Server Configuration** section, located at the bottom of the screen, provides an interface to upload a configuration file from a file system accessible to the local web browser host computer. Click the **Browse...** button, then locate and select the desired configuration file. Click the **Upload** button. Once uploaded, the file appears in the **Select Configuration** pull-down menu, where it can be managed as described above (renamed, installed, deleted, etc.).



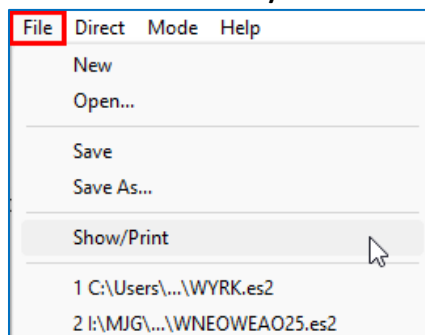
Upload DASDEC Server Configuration Section

Attention: The process of uploading a server configuration 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 **Select Configuration** pull-down menu and installed by clicking the **Install Config** button.

Sage

The system supports importing **SAGE ES2** Third-party software configurations into the DASDEC.

1. Open the desired .es2 file and select **File > Show/Print**.



ES2 File screen

2. Click on **Copy** to copy the text to the clipboard.



Show Settings Screen

- Open a blank .txt file and **Paste** the copied text into the blank file.
- Save** the new .txt file.
- In the DASDEC, navigate to **Setup > Main > Configuration Mgmt.**
- Select the **Choose File** button to select the recently saved .txt file.
- Once the .txt file is selected, click the **Upload** button to generate a configuration file based on what was saved in the .txt file.
- The configuration file will have **dasdecES2** in the name, instead of the standard dasdecV6.

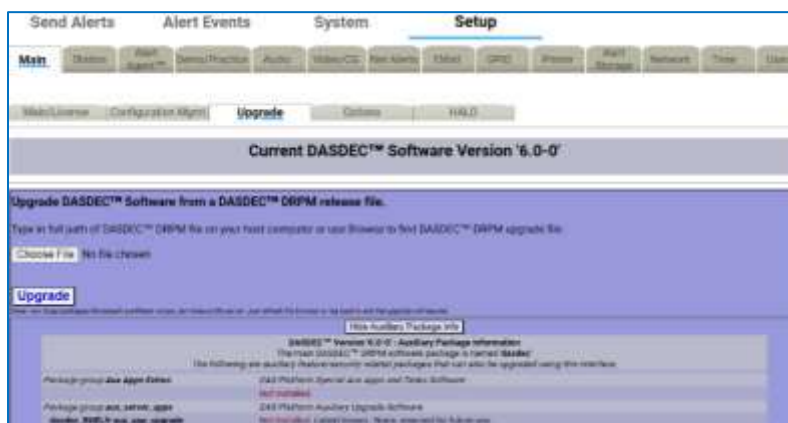


Configurations screen

Note: The uploaded configuration file does not include all of the settings from the ES2 file, so some manual editing will need to be done by the user.

Upgrade

Software can be quickly and conveniently upgraded by going to the **Setup > Main > 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' customer service via email at support@digitalalertsistemas.com or by calling 585-765-2254.

Software upgrade instructions and the enabling key will be delivered via email. To install the upgrade, read through the entire email before starting, then follow the step-by-step instructions in the email.

Options

The **Setup > Main > 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.

The screenshot displays the 'Options' configuration screen. At the top, there's a navigation bar with 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', a row of buttons includes 'Main', 'Station', 'Alert Agent', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'EMail', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. Below this, another row of buttons shows 'Main/License', 'Configuration Mgmt', 'Upgrade', 'Options' (which is highlighted), and 'HALO'. The main content area contains the following settings:

- ☐ **Debug Log Interface.** *Disabled. Check to enable. Change effective immediately!*
- Select Text Encoding Option. Change Effective Immediately!**
 - ☐ Windows 1252
 - ☒ UTF-8
- CAP output encoding is always UTF-8.**
- EAS NET output encoding is set to system encoding or UTF-8 if single byte output is forced below.**
- Single byte encoding approximates accented and other special characters with standard Latin characters.*
- ☒ **Force Single Byte UTF-8 encoding for CAP and EAS NET.** *Enabled. Change Effective Immediately!*
- ☐ **Monroe 988 Clock Sync Support.** *Disabled. Check to enable; then restart platform software after plugging in 988 USB cable.*
- [Link to page with restart buttons.](#)
- [Link to 988 USB Status page.](#)
- ☐ **Override default IP address when using CAP IPAWS Server Emulation.** *Disabled. Check to enable and enter DNS hostname.*

Setup > Main > Options Screen

The **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 the **Debug Log Interface** is enabled, those changes are immediate and a hyperlink titled **Link to Debug Log pages** is made visible and navigates to the **System > Debuglogs** screen. This screen contains the following sub-tabs: **Decoder**, **Main Server**, **Serial**, **Audio**, **Video**, **Network**, and **Web Server**.



Debug Log Screen

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 debugging is no longer needed, uncheck the **Debug Log Interface** check box.

Select Text Encoding Option

The 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, including foreign characters.

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 EAS equipment, this setting can be left unchecked.

The Digital Alert Systems/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. 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 > Main > Main/License** screen where a **Restart System** 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

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

HALO Configuration Screen

The HALO sub-tab is available when a valid **HALO Client License 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 Sent to HALO**, and **Automatic HALO Updates**.

HALO Connection

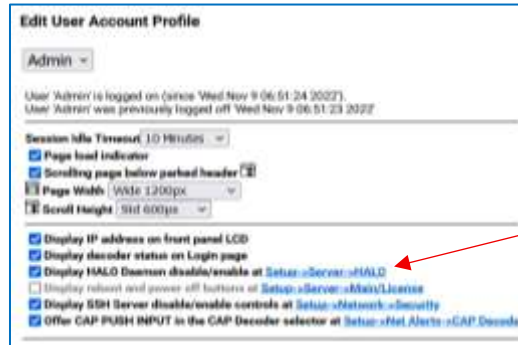
This top-most section of the screen is focused on settings necessary to connect this device to the HALO server.

Enable HALO Connection

Checking the **Enable HALO Connection** check box either enables or disables 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 settings may be configured. The checkbox may not be visible. The Admin user determines whether to display or not to display this check box to all users.

Setup > Main > HALO Enabled Screen

Admin users can navigate to the **Setup > Users** screen. There are several display options visible including **Display HALO Daemon disable/enable** at **Setup > Main > HALO** page. Checking (enable) this check box will display the check box on the **Setup > Main > HALO** screen for all users. Unchecking (disable) this check box will not display this same check box.



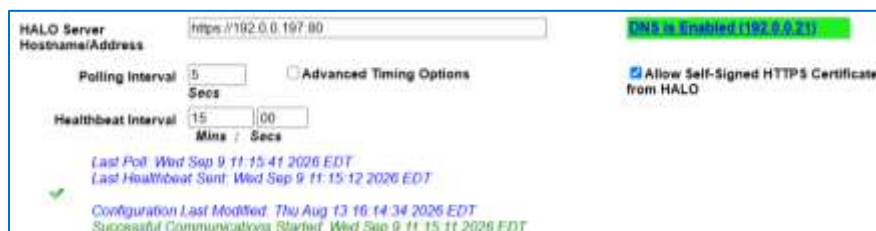
Display HALO Daemon disable/enable

Within the **Setup > Main > HALO** screen the system displays whether the HALO Daemon connection is Enabled or not, and whether the HALO Daemon is running or not. There is a button to Restart HALO Daemon. This check box enables an Administration Level user to remove those buttons for all users. This setting is only available for Administration Level users.

The HALO Daemon is an Auxiliary Package charged with the task of managing the connection to the HALO server. This package must be in the **Running** state with a HALO connection. The current HALO Daemon Status is displayed below the **Enable HALO Connection** check box. A green check mark will be displayed to the left of the **HALO Daemon is Running** status.

Restart HALO Daemon

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



HALO Server Hostname/Address Screen

HALO Server Hostname/Address

Use the **HALO Server Hostname/Address** text box to enter either the 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 screenshot, the URL is 'https://192.0.0.197:80' - where the

'https://' denotes a secure connection, '192.0.0.197' 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) the **Allow Self-Signed HTTPS Certificate from HALO** check box on the right side of the interface. 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 the **Polling Interval**. Use the text box to enter a value ranging 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. The **Healthbeat Interval** is pre-set to 15 minutes and can be changed by the user in the provided **Mins** and **Secs** text fields.

Below the **Healthbeat Interval** setting on the interface screen is a log that lists the date and time of the most recent Poll, Healthbeat sent, Configuration sent, and Configuration Modification.

Advanced Timing Options

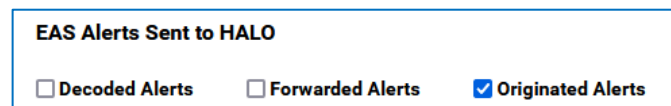
Checking (enabling) the **Advanced Timing Options** checkbox allows the user to set the **Connection request timeout** and the **Maximum response time**.

A screenshot of the 'Polling Interval Settings' interface. It features a 'Polling Interval' text box with the value '5' and a 'Secs' label below it. To the right is a checked checkbox for 'Advanced Timing Options'. Below this checkbox are two more text boxes: 'Connection request timeout' with the value '10' and 'Maximum response time' with the value '11'. Both of these have labels below them indicating ranges and defaults: '(3 - 30 seconds) (Default: 3)' for the first and '(6 - 60 seconds) (Default: 10)' for the second.

Polling Interval Settings

EAS Alerts Sent to HALO

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 are decided in this section of the screen.

A screenshot of the 'EAS Alerts Sent to HALO' interface. It shows three checkboxes: 'Decoded Alerts' (unchecked), 'Forwarded Alerts' (unchecked), and 'Originated Alerts' (checked).

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 **to be sent** to the HALO server. Uncheck the boxes for those event types **not to be sent** the HALO server.

Automatic HALO Updates

A 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.



The screenshot shows a configuration window for HALO updates. At the top, there is a checkbox labeled 'Automatic HALO Updates' which is checked. Below it, the text 'Configuration Update Time:' is followed by two numeric input fields: the first is '0' and the second is '00'. Below these fields, the labels 'Hrs' and 'Mins' are visible. At the bottom of the window, there are two buttons: 'Accept Changes' (green) and 'Cancel Changes' (red).

HALO Sub-Tab - EAS Alerts Section

Configuration Update Time

The two **Configuration Update Time** 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.

Network Setup

There are four sub-tab categories within the **Setup > Network** screen. 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.

Sub-Tab	Description
Configuration	This screen displays the current network state and provides controls to configure the Network Hostname, Network Ethernet IP Addresses, Gateway, and Static Routes.
Security	This page provides security controls for Web Interface Security, Web Interface SSL SSHD Certificate, Incoming Secure Shell Connection, SSHD Whitelist Configuration, and EASNET/CAP push SSH Peer Key Management Interface.
Proxy	The server can be optionally configured to access remote HTTP and/or HTTPS data (for CAP data) via a defined proxy server address and can be optionally configured to use HTTP proxy server for Open ID Connect (OIDC).
AWS S3	The server can optionally be configured to enable AWS S3.

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.

Configuration

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

Setup > Network > Configuration Screen (top half)

DASDEC-III EAS device models include one network interface (or NIC) standard and 2 additional NICs are optional. 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. An optional USB-1NICGIG dongle can provide a second NIC for model DAS3-EL or a fourth NIC in other models.

The current IP address is displayed just above the entry field for the **Network Hostname**. Other important network configuration info is displayed on the bottom half of the page.

Network Hostname

The **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 name can also be very important for the correct functioning of email. Some email 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 **Network Hostname** into the 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, 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 Network Interface
- 2nd Network Interface

Radio buttons for additional Network Interfaces will be present if enabled.

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 as green in the screenshot below) 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.

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. Additional configuration text fields will appear.
2. Enter the desired IP address into the **IP Address of Primary Nameserver**.
3. Enter the desired IP address into the **IP Address of Secondary Nameserver**.
 - If available, enter the **DNS Domain name (optional)**.
 - If available, enter the **DNS Search name (optional)**.

Network Interface Configuration – Use DNS Enabled

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.

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.

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.

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 text field. Either a 1 or 2 value may be entered.

Test Name

This text 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.

Successful DNS Test

For DHCP:

1. Select the **Automatic (via DHCP)** radio button.
2. Check the **Use Static Gateway IP Address for DHCP** box on the left side of the interface. The address of the gateway server will be displayed in the **IP Address of Gateway** text field.
3. Click on the **Accept Changes/Restart Network** button at the bottom of the screen.
4. Log in again under the new IP address.

Network Interface Configuration – Automatic via DHCP Network

A second, third, and fourth network interface may be enabled by checking the corresponding Network Interface check boxes found just below the Main Network Interface. Follow the above procedure for configuring the additional NICs.

The Network Interface box has three different color statuses:

- **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:** 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.

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:

```

current IP routing table
Destination      Gateway         Genmask         Flags metric ref  use iface
0.0.0.0          192.0.0.1       0.0.0.0         U        0    0    0  eth0
10.0.0.0         0.0.0.0         255.255.255.0   U        0    0    0  eth0
10.1.0.0         0.0.0.0         255.255.255.0   U        0    0    0  eth1
100.250.0.0      0.0.0.0         255.255.0.0     U        0    0    0  eth0
100.250.0.0      0.0.0.0         255.255.0.0     U        0    0    0  eth1
100.250.0.0      0.0.0.0         255.255.0.0     U        0    0    0  eth2
252.0.0.0        0.0.0.0         255.255.255.0   U        0    0    0  eth0

```

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

```

#cat: net 10.0.0.0 netmask 255.0.0.0  eth0
#cat: 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

Static Route 2: ☐ Enable

IP Address

Netmask

Gateway

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: flags=4096<UP,BROADCAST> mtu 1500
    link/ether 08:00:27:00:00:00 netmask 255.255.255.0 broadcast 192.168.0.255
    inet 192.168.0.1 netmask 255.255.0.0 prefixlen 24 scopeid 0x20
    ether 08:00:27:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 1000000 RX bytes 1000000000 (953.6 MiB)

```

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.

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

Static Route 2: ☐ Enable

IP Address

Netmask

Gateway

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'.

Static Route Configuration Interface

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 from the **Device** 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.

Static Route Configuration Interface – Device Menu

To disable a static route:

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

Note: A conflicting route can block network connectivity.

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.

Remote Rsyslog Configuration Interface

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.

The remaining sections on the Network Configuration page display current configuration and settings status of the Network Configuration, DNS config, Network Hosts, Main Device, and enabled NICs.

Security

This page provides controls for managing and configuring network security. The following security elements are:

- **Web Interface Security** - Switching web access between secure mode (HTTPS) and/or regular mode (HTTP).
- **Web Interface SSL (HTTPS) Certificate** – Use the pull-down menu to select the certificate.
- **Incoming Secure Shell Connection (SSHD)** – Use to enable or disable an SSHD connection.
- **SSD Whitelist Configuration** – Use to enable or disable a remote host.
- **EASNET/CAP push SSH Key Management Interface** – Used to allow regen of the outgoing EASNET/CAP SSH connection keys.
- **Reset outgoing EASNET/CAP on SSH Keys on Local and authorize on each peer** – Use the pull-down menu to select the SSH Key Type.
- **Incoming SSHD Connection Authorized Public Keys Management** – Used to allow direct login authentication on this platform from remote platforms holding the matching private key.

Network Security Screen top section

Web Interface Security

Use the **Web Interface Security** check box to force HTTPS SSL-based communication to the internal web server.

Check To Only Allow HTTPS Secured Web Access to this platform. Effective immediately!

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.

If the box is unchecked:

- Enables both HTTP and HTTPS. The change is immediate.

Enhanced HTTPS SSL Strength. Effective Immediately!

This option changes the https and web browser connection. If checked, this selection will end your current session.

Web Interface SSL (HTTPS) Certificate pull-down menu

- Default

Upload PEM format certificate file and private key pair:

- .crt file: **Click on Browse to select a file**
- .key file: **Click on Browse to select a file.**
- Click on the **Upload** button to upload the change.

Enforce constant remote IP address connection throughout user session. **Enabled.** Effective immediately! Change forces new login.

CAREFUL! Only Disable to operate behind a Web server load balancer. This option provides extra security!

Incoming Secure Shell Connection (SSHD)

SSHD (Daemon) Server provides 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.

Incoming Secure Shell connection (SSHD) is **NOT Enabled**

☐ Check to enable SSHD. Effective immediately!

IMPORTANT: SSHD is required for EAS NET receive and CAP push receive!

NOTE: When SSHD is enabled, it is configured to ALLOW remote access by password authentication (including root).

Password authentication not needed for EAS NET receive/CAP push receive, which requires public key authorization on receiving platform. See below.

SSHD Status Section – NOT Enabled

Incoming Secure Shell connection (SSHD) is **Enabled**

☒ Check to enable SSHD. Effective immediately!

IMPORTANT: SSHD is required for EAS NET receive and CAP push receive!

SSHD configured to ALLOW remote access by password authentication (including root).

☒ **SSHD password authentication? Enabled. Uncheck to stop all remote SSH access by user password authentication. Effective immediately!**

Password authentication not needed for EAS NET receive/CAP push receive, which requires public key authorization on receiving platform. See below.

SSHD enhanced security. Effective Immediately!

Disabled - Legacy compatibility only ▼

Disabled: NOT RECOMMENDED. Only use this setting as the last option for remote SSH connections from legacy devices.

SSHD Status Section – Enabled

To enable the SSHD:

1. Utilizing the **Check to enable SSHD** check box will start the SSH Server Daemon and will change the status of this feature to **Enabled** from **NOT Enabled**. An additional check box will also become available
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 **Security** screen.

Edit User Account Profile Interface

SSHD configured to ALLOW remote access by password authentication (including root)

The **SSHD password authentication?** check box enables remote access by password authentication. Click this check box to enable remote access by password authentication to go into effect immediately.

SSHD enhanced security. Effective immediately!

This pull-down menu provides enhanced security levels. The setting **Disabled** is **NOT RECOMMENDED** only use this setting as the last option for remote SSHD connections from legacy devices.

SSHD Enhanced Security – Pull-Down Menu Expanded

Note: **Maximum – V5 only SSH client support** is the recommended setting for V5+ system interoperability. However, if this breaks the remote the EAS_NET/SSH connections, then select **Strong – V5/other SSH client support**.

SSHD Whitelist Configuration

SSHD Whitelist Configuration is used to designate a Remote Host. Only allow specific remote hosts SSH connection access.

SSHD Whitelist Configuration

Only allow specific remote hosts SSH connection access. Enter 1 or more IP addresses.

☒ **Enable** ☐ **No defined remote hosts.**

Add Remote Host

Add a numeric IPV4 address (eg 10.1.23.201), IPV4 CIDR (eg 10.1.0.8/29), partial IP (eg 10.1.) or wildcard * or ? in last octet (eg 10.1.23.2* -> 10.1.23.2, 10.1.23.20 to 29, 10.1.23.200 to 255 or 10.1.23.1? -> 10.2.1.23.10 to 19)

EASNET/CAP push SSH Peer Key Management Interface

This local platform allows regen of the outgoing EASNET/CAP SSH connection keys. Simultaneously, a defined group of remote peer hosts (offering currently active EASNET/CAP daadec_netin SSH connections from this platform) can authorize connection from the new public key.

NOTE: If other DASDEC units share one public key with the peer, then set the Preserve Existing Public Key option on each peer target during key regeneration. After regeneration, remove the outdated public key directly on each remote host peer.

Key reset should be performed initially and then periodically. **CAREFUL:** Local only SSH reset without peer authorization will break any existing SSH peer connection!

Add remote peer SSH host

No remote SSH peer host targets have been created.

RSA SSH Key Type

Reset outgoing EASNET/CAP SSH Keys on Local and authorize on each peer

SSHD Whitelist Configuration

To allow access to a specific remote host:

1. Click **Enable**.
2. Click the **Add Remote Host** button.
3. Enter a full numeric IPV4 address, such as 10.1.23.201 or hostname, such as mysshclient.com or matching pattern with a wild card such as 10.1 or 10.1* (where * is the wildcard).

EASNET/CAP push 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 peer SSH Host, click the **Add remote peer SSH host** button each time to add a Remote peer SSH Host. 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.

EASNET/CAP push SSH Peer Key Management Interface Screen

Warning: DO NOT MODIFY an SSH Key without consulting with Digital Alert Systems.

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).

Change the following:

- **Interface Name**
- **Remote Peer EASNET.CAP SSH Host IP Address**
- **Preserve Existing Public Key authorization of this local DASDEC on this remote peer host.**

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)

Click the:

- **Accept changes to peer interfaces** button for changes to go into effect.
- **Cancel changes to peer 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. Results might take a few seconds.

Accept changes or Cancel changes to group interfaces.

SSH Key Type pull-down menu:

- DSA
- ECDSA
- RSA

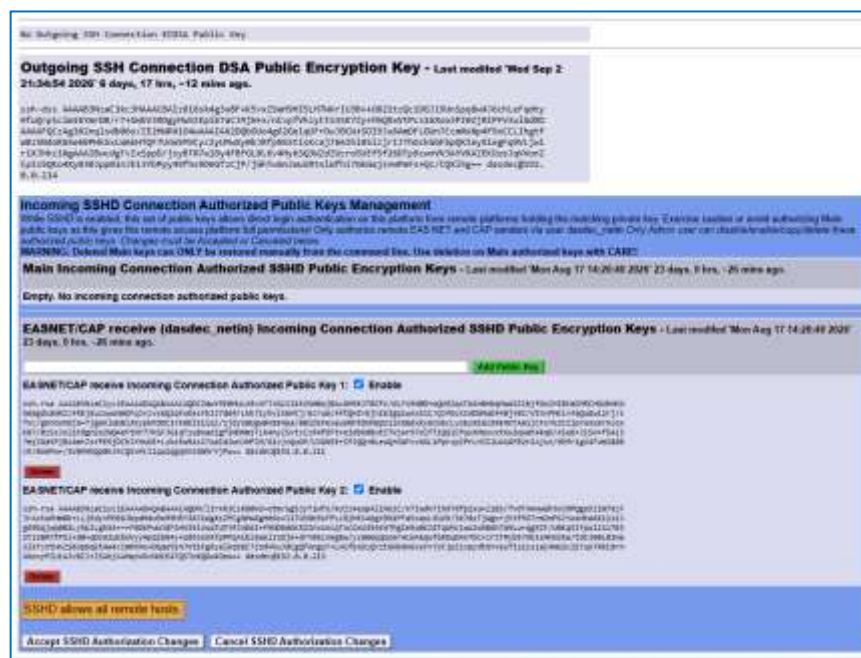
Check Boxes

- **Generate a different key per SSH device**
- **Preserve existing local platform incoming authorizations**
- **Make SSH group authorizations global**

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 **Reset 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 **Reset 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.

The Reset Outgoing EASNET/CAP SSH Keys on Local and authorize each peer. Only click on this button to reset the SSH key after changing the SSH Key Type.



SSH Authorization Section

Outgoing SSH Connection DSA Public Encryption Key

Provides Outgoing SSH Connection Public Encryption Key information and installed or last modified date.

Incoming SSHD Connection Authorized Public Keys Management

The **Incoming SSHD Connection Authorized Public Key Management** section (blue section found at the bottom of the **Network > Security** 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.

Main Incoming Connection Authorized SSHD Public Encryption Keys

Provides the installation and/or latest modified date and time.

A printout of the “authorized keys” file, which shows remote hosts authorized for SSH connections to this EAS device.

EASNET/CAP receive (dasdec_netin) Incoming Connection Authorized SSHD Public Encryption Keys

1. Use the Text box to add a Public Key.
2. Click the **Add Public Key** button to enable the change.
3. Click **Accept SSHD Authorization Changes** to save the key

Note: The latest SSH security protocol and open SSL-based communication, are not compatible with EAS-NET on DASDEC/ONE-NET units running V4.4 or lower.

EASENET/CAP Receive Incoming Connection Authorized Public Key 1

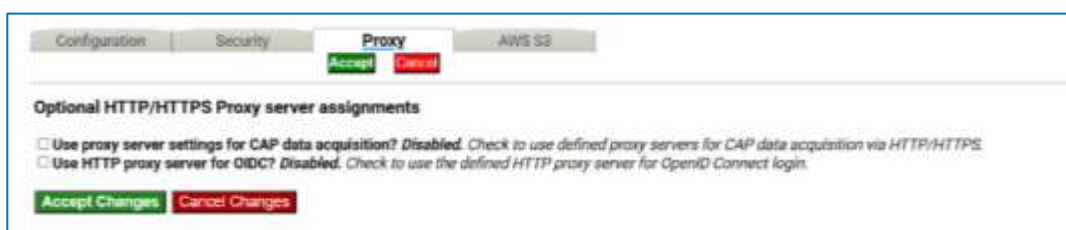
The **Enable** check box is normally checked, which enables this key for use. By unchecking this check box, that key will not be used and communication with that device or group of devices will be discontinued. Only enabled keys are utilized.

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

Proxy

Optional HTTP/HTTPS Proxy server assignments

The server can be optionally configured to access remote HTTP and/or HTTPS data (for CAP data) via a defined proxy server address and can be optionally configured to use HTTP proxy server for OIDC. Enable these options if defined proxy servers for CAP data acquisition are to be used.



Proxy Sub-Tab Screen

To configure a proxy server with the EAS device:

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

To configure an HTTP proxy server for OIDC:

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

AWS S3

Optional Amazon Web Services (AWS) S3 Filesystem for DASH MPEG

The server can optionally be configured to enable AWS S3 with a valid AWS S3 license.

To enable AWS S3:

1. Click on **Setup > Network > AWS S3**.
2. Click the **Enable S3** checkbox to enable S3.

3. Click on the **Selected Bucket** pull-down menu to select: Bucket 1, Bucket 2, or Bucket 3.
4. Enter the server name in the **Access Key** text field.
5. Click on the **Subfolder** to display the access status of the user.
6. Click on **Accept Changes** or **Cancel Changes** depending on whether the user wants to save or cancel the changes.

The screenshot displays the 'AWS S3' sub-tab within the 'Setup' section of the software. The top navigation bar includes tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs for 'Main', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network' (selected), 'Time', and 'Users'. Below these, there are further sub-tabs for 'Configuration', 'Security', 'Proxy', and 'AWS S3'. The 'AWS S3' sub-tab contains a section titled 'Optional AWS S3 Filesystem for DASH MPEG' with a checked 'Enable S3' checkbox and a red warning message 'S3 FS is NOT running!'. Below this is a 'Selected Bucket' dropdown menu currently set to 'Bucket_1'. There are three rows of input fields for 'Bucket Name', 'Access Key', and 'Subfolder' for Bucket 1, Bucket 2, and Bucket 3. At the bottom of the sub-tab are 'Accept Changes' and 'Cancel Changes' buttons.

AWS S3 Sub-Tab Screen

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 the following sections that are used to configure the settings: Date and Time, Time zone, Broadcast Week, and Network Time Protocol (NTP).

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.

Date and Time Screen

Date and Time

The **Date and Time** section provides three important functions: It displays the current time, provides a means to manually set the time, and establishes 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.

A 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).

Network Time Protocol (NTP)

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.

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 the name or IP address of a remote NTP server that is readily accessible from the EAS device in the **NTP Server name or IP Address** text field.
3. Check the **Check this 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 Name or IP Address (restart NTP to submit changes)

NTP Server Info is located in a gray shaded area below the NTP settings. This is an informational display area that provides information 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 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.

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

Users Setup

The **Setup > Users** screen is used to manage user accounts within the EAS device. Each EAS device comes configured with a single Admin user account. 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 **Setup > Users** screen is divided into two sections: **Edit User Account Profile** and **Add New User Account**.

Note: In the event of an account suspension, it will be displayed on this screen.

Send Alerts **Alert Events** **System** **Setup**

Main Station Alert Agent™ Demo/Practice Audio Video/CG Net Alerts Email GPIO Printer Alert Storage Network Time **Users**

Edit User Account Profile

Admin ▾

User 'Admin' is logged on (since 'Thu May 28 14:35:24 2026').
User 'Admin' was previously logged off 'Thu May 28 14:35:24 2026'

10 Minutes ▾ Session Idle Timeout

☒ Page load indicator

☒ Scrolling page below parked header

Page Width Wide 1200px ▾

Scroll Height Std 600px ▾

☒ Display IP address on front panel LCD

☐ Display decoder status on Login page

☒ Display HALO Daemon disable/enable at [Setup->Server->HALO](#)

☒ Display reboot and power off buttons at [Setup->Server->Main/License](#)

☒ Display SSH connection disable/enable controls at [Setup->Network->Security](#)

☒ Offer CAP PUSH INPUT in the CAP Decoder selector at [Setup->Net Alerts->CAP Decode](#)

Add New User Account

Enter unused login name

View Only Level ▾ Set permission level

Enter account comment

User & Password ▾ Authentication Type

Set Password for new account

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

Retype the password

8 to 16 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.
- D. Time setup.
- E. Alert storage management setup.
- F. Networked GPIO setup.

Basic Operation Level:

- A. Can encode and forward alerts and run local access forwarding interface.
- B. Can terminate EAN with password re-entry.
- C. No Setup operations.

EOC Operation Level: Special simplified level for Emergency Operation Centers.

Using Local User/Password Authentication

Change Password

Enter Current Password

Enter New Password (space, #, & not allowed)

Re-enter New Password

8 to 16 characters, with both letters and numbers

PASSWORD last modified 'Fri Feb 20 13:57:08 2026 EST' (96 days ago)

Submit Changes? Cancel Changes

Back Refresh Top Bot Stat.Srvr/ GPIO OpLog SessionLog Audio.Out /In /Radios /MP Set-Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts.Sent/ In/ Decd/ All RWT

Digital Alert Systems, Inc. All rights reserved. 2026

6.0 Users Setup Screen

The **Edit User Account Profile** section of the screen is where existing User Account profiles are updated, including 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.

Account status pull-down menu

The pull-down menu under the **Session Idle Timeout** menu displays the permission level assigned to that user. Permission levels have been defined to meet the roles and responsibilities of personnel needing access.

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.

Permission Levels

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 have access to 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: • 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: • Decoder channel enable/disable • Encoder required test setup • Configuration file interface • Time setup • Alert storage management setup • Networked GPIO setup
Basic Operation Level	Can encode and forward alerts, run local access forwarding interface, and terminate EAN (National Emergency Message) with password re-entry. No setup operations
EOC Operation Level	Special simplified level for Emergency Operation Centers. Can encode alerts and terminate EAN with password re-entry. No setup operations

View Only Level	Decoded, originated, and forwarded alerts and status can be viewed. No alerts can be originated. No manual forwarding. No cancellation. No setup operations
------------------------	---

Edit User Account Profile

Admin ▾

User 'Admin' is logged on (since 'Thu Mar 5 11:11:57 2026').
User 'Admin' was previously logged off 'Thu Mar 5 11:11:57 2026'

10 Minutes ▾ Session Idle Timeout

☒ Page load indicator

☒ Scrolling page below parked header

Page Width Wide 1200px ▾

Scroll Height Std 600px ▾

☒ Display IP address on front panel LCD

☒ Display decoder status on Login page

☐ Display HALO Daemon disable/enable at [Setup->Server->HALO](#)

☐ Display reboot and power off buttons at [Setup->Server->Main/License](#)

☒ Display SSH connection disable/enable controls at [Setup->Network->Security](#)

☒ Offer CAP PUSH INPUT in the CAP Decoder selector at [Setup->Net Alerts->CAP Decode](#)

Using Local User/Password Authentication

Change Password

Enter Current Password

Enter New Password (space, #, & not allowed)

Re-enter New Password

8 to 16 characters, with both letters and numbers

Search

Edit User Account Profile

PROD17 ▾

User 'PROD17' was previously logged on 'Wed Nov 9 06:57:22 2022'
User 'PROD17' was previously logged off 'Wed Nov 9 06:59:07 2022'

☐ Allow user to change password. Disabled. Check to enable. Effective immediately.

Operation Level ▾ Permission Level

Production Account Comment

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 'Wed Nov 9 06:42:48 2022 EST' (2 days ago)

Submit Changes? Cancel Changes

Delete this User?

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

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 Level users when viewing other users and will have an immediate effect. This option is disabled for users with View Only or EOC Operation Level permissions

Session Idle Timeout

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

Page load indicator

When checked, the 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.

Scrolling page below parked header

When checked, the header will appear at the top of each screen and scrolls everything below the sub-tabs. This setting is available to all user levels.

Page Width

The page width settings for the web interface increases in increments of 200px starting at 800px to

1800px, and 3000px. Use the pull-down menu to select the desired page width. This setting is available to all user levels.

Scroll Height

The scroll height settings for the web interface increase in increments of 200px starting at 400px to 1800px. These settings represent the height from the bottom of the header to the bottom of the web interface when the **Scrolling page below parked header** feature (above) is enabled. Use the pull-down menu to select the desired scroll height. This setting is available to all user levels.

Display IP address on front panel LCD

When enabled, the IP address will be displayed on the front panel LCD.

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 Digital Alert Systems device. At the top left is the logo and name 'Digital Alert Systems'. To the right, it says 'DASDEC EAS Decoder' with 'Serial: 90321' and 'Platform ID: FNVZBIYWALF3HWJANGN'. Below the logo are input fields for 'Username' and 'Password', and a blue 'Sign me in' button. To the right of the login fields are two columns of status indicators. The 'Analog' column lists 'WBAP LineL ZERO', 'KSCS LineR ZERO', and 'NOAA LineL ZERO'. The 'Digital' column shows 'PUSH INPUT Connected' and 'FEMA /PAWS Connected' in green boxes. At the bottom, there is a copyright notice for 2026 and a disclaimer.

Login Screen with Decoder Status Display

Display reboot and power off buttons at [\(link\)](#)

Within the **Setup > Main > Main/License** screen there is a **Restart System** button. This screen displays the status of license keys. This check box enables an Administration Level user to display/hide a **Reboot** and **Power Off** button for all users. This setting is only available for Administration Level users.

Display SSH connection disable/enable controls at [\(link\)](#)

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.

Offer CAP PUSH INPUT in the CAP Decoder selector at [\(link\)](#)

Within the **Setup > Net Alerts > CAP Decode** 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.

Using Local User/Password Authentication

This section allows the user to change their password if authorized by the Admin.



Using Local User/Password Authentication

Change Password

Enter Current Password

Enter **New Password** (*space, #, & not allowed*)

Re-enter **New Password**

8 to 16 characters, with both letters and numbers

PASSWORD last modified 'Fri Feb 20 13:57:08 2026 EST' (96 days ago)

Using Local User/Password Authentication

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, these changes are immediate.

Cancel Changes

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

Delete this User?

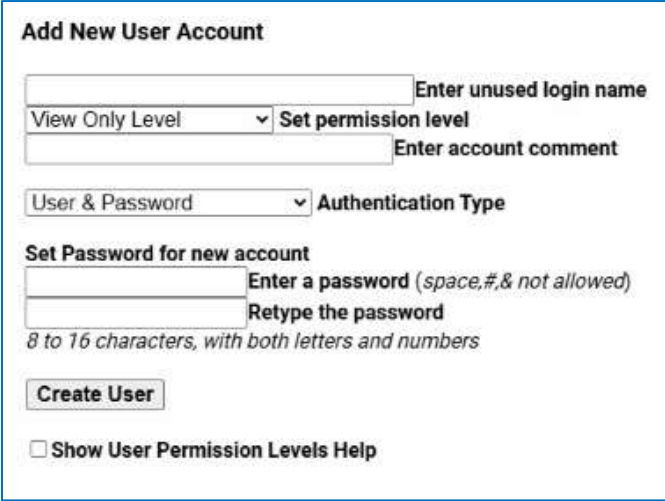
This button is only shown when an Administration Level account is editing other users. Clicking this button will immediately remove the selected user account.

Password Policy

Details of the password policy can be found in the Initial Setup section of this manual as well as below. Click on the following link to review: [Password Policy](#)

Add New User Account

The **Add New 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.



The image shows a web form titled "Add New User Account". It contains several input fields and dropdown menus. At the top is a text field for "Enter unused login name". Below it is a dropdown menu for "View Only Level" with a "Set permission level" label. Next is a text field for "Enter account comment". Below that is a dropdown menu for "User & Password" with an "Authentication Type" label. Underneath is a section for "Set Password for new account" with two text fields: "Enter a password (space, #, & not allowed)" and "Retype the password". Below these fields is a note: "8 to 16 characters, with both letters and numbers". At the bottom of the form is a "Create User" button and a checkbox labeled "Show User Permission Levels Help".

Add New User Account Interface

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

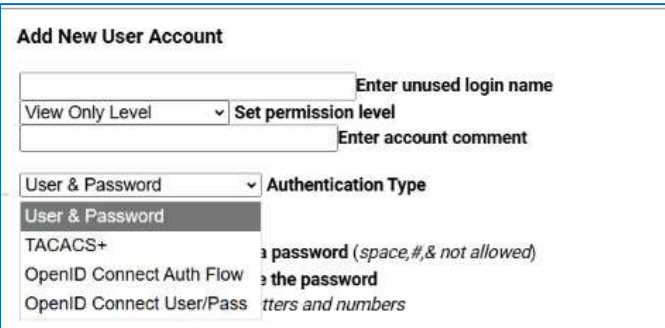
Click on the pull-down menu to see the six permission levels. Select the desired level by clicking on it.

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.

Authentication Type

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



This image is similar to the one above, but the "Authentication Type" dropdown menu is open, showing four options: "User & Password", "TACACS+", "OpenID Connect Auth Flow", and "OpenID Connect User/Pass". The "User & Password" option is currently selected and highlighted. The rest of the form fields and labels are the same as in the previous image.

Add New User Account

Set Password for new account

The password for any new account must be entered twice to ensure accuracy. Please review the [Password Policy](#) above or at the beginning of the document. 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 policy, 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.

Creating New User Accounts

To create a new user account:

1. Make sure an Administration Lever User is selected in the User Account pull-down menu.
2. Enter a unique name in the **Enter unused login name** text 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** text fields. Please review the [Password Policy](#).
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.

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.

Edit User Account Profile – MultiStation Mode

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 'account name' text display. For instance, if Admin is logged on twice, the header displays 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 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.

Email Setup

The EAS device can be configured to send email upon alert decoding, origination, and forwarding. The **Setup > Email** page is used to configure an outgoing email server and to configure the user send options. There are two sub-tabs within the **Email** setup section: **Settings** and **Users**.

Sub-Tab	Description
Settings	Where the outgoing mail settings are configured.
Users	Where a list of all current email recipients is found.

Settings

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

EMail Settings Screen

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

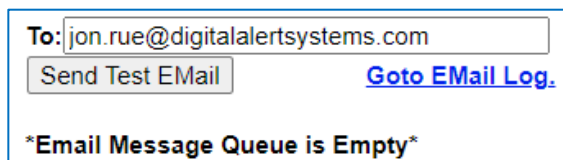
1. Go to **Setup > EMail > Settings**.
2. Enter the name of the outgoing mail server in the **Outgoing EMail Server Name** text field.
3. Click the **Set & Test Mail Server & From Names** button. The EAS device will attempt to contact (via a ping) this email server. If it succeeds, the message **OK: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

Many email services require a valid email address in order to send emails. In these cases, enter the appropriate email 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 email service on this device.

The screenshot shows a web interface for testing email. It features a 'To:' text field containing the email address 'jon.rue@digitalalertsystems.com'. Below the text field is a 'Send Test Email' button. To the right of the button is a blue hyperlink labeled 'Goto EMail Log.'. Below these elements, a status message reads '*Email Message Queue is Empty*'.

To: jon.rue@digitalalertsystems.com

Send Test Email [Goto EMail Log.](#)

Email Message Queue is Empty

Test EMail Section

To test this email client is configured correctly by means of the chosen email server, type a valid email address in the **To:** text field and click **Send Test Email**. An email titled *Test Email from DASDEC* will be sent to the entered addressee. Confirmation of proper configuration is established when this email 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.

The screenshot displays the 'Unsent Messages in Queue' section. At the top, there are two buttons: 'Resend Frozen Queued Messages' and 'Delete All Queued Messages'. Below these buttons, a message box states '1 Unsent Messages in Queue' and provides instructions: 'If any are frozen, check mail server name or DNS reliability. Frozen messages are automatically resent every 4 minutes.' Below the text, an email header is shown: '0m 420 1q4LSn-0002BY-01 <eas@rochester.rr.com> jon.rue@digitalalertsystems.com'.

Resend Frozen Queued Messages Delete All Queued Messages

1 Unsent Messages in Queue
If any are frozen, check mail server name or DNS reliability. Frozen messages are automatically resent every 4 minutes.

0m 420 1q4LSn-0002BY-01 <eas@rochester.rr.com>
jon.rue@digitalalertsystems.com

Unsent Messages in Queue

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.

The **Go to Email Log** hyperlink will direct to **System > Logs > Email Log**. This is where the list of the Email Submission Queue and the Email Send Queue can be found.

Users

The Users sub-tab is where a list of all current email recipients is found. Recipients can be added, deleted, or edited in this section. This sub-tab also includes a check box to enable/disable categorization of weekly and monthly EAS Event Reports.

The screenshot shows the 'Email Users Screen' within a software application. The top navigation bar includes tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under the 'Setup' tab, there are sub-tabs for 'Users', 'Email', 'GPO', 'Printer', 'Alert Settings', 'Network', 'Time', and 'Users'. The 'Users' sub-tab is selected. Below the sub-tabs, there is a 'Settings' section with a 'Users' checkbox. Below this, a message states 'No email users yet.' and there is an 'Add New User' button. At the bottom, there is a checkbox for 'Weekly and Monthly EAS Event Report is Categorized (sorted)'.

Email Users Screen

When adding or editing a user, **Accept** and **Cancel** buttons will appear below the **Users** sub-tab label. Once any desired updates have been made to the **Users** screen, click the **Accept** button to input these settings. The **Cancel** button is used to cancel any updates and refresh the screen.

To add a new user:

1. Click on the green plus sign next to **Add New User**. A new email user will be created with a temporary email address.

Add New User screen

2. Click the **Edit** button to edit the new user information. In the **Edit** screen, change the new users email address in the **Email Address** text field. Give the user a “friendly” name in the **Name** text field.
3. On the right side of the screen is a list of available reports that can be emailed to the user. There are twelve different reports that a user can have sent to them.

Email User Confirmation Screen

The following table gives a brief description of each report.

Report Option	Description
Weekly Report	Weekly EAS event report. Email sent at the beginning of the broadcast week.
Monthly Report	Monthly EAS event report. Email sent the first day of each month.
Decode Error	EAS event report. Email sent in the event of a decode error.
Missed Weekly Test (RWT)	EAS event report. Email sent in the event of a missed required weekly test.
Missed Monthly Test (RMT)	EAS event report. Email sent in the event of a missed required monthly

	test.
CAP source online/offline status change	EAS event report. Email sent in the event of a CAP source status change.
Decoded Alerts	Decoder report. Email sent upon alert decoding.
Forwarded Alerts	Decoder report. Email sent upon alert forwarding.
Originated Alerts	Encoder report. Email sent upon alert origination.
Login Success	Server access report. Email reporting of successful login.
Login Failure	Server access report. Email reporting of failed login.
Changed Radio Tuning	Server access report. Email reporting of changed radio tuning.

Use the corresponding check boxes to enable or disable the emailing of the selected reports. Click the **Accept** button to save the new user information and settings.

The **Edit** button to the right of any previously added user opens the user setup screen. This allows you to edit the recipients email address, the users “friendly” name, and what reports that particular user wants to receive at any time. Always click the **Accept** button to save any changes made.

The **Delete** icon, also to the right of the previously added users, can be utilized to delete any unwanted email user profiles.

The **Weekly and Monthly EAS Event Report is Categorized (sorted)** check box is used to enable/disable a combined weekly and monthly EAS event report. When enabled, this option puts all the reports in groups by type: originated alerts, forwarded alerts, and then decoded alerts. They are then put in order by date and time.

Add New User

Audio Setup

Audio is at the heart of an EAS system. Because the EAS device 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** sub-tabs 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 **Setup > Audio** page contains two sub-tabs: **Audio Inputs** and **Audio Outputs**. With a valid

MultiStation license, the Multiplayer sub-tab will also be present.

Sub-Tab	Description
Audio Inputs	This sub-tab is where the audio inputs are configured.
Audio Outputs	This sub-tab is used to configure the audio output for the Front Panel Speaker, and Primary Output, and Secondary Output.
AES-67/LiveWire+	Invokes livewire compatible devices to switch to and from the DASDEC digital audio stream during and after alerts, respectively.
Multiplayer	This tab is used when a MultiPlayer license is installed to configure audio settings.

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 or selection boxes and clicking buttons on these pages take immediate effect.

Audio Inputs

This sub-tab is where the audio inputs are configured. Here you can select the Primary, Secondary and Optional Tertiary inputs and configure their settings.

Audio Inputs Configuration

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

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

For a radio to be utilized by the EAS device, the device must be set to the internal audio source that indicates a radio is available. The chosen radio frequency settings are automatically recalled at boot time following a software restart.

The Audio Inputs sub-tab is divided into four sections: Primary, Secondary, Post Decoded Alert Auto-Snapshot, and Select audio device for alert audio file recording. The Primary and Secondary sections provide names and controls for two decoders to be selectively enabled/disabled and for decoder input levels to be set. Typically, all decoders can be enabled, but it is not required. The EAS device supports two decoders per stereo line input channel. This results in each sound card device providing two decoders. Each decoder is displayed separately and can be enabled/disabled by checking or unchecking the check box before its name.

The screenshot shows the 'Audio Inputs' configuration window. It features four tabs: 'Audio Inputs', 'Audio Outputs', 'AES-67 / Livewire+', and 'Multicast'. The 'Audio Inputs' tab is selected. Under the 'Primary' section, there are two radio input configurations: 'Radio 1' (VHF-FM, 98.1 MHz) and 'Radio 2' (WFC, 98.9 MHz). Each has a 'Level' status indicator (red for Low, green for OK, yellow for Elevated, red for High), a 'Level Adjust' slider, and an 'Autotune' button. Under the 'Secondary' section, there are two configurations: 'L2 SOURCE' (NOAA) and 'R2 SOURCE' (NWS), each with similar level indicators and adjustment options. At the bottom, there is a checkbox for 'Post Decoded Alert Auto-Snapshot' and a section for 'Select audio device for alert audio file recording' with options for 'Main Audio (Microphone)' and 'Auxiliary Audio 1 (Microphone)', and a sub-section for 'Input Source' with options for 'Microphone Input' and 'Line Input Left'.

Audio Inputs Settings

Primary

The Primary menu includes the two options of analog audio input Line-In Jack for L1 Source or R1 Source. Typically, this will be set to the Radio1/Radio2 setting for the Primary input. To connect external radio receivers, use the Line-In Jack setting on the appropriate sound card device.

Radio1/Radio2

The decoder base names, Radio1 and Radio2, are automatically set by the server and provide an identification tag for the decoder. Additionally, the text box to the right of this designation can be used to give each input a more specific designation.

Frequency

This option only appears when you have radio licenses. This pull-down menu contains three frequency options: AM, FM, or NOAA. Once one has been chosen, use the text box to indicate the actual frequency which is desired. The range available is indicated next to the text box.

Level

EAS decoding is sensitive to audio input levels. The quality of the input level is constantly being rated in real time. The Level status is automatically rated by:

- Zero (red)
- Low (red)
- OK (green)
- Elevated (yellow)
- High (red)

Level Adjust

Use the Level Adjust text box to change the input level as needed. Enter a value between 1 and 100 until the Level Status is OK (green) or occasionally Elevated (yellow).

Use the Refresh button in the header of the page to make multiple checks of the Level quality. This will assist in setting the correct level setting.

Snapshot

Each decoder is given a Snapshot button. Snapshot captures the current audio decoding buffer for this channel. When clicked, a sample of the corresponding decoder audio input buffer is saved, dated, and displayed as a hyperlink to the right of the Snapshot button. The file name is the day of the week, month, day, time (in hh:mm:ss 24hr format), and year the file was created. It can be viewed by clicking on the hyperlink.

Autoscale

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. In the Autoscale pull-down menu you can choose to select None, FFT Filter, or Amplification.

Monitor

The Monitor pull-down menu allows you to select the appropriate monitor output to hear the audio from. You can choose to select None, Front Panel Speaker, Main Audio output, Aux1 Audio, MP3 Stream (http identified), or OGG/Vorbis Stream (http identified).

Selecting the MP3 or OGG/Vorbis Stream monitor option allows 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 a location apart from the device location. The host computer web browser will need a streaming audio player that can support either MP3 or OGG/Vorbis audio format.

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.

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

Post Decoded Alert Auto-Snapshot

Post Decoded Alert Auto-Snapshots are displayed chronologically, newest to oldest, and numbered accordingly under the input for which they were run. The file name is the day of the week, month, day, time (in hh:mm:ss 24hr format), and year the file was created. It can be viewed by clicking on the hyperlink.

The **Post Decoded Alert Auto-Snapshot** check box enables/disables the **Post-Alert Snapshot**. The default value is enabled (checked) and should usually remain this way. This feature allows for a snapshot .WAV file to be generated after an alert is decoded or after a decode error is detected. It can also provide 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.

Select audio device for alert audio file recording

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

In addition to the Primary Audio card, the standard EAS device (excluding the DAS3-EL and DAS3-ELR models) provides one secondary 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 either Main Audio (/dev/mixer0) or Auxiliary Audio 1 (/dev/mixer2) by using the corresponding radio button to choose the recording source.

Input Source

Once the source sound card is selected, set the **Input Source** by choosing one of the following radio buttons: **Microphone Input** or **Line Input Left**. The selection is determined by the actual source from which you will record.

Record Input Level

Use the **Record Input Level** text box to set the level for the recording input gain level. Enter a value from 0 - 100 in the text box. After you set the value, a Save Info box will appear to show you the status of the value you have set.

Audio Outputs

The **Audio Outputs** sub-tab is used to configure the audio output for the Front Panel Speaker, Primary Output, and Secondary Output. Each output device results in an audio configuration interface on this page. Audio tones can be played through each available audio output to test audio connections and calibrate levels using audio test equipment. Audio .WAV and .MP3 files can be uploaded into the EAS device from this page.

Audio Outputs Settings

All standard EAS devices come from the factory with:

- Front Panel speaker
- Primary Output device

Front Panel Speaker

The **Front Panel Speaker** interface allows for editing the volume of the front panel speaker, as well as playing test tones and .WAV files.

Level Adjust

The **Level Adjust** text box sets the volume from 0 (mute) and 100 (full volume). Enter the desired value in the text field. Level values near 70 are a good starting point.

Duration

There are several audio test options available. **853 Hz Tone Test**, **960 Hz Tone Test**, or **Attention Signal Test** buttons are available. The **Duration** text field determines the length of the test (1 to 180 seconds).

There is also the option to play an uploaded audio .WAV file from the **Audio Test File** pull-down menu. When an Audio Test File is selected, the following information is displayed directly under the pull-down menu:

- Duration of the audio file in seconds
- Rate in sample/sec
- Mono or stereo audio
- **Note:** Resample to avoid run time resampling!
- A Play icon 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 Resample icon to resample the uploaded audio files.
- A Delete icon to delete the selected test audio file

Mute During Alert and Audible Decode

The option to mute the front panel speaker is available and can be enabled/disabled by checking the **Mute During Alert** check box.

Audio Decode

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

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

Primary Output

The **Primary Output** section operates like the **Front Panel Speaker** section described above, with some key differences. Check boxes are provided to enable/disable:

- Alert Audio Passthrough
- HDMI Alert Audio Output
- **Note:** The station configuration may override these settings.
- Originated Alert Audio Output
- Forwarded Alert Audio Output

Testing Levels

To test the Primary output, attach speakers to the EAS device audio output ports. Testing can then proceed as it does for the Front Panel Speaker.

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

Alert Audio Passthrough

The **Primary Output** section has a special check box that controls the state of the primary analog audio passthrough circuit. This circuit controls analog audio input/output passthrough on the associated Cat5 audio connector on the back of the EAS device. Passthrough audio allows external balanced audio to be passed through the EAS device and interrupted during an EAS audio activation.

If the Primary Output is to be tested by playing a file or a tone, or if passthrough audio is not needed, the **Alert Audio Passthrough** check box should be disabled. This will enable full time output of internal

audio. Otherwise, check to enable analog audio passthrough. When Passthrough is enabled, the only time EAS device generated audio is played on the Primary Output port is during an EAS alert.

HDMI Alert Audio Output

The HDMI Alert Audio Output enables EAS audio output on the HDMI signal. Use this check box to enable or disable this function.

Originated Alert Audio Output and Forwarded Alert Audio Output

The **Primary Output** section displays an active hyperlink and two check boxes showing whether the originated and forwarded alert audio is output on the audio device.

Secondary Output

It is possible to have multiple audio interface sections. The Secondary Output is optional and thus may not appear.

The Secondary Output functions similarly to the Primary Output with the same testing functions, but some key differences:

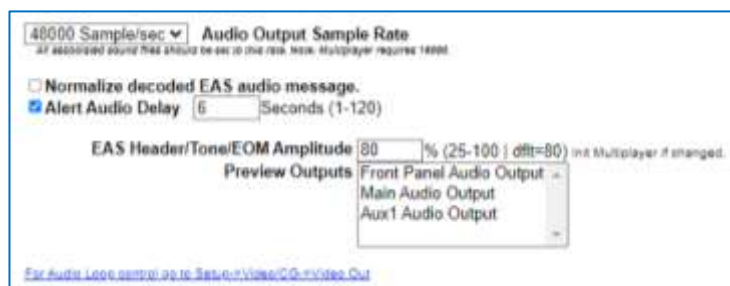
- Provides stereo output volume level control: Left Level Adjust and Right Level Adjust.
- Does not include the Alert Audio Passthrough or HDMI Alert Audio Output options.

The Secondary Output should be configured in the same manner as the Primary Output.

Audio Output Sample Rate

The Audio Output Sample Rate controls the sample rate of audio played from the EAS device. The sample rate can be changed by selecting a sample rate in the **Audio Output Sample Rate** pull-down menu. The default sample rate is 16000 sample/second. The pull-down menu contains 16000, 32000, 44100, and 48000 sample/second options. All associated sound files should be set to the same rate.

- For EAS devices with AES digital audio output, set the rate at 32000 or higher sample/second.
- Multiplayer requires 16000 sample/second.



Audio Output Sample Rate Interface

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.

Alert Audio Delay

The **Alert Audio Delay** check box is 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 between 1 and 120.

EAS Header/Tone/EOM Amplitude

The **EAS Header/Tone/EOM Amplitude** text box sets the loudness of the EAS Header, the Attention Signal, and the End of Message Tone. Any percentage between 25 and 100 is valid. The default value is

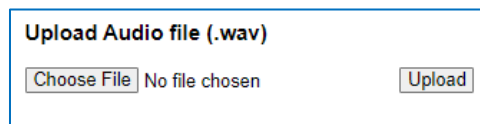
80. The Multiplayer should be initialized if the value is changed.

Preview Outputs

Preview Outputs displays all 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 Ctrl key while clicking to select.

- Front Panel Audio Output
- Main Audio Output
- Aux1 Audio Output

A hyperlink to **Setup > Video/CG > Video Out** is provided for Audio Loop control.



Upload Audio File Interface

Upload Audio file (.WAV)

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

1. Click the **Choose File** button to locate the file on the computer.
2. Click the **Upload** button. MP3 files are converted automatically into WAV files.

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

AES-67/LiveWire+

Invokes livewire compatible devices to switch to and from the DASDEC digital audio stream during and after alerts, respectively. In the event the AES-67/LiveWire+ is not licensed, the following screen is displayed.



AES-67/LiveWire+ Interface

Click this link to access **Setup > Main > Main License** to check the status of the license.

Click the **Upgrade** tab to upgrade the DASDEC using the associated software. This enables **AES-67/LiveWire+**. Once upgraded, the following screen is displayed:

AES-67/LiveWire+ Screen

Enable AES67 Audio

Click this box to **Enable/Disable AES67**.

Output Name

Enter the **Output Name** or select from a pull-down menu if offered.

Unicast or Multicast IP Address

Enter the targeted **IP Address**.

Multicast Network device

Select the AES67 multicast Ethernet device name directly from the pull-down menu used to choose which network card to use.

Originated Alert Audio Output

Check this box to select the **Originated Alert Audio Output**.

Forwarded Alert Audio Output

Check this box to select the **Forwarded Alert Audio Output**.

Duration

Use the text box to enter the desired **Duration** of the test audio output in seconds.

Audio Test File

Use the pull-down menu to select the type of **Audio Test File** desired.

LiveWire+

Check **ENABLE LiveWire Device** to enable a specific device.

Interface Name

Enter the **Interface Name** of the remote **LiveWire Device** to be enabled.

Device Type

Enter the Device Type of the remote **LiveWire Device** to be enabled.

IP Address

Enter the IP Address of the remote **LiveWire Device** to be enabled.

Select Output IDs

Select the **Output IDs** by clicking in the box under the desired number.

FIPSS Group

Enter the targeted **FIPS Group**.

EAS Group

Enter the targeted **EAS Group**.

Multiplayer

The Multiplayer sub-tab will only be visible if a valid MultiStation license has been installed. Once installed, settings for the Multiplayer will be accessible in this sub-tab.

Click on **Enable Multiplayer Interface** to display the configuration options.

Multiplayer Network Access Configuration settings include:

- Multiplayer IP address
- Multiplayer FTP User Name
- Enter New Password

The screenshot shows the 'Multiplayer Configuration Options' screen. At the top, there are tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs: 'Main', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. The 'Audio' sub-tab is selected, and within it, the 'Multiplayer' option is highlighted. Below this, there are fields for 'Multiplayer Network Access Configuration', including 'Multiplayer IP Address' (set to 'guest'), 'Multiplayer FTP User Name' (set to 'guest'), and 'Enter New Password'. A message below these fields states: '(Password is set) Missing or invalid Multiplayer IP address.' At the bottom, there are 'Accept Changes' and 'Cancel Changes' buttons.

Multiplayer Configuration Options

Video/CG Setup

Select **Setup > Video/CG** to access settings for controlling operation of external and internal character generation. 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. The system provides support for a single HUB extender with optimized matching for specific USB devices.

The screenshot shows the 'Video/CG Setup' screen. At the top, there are tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs: 'Main', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. The 'Video/CG' sub-tab is selected. Below this, there are sub-tabs for 'Video Out', 'Main Serial', 'USB Serial 1', 'USB Serial 2', 'USB Serial 3', and 'USB Serial 4'. The 'Video Out' sub-tab is currently selected.

Video/CG Sub-Tabs

In Broadcast mode, with a valid Plus Package License Key, there are six sub-tabs within the **Video/CG** navigation tab:

Sub-Tab	Description
Video Out	Provides settings for Page Display, Duration, Title, Color, and Font control.
Main Serial	Provides options for Main Serial Port Configuration of Character Generators and other Devices.
USB Serial 1	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.
USB Serial 2	
USB Serial 3	
USB Serial 4	

Video Out

The **Video Out** sub-tab contains two check boxes:

- Internal Video Slate
- Linux CLI prompt after video output

The EAS device can generate HDMI video output for originated and forwarded alerts. When video output is generated, a set of details pages will be played out of the HDMI video output port.

Video Out Sub-Tab

Internal Video Slate

Use this check box to enable or disable the **Internal Video Slate** configuration options, if licensed and the hardware support is enabled. The EAS device can provide a full screen HDMI video display, with embedded EAS Audio, of the current originated or forwarded alert.

Video Out – Internal Video Slate Screen

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 > Station >**

Page Display

The **Page Display** pull-down menu has two settings available:

- Page duration for multi-page display is a fixed number of seconds
- Page duration for multi-page display is ≤ 20 secs based on Video Duration

Multi-page Duration

Enter the number of seconds per page in the text field provided.

Safe Title

Safe title checkbox is used to alert video text output & DASH & streaming video alert text.

Page Color

The following color selections are available within this pull-down menu:

- Red outline around Dark Blue-Violet
- Red
- Dark Red
- Orange
- Chromakey Green
- Chromakey Blue
- Blue
- Dark Blue-Violet
- Black

Font Size

This pull-down menu sets the font size for the video page output. Available sizes range from 16 to 72.

Font Style

This pull-down menu sets the font type for the video page output. There are 14 available fonts with a mix of serif, sanserif, bold, italic, and narrow.

Custom first line of text

The text entered into this field will be displayed as the first line of each page of the alert. This is an optional field.

Create page title override

Check this box to display the **Alert page title override** text field. Once displayed, enter the message details.

Display

These are a series of five buttons used to test the HDMI output:

- **Show Color Bars** – Displays color bars on the HDMI output
- **Show Date/Time** – Displays the current date and time on HDMI output
- **Show Character Set** – Displays a set of characters based on the configured font, size, and color on the HDMI output.
- **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.

Generate MPEG DASH

Check this box to generate **MPEG DASH**. In the event DASH MPEG is licensed but has no outgoing connection to HDMI, VGA, or a ghost terminator plug, the following message will be displayed with a dark background "DASH MPEG licensed, but requires HDMI or VGA monitor or ghost terminator plug."

Video Out Main Serial USB Serial 1 USB Serial 2 USB Serial 3 USB Serial 4

Multistation Active. **NOTE:** Override station setting. Specific station config has its own video enabled setting.

☒ **Internal Video Slate**

Page Display: Page duration for multi-page display is a fixed number of seconds

Multi-page Duration: 5 Seconds per page

Safe Title: ☒

Page Color: Red outline around Dark Blue-Violet

Font Size: 32

Font Style: Luxi Serif Mono Bold

Custom first line of text: (Optional)

☐ Create page title override

Display: Show Color Bars Show Date/Time Show Character Set Clear Release Video

☒ **Generate MPEG-DASH**

Manifest Format: ISO-BMFF

Audio/Video Options: Audio Only

Manifest file name: manifest

H.264 Compression Quality: 32

H.264 Profile Value: Main (Default)

Generate MPEG-DASH options

Manifest Format

Provides a pull-down menu for options of CIF and ISO-BMFF.

Audio/Video Options

Provides the following options:

- Audio+Full Video
- Audio+LoRes Video
- Audio Only

Note: Audio Only has been added to the options.

Manifest file name

Text box used to enter the **Manifest file name**

H.264 Compression Quality

Provides a pull-down menu of compression options, the default is 32.

H.264 Profile Value

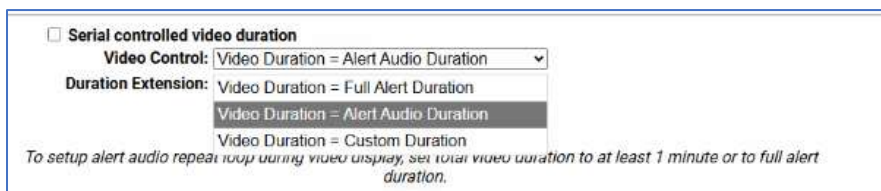
Provides a pull-down menu of options, the default is **Main**.

Serial controlled video duration

The checked box uses default Serial controlled video duration.

The un-checked **Serial controlled video duration** allows the user to manually configure the following variables:

- **Video Control**
 - Full Alert Duration
 - Alert Audio Duration
 - Custom Duration



Video Control Pull-Down Menu

- **Duration Extension – Optional Max 1 hr**

- Minutes
- Seconds



Duration Extension Options

To set a custom duration, input the desired minutes and seconds into the appropriate text fields. The maximum duration allowed is one hour.

Linux CLI prompt after video output

The **Linux CLI prompt after video output** check box forces the video output to display the command line prompt. Enabling this option will cause a four second delay in the alert video – NOT RECOMMENDED.

Click **Accept Changes** to apply changes to this page. Click **Cancel Changes** to cancel the changes and refresh the screen.

Click the **Accept** button under the **Video Out** sub-tab label to accept all changes that have been made to the sub-tab. Click **Cancel** to cancel any changes.



Linux CLI Prompt After Video Output

Main Serial

The **Main Serial** sub-tab allows Serial Port Configuration of Character Generators and other Devices.

Serial Port Configuration - Character Generators and Other Devices.

Check one option to select the protocol used when an alert is originated or forwarded to this serial port.
The device should be connected to the server serial port using the correct serial cable (TFT,VDS : NULL modem cable, Monroe,XBOB,CODI CGs,BDI Switcher: straight through cable, SAGE Generic depends on specific CG). Use SAGE Generic for Evertz CG.

☒ Off
 ☐ Monroe R194 CG
 ☐ Monroe CEMS-0500/1000
 ☐ Standard TFT
 ☐ VDS
 ☐ Sage Generic CG
 ☐ Sage News Room
 ☐ Chyron CODI
 ☐ XBOB CG
 ☐ XBOB4 CG
 ☐ BETABRITE LED Sign
 ☐ Monroe Envoy
 ☐ BDI GPM-300 Matrix Switcher
 ☐ BTI MSRP Audio Switcher
 ☐ DM Engineering MSRA/MSRE Audio Switcher

☒ View Advanced Options (unchecked to remove view).

Global Serial Port Timeout (secs)

☐ Port Ready Confirm mode. Disabled. Check to enable.

Accept Changes Cancel Changes

Main Serial Sub-Tab

Serial Port Configuration - Character Generators and Other Devices

The radio button selected shows the Character Generator (CG) used when a decoded alert is forwarded or encoded, or if no CG is being used. The supported character generator protocols are:

- Monroe R194 CG
- Monroe CEMS-0500/1000
- Standard TFT
- VDS
- Sage Generic CG
- Sage News Room
- Chyron CODI
- XBOB CG
- XBOB4 CG
- BetaBrite LED sign
- Monroe Envoy
- BDI GPM-300 Matrix Switcher
- BTI MSRP Audio Switcher
- DM Engineering MSRA/MSRE Audio Switcher

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.

The CG should be connected to the server serial port (on the back panel) using the correct serial cable:

- TFT, CODI, and VDS use NULL modem cable.
- Monroe CGs use straight through cable.
- SAGE Generic depends on specific CG, usually a straight through cable.

Choose the appropriate protocol for the connected serial device and select that option. 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 can be configured to run repetitions of the video output during an alert.

The screenshot shows the 'Setup' tab with the 'Video/CG' sub-tab selected. Under 'Main Serial', 'XB0B4 CG' is chosen. The 'XB0B4 CG Attribute Settings' section includes the following options:

- Vertical Line Position (0-16; 0 or 1 is standard top of screen EAS broadcast position)**: Set to 1.
- White Character/Clear Background**: Set to 'Draw Mode'.
- Hardware Flow Control**: Set to 'Serial Port Flow Control'.
- Iterations (1-5)**: Set to 1.
- Do Not Repeat Video**: Set to 'Repeat Alert Video Display'.
- Test Display**: A button to test the settings.
- Stop Display/Clear Screen**: A button to stop the crawl and clear the screen.
- Remove Splash Screen**: A button to clear the default XB0B4 boot startup splash screen.
- Periodic Text Display**: A checkbox that is currently unchecked.
- Use Simultaneous Override Alert Text**: A checkbox that is currently unchecked.
- Override Station Alert Text Mode**: A pull-down menu.

XB0B4 CG Attribute Settings

CG Attribute Settings Section

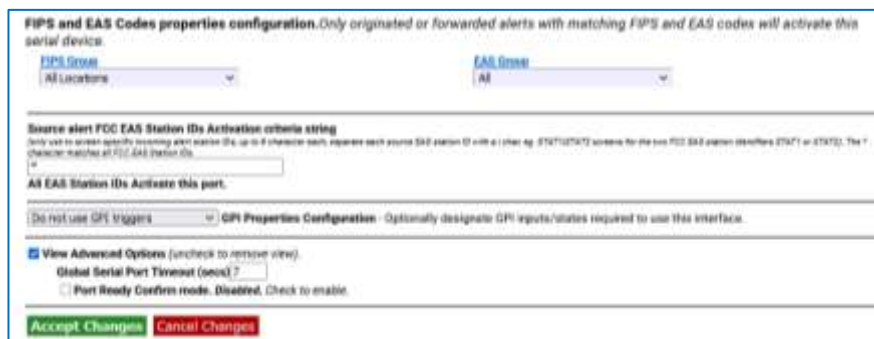
The options displayed in the **Attribute Settings** depend on the selected CG protocol.

The screenshot above shows the Decade Engineering XBOB-4 CG selected. A user would choose the correct settings for:

- Vertical Line Position
- Draw Mode
- Serial Port Flow Control
- Iterations
- Repeat Alert Video Display

There are also **Test Display**, **Stop Display/Clear Screen**, and **Remove Splash Screen** buttons, which can be used to test the settings selected.

This interface includes a **Periodic Text Display** check box, as well as an **Override Station Alert Text Mode** pull-down menu as additional settings that can be modified.



FIPS and EAS Codes Properties Configuration Section

FIPS and EAS Codes properties configuration

Use this section to edit activating FIPS Groups and EAS Code Groups. Originated or forwarded alerts with the matching FIPS and EAS codes selected here will activate the serial device.

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, edit, or delete) the FIPS Group 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 (NIC and EAT event codes are displayed red). 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 Activation criteria string

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

GPI Properties Configuration

A pull-down menu is provided to select a specific GPI's state (open, closed, or do not use) 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.

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 screenshot shows the 'Setup' tab with 'Video/CG' selected. Under 'USB Serial 1', the 'Expansion USB Serial 1 OK' status is shown. The configuration options include radio buttons for various protocols: OFF, Monroe R194 CG, Monroe CEMS-0500/1000, Standard TFT, Sage Generic CG, Sage News Room, Chyron CODI, XBOB CG, XBOB4 CG, VDS, BETABRITE LED Sign, BDI GPM-300 Matrix Switcher, BTI MSRP Audio Switcher, and DM Engineering MSRA/MSRE Audio Switcher. The 'View Advanced Options' checkbox is checked, showing a 'Global Serial Port Timeout (secs)' of 7 and a 'Port Ready Confirm mode' checkbox which is disabled. At the bottom, there are 'Accept Changes' and 'Cancel Changes' buttons, and a footer with navigation links and copyright information.

USB Serial 1 Screen

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
- XBOB CG
- XBOB4 CG
- 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.

USB Serial port CG Attribute Settings

The supported character generator protocols and their options are outlined 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 menu 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.

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 is a minimum of 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, notification and alert command access are given 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

This option is typically used when 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**, **Software**, or **No Flow Control** depending upon the hardware support on the remote device.

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 menu 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**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
- 240 Pix/Sec NTSC
- 360 Pix/Sec NTSC
- 480 Pix/Sec NTSC
- 600 Pix/Sec NTSC
- 720 Pix/Sec NTSC
- 840 Pix/Sec NTSC
- 900 Pix/Sec NTSC
- 1080 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 Anti-aliased – default enabled

When enabled, the text is anti-aliased 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.

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 menu 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 menu 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 Port Flow Control

Select **Hardware**, **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 (below).

Set Alert Video Repetition Period (minutes:seconds)

After selecting a **Repeat Alert Video Display** pull-down menu 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 XBOB4 CG.

Stop Display/Clear Screen

Click this button to stop the Test Display and clear the video output.

Remove Splash Screen

Click this button to 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 Control

- 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 (topmost) to 208 (bottom)

Speed – Defaults to Med

- Slow
- Medium
- Fast

Crawl Font – Defaults to one

Set from 1 to 4.

Char Color – Defaults to whiteClear, key over video

- Yellow
- Bright Green
- Bright Red
- Gray
- Cyan
- Magenta
- Blue
- White
- Bright Cyan
- Bright Magenta
- Bright Blue
- Dull Yellow
- Green
- Red
- 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:

- Full Alert Duration
- Alert Audio Duration
- Custom Duration (displays duration settings in Minutes and Seconds)

The Full Alert Duration and Alert Audio Duration options apply to Originated and Forwarded alerts, while the Custom Duration option applies to Decoded alerts.

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 IDs. 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, edit, or delete) 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 (deprecated NIC and EAT event codes are displayed in red). 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 Activation criteria string

This is additional filtering 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 the station ID(s). By using the wildcard character (*), all station IDs will activate this serial port.

GPI Properties Configuration

A pull-down menu is provided to select a specific GPI's state (open, closed, or do not use) 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.

Alert Agent™ Setup

Alert Agent™ is a unique and powerful feature for the DASDEC giving users better control and functionality when configuring the EAS device and managing EAS alerts. The Alert Agent™ tab includes the following sub-tabs:

Sub-Tab	Description
Alert Policies	Configure the decoder alert language, duplicate EAS handling, triggered CAP polling, 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 five sections: Decoder Alert Languages, Configure Duplicate EAS Alert Handling for Decoder Forwarding, Triggered CAP Polling - Global Settings, Configure Update Policy for Active EAS Alerts, and Configure Pending Alert Acknowledgment. All changes to settings in this screen are immediate.

Note: Modified Triggered CAP Poling does not allow on/off state or selection by Alert Node. New rules mandate it is always on and cannot be uniquely assigned to specific events.

The screenshot displays the 'Alert Policies' sub-tab interface. At the top, there are navigation tabs: 'Alert Policies' (selected), 'Manage Alert Nodes', 'Local Access Forwarding', 'Custom Msg Forwarding', 'FIPS Groups', and 'EAS Code Groups'. The main content area is divided into several sections:

- Decoder Alert Languages:** Includes a dropdown menu with options: English, French, Spanish, and Other.
- Configure Duplicate EAS Alert Handling for Decoder Forwarding:** Contains a description of duplicate alerts and a 'Duplicate Alert Active List Options' section with checkboxes for 'Discard exact duplicate alerts upon decode' (checked), 'Duplicate detection for CAP Carcast Alert messages' (checked), and 'Duplicate detection for CAP Carcast Update messages' (checked).
- Triggered CAP Polling™ - Global Settings:** Includes a description of the polling service and a 'Global Window (10-120 Seconds)' dropdown set to 25.
- Configure Update Policy for Active EAS Alerts:** Includes a description of the update policy and a section for 'Auto-expire updated decoded and forwarded alerts' (checked), with options for 'Global FIPS match' (checked) and 'Matching Station ID' (unchecked).
- Configure Pending Alert Acknowledgment:** Includes a description of the acknowledgment process and a section for 'Pending Manual Forward Acknowledgment' with checkboxes for 'Acknowledge the pending alert from the Web interface or by pressing the front panel button' (checked), 'Play audio announcement unacknowledged **Alert** alerts' (checked), 'Play audio announcement unacknowledged **Test** alerts' (checked), 'Play audio announcement unacknowledged **Watch** alerts' (checked), 'Play audio announcement unacknowledged **Warning** alerts' (checked), and 'Play Acknowledgment Announcement on **Phone/Buzz** devices' (checked).

Alert Policies Sub-Tab 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 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 **Duplicate Alert Auto-Forward Options** pull-down menu to choose the setting to control manual or auto-forwarding for these alerts.

Triggered CAP Polling™ - Global Settings

Triggered CAP Polling is always enabled and provides a timed window where CAP sources are rapidly polled to determine if a duplicate to a decoded EAS message exists. The **Global Window** time defines the amount of time after an EAS message is decoded that 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 event codes. Additional Triggered CAP Polling controls can be found for individual Alert Nodes.

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** screen (hyperlink provided) 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 Preview Audio Devices are configured in the **Setup > Audio > Audio Outputs** screen. By checking this box, the Acknowledgment Announcement plays out the selected Preview Audio Devices. A **Preview Audio** hyperlink is provided to navigate to the Preview Audio 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** in the **Alert Forwarding** 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.

The screenshot shows the 'Manage Alert Nodes' screen with the following sections:

- Manage Decoded Event Properties:** Includes fields for 'Incoming Decoded Event', 'Event Code', 'EAS Code', and 'Station ID List'.
- Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN/NPT):**

Input Source	Forwarding Action	Play Scheduling	Alert Mode	Pre-Alert Audio	Alert Audio	Post-EM Decoding Audio	Post-Alert Audio
All Sources	Immediate	Play Scheduling	Off	None	Original, if any	Test-to-Speech if no audio	None
- Default Decode/Forwarding Node for Monthly Tests (RMT):**

Input Source	Forwarding Action	Play Scheduling	Alert Mode	Pre-Alert Audio	Alert Audio	Post-EM Decoding Audio	Post-Alert Audio
All Sources	Manual	As Soon As Possible	Off	None	Original, if any	Test-to-Speech if no audio	None
- Default Decode/Forwarding Node for Weekly Tests (RWT):**

Input Source	Forwarding Action	Play Scheduling	Alert Mode	Pre-Alert Audio	Alert Audio	Post-EM Decoding Audio	Post-Alert Audio
All Sources	Block Forwarding	Play Scheduling	Off	None	Original, if any	Test-to-Speech if no audio	None
- Default Decode/Forwarding Node for Non-National Alert Events (DFLT):**

Input Source	Forwarding Action	Play Scheduling	Alert Mode	Pre-Alert Audio	Alert Audio	Post-EM Decoding Audio	Post-Alert Audio
All Sources	Manual	As Soon As Possible	Off	None	Original, if any	Test-to-Speech if no audio	None

At the bottom, it states: 'All remaining events are DEACTIVATED.' and includes 'Accept Changes' and 'Cancel Changes' buttons.

Manage Alert Nodes Screen

The Manage Alert Nodes screen is divided into two sections: an Alert Node Tests (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:

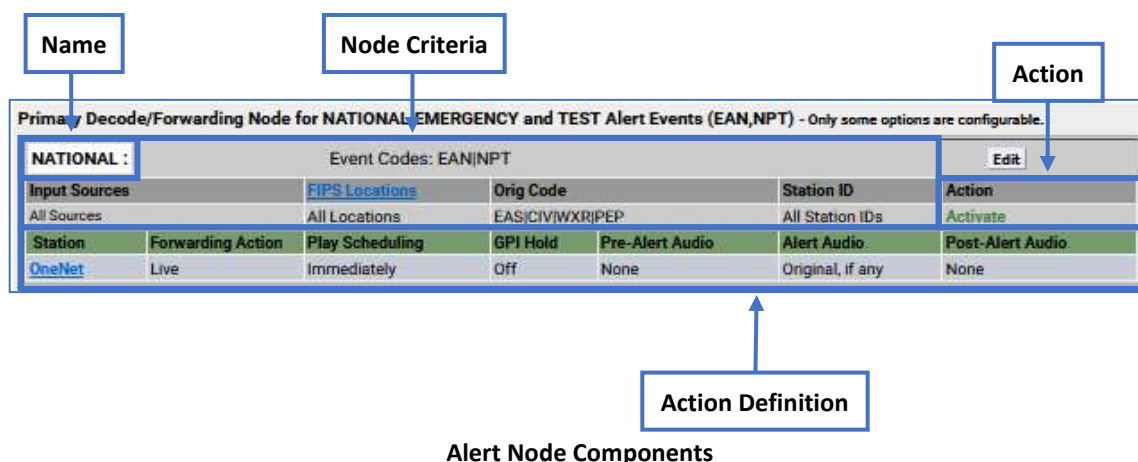
An EAS device is configured to monitor three radio sources: LP-1, LP-2, and the National Weather Service (NWS). The NWS source covers your service area, as well as areas outside your service area, along with providing Required Weekly Tests. The RWT's broadcast by this NWS source duplicates RWT's received 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 Manage Alert Nodes 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.



Editing Alert Node Criteria

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 Locations
- Event Codes
- Orig (Originator) Code
- 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 list provided by clicking each item. Pressing the CTRL key while clicking input sources will allow the user to select multiple sources.

FIPS Locations

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.

Event Codes

At the top of each Alert Node is the **Event Codes** section which includes a hyperlink to the **Setup > Alert Agent™ > EAS Code Groups** sub-tab where available EAS Code Groups can be selected. The default setting is All Codes when no specific EAS Event Code Group is needed. Only one selection may be made for this section

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 (United States Government)

Station ID

Found in the EAS header, this 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.

Action Definition

The following settings are available when an Alert Node Action is set to **Activate**:

- Forwarding Action
- Play Scheduling
- GPI Hold
- Pre-Alert Audio
- Alert Audio
- Post-Alert Audio



Editing Action Definition Settings

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

There are eight available options from this pull-down menu:

- **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 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.
- **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** 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 Outputs** sub-tab.

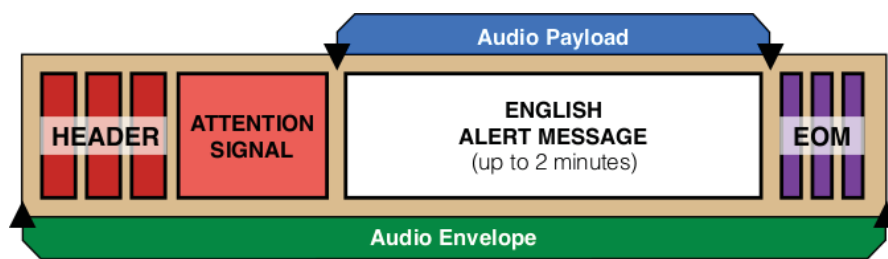


Originated/Forwarded EAS Alert Message
(with Pre-Alert, Post-Alert, & Ext. Alert Language Audio Options)

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.



Incoming EAS Alert Message
(FSK Audio)

Post EOM Omnilingual Audio

This setting is only available with a valid OmniLingual™ Enable Key. There are three options available when enabled:

- **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 Outputs** sub-tab.

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.

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.

Custom Decode/Forwarding Node for Non-National Alert Events - Decoded events are compared to each custom property in the following order until a match. If no match then drop to the Default property. No match at all results in a deactivation.

[Add custom alert node to list top](#) [Add custom alert node to list end](#)

1	Orleans Co	Event Codes: All Codes	Enabled	Edit	Remove Node
Input Sources	1003 Location	Orig Code	Station ID	Action	
All Sources	/weekly_test_file (000073)	EAS/CIVWXR/PEP	All Station IDs	Activate	
Station	Forwarding Action	Play Scheduling	SPI Hold	Pre-Alert Audio	Alert Audio
On/Off	Manual	As Soon As Possible	Off	None	Text-to-Speech if no audio
					Post-Alert Audio
					None

2	WVTS Node	Event Codes: All Codes	Enabled	Edit	Remove Node
Input Sources	1003 Location	Orig Code	Station ID	Action	
All Sources	All Locations	WXR	All Station IDs	Activate	
Station	Forwarding Action	Play Scheduling	SPI Hold	Pre-Alert Audio	Alert Audio
On/Off	During Auto-Forward Mode	As Soon As Possible	Off	None	Text-to-Speech if no audio
					Post-Alert Audio
					None

Priority of Alert Nodes

Alert Node Priority

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.

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.

1. Assign a descriptive name.
2. Configure the desired Node Criteria.
3. Select the appropriate Action (Deactivate/Log Only or Activate).
4. Configure the Action Definition settings.
5. Click the **Accept Changes** button.

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. Located at the top of the **Manage Alert Nodes** sub-tab, there are 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 screenshot displays the 'Manage Decoded Event Properties' window. It includes a 'Test Node' section with a 'Test Node' button and a 'Test Results' field. Below this is a table for 'Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN/NPT)'. The table has columns for 'Event Codes - EAN/NPT', 'Station ID', 'Action', and 'Station ID List'. The 'Event Codes - EAN/NPT' column is expanded, showing a table with columns: 'Input Sources', 'All Sources', 'All Locations', 'EAS/OWNS/PEP', 'Station', 'Forwarding Action', 'Play Scheduling', 'SPY Hold', 'Pre-Alert Audio', 'Alert Audio', and 'Post-Alert Audio'. The 'Station' column is expanded, showing a table with columns: 'Forwarding Action', 'Play Scheduling', 'SPY Hold', 'Pre-Alert Audio', 'Alert Audio', and 'Post-Alert Audio'. The 'Forwarding Action' column is expanded, showing a table with columns: 'Forwarding Action', 'Play Scheduling', 'SPY Hold', 'Pre-Alert Audio', 'Alert Audio', and 'Post-Alert Audio'.

Test Node Interface with Results

The first step in running an Alert Node test is to input the test settings. There are five settings to input. Once these settings have been selected, click the **Test Node** button to run the test.

Input Source

This pull-down menu contains all the available sources (radios, CAP/IPAWS, 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.

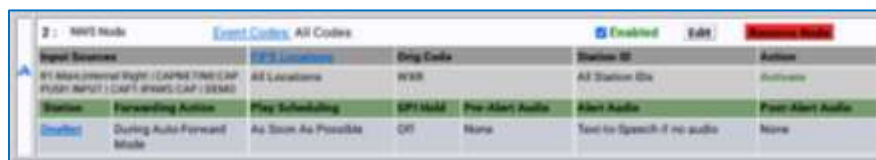
Station ID List

The default value for this text field is an asterisk '*', indicating all Station IDs. When testing a Node for a specific Station ID, replace the asterisk with the desired Station ID.

The **Results Field** is located in the lower left corner of the Test Node interface; 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 above.)

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.



Alert Node with MultiStation Input Sources

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 playout of the incoming alert and what audio is associated with that alert message.

Local Access Forwarding

The **Local Access Forwarding** 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 (Custom Emergency Message)**.

Local Access Forwarding Screen

Custom Text Translation for CEM (Custom Emergency Message)

This check box controls activation of the local access forwarding feature. When enabled, as shown in the above screenshot, 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:

Decoder Local Access Forwarding – Status Section

When a CEM alert is forwarded under control of Local Access Forwarding, the status window will display the EAS device 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.

Send Alerts **Alert Events** **System** **Setup**

General Alerts One-Button Alert **Custom Message**

Password for user 'Admin' is older than 180 days!

Custom Message Options NOTE: Changes made on this page effective IMMEDIATELY

Load Custom MSG Template: None **Delete Template** **Save Template As:** _____

Send Custom Message No Active custom messages at this time.

Message Type Control
Non EAS custom message

Message Display Control
Repeat custom message payout for a fixed number of times (or until stopped) ▾
Number of repetitions: 3
1 00 Time in min:secs between end of payout and replay.
Mins : Secs
Play audio message with every display repetition ▾
Audio repetition control

Set Message Max Active Duration
Hours 0 Mins 15 ▾

Custom Text Message
Text Test Test

Custom text size = 14.

Read text file: None **Delete Text File**
Save Text to File _____

Audio Messages
Optional Pre-Alert Audio Announcement
No Audio ▾
Convert Text Message to Speech ▾
English Voice: ☒ David(US English) ☐ William(US English)
Test Making Text to Speech Audio File
Optional Post-Alert Audio Announcement
No Audio ▾
[Go to >>> Setup Audio Output Levels](#)

Active CEM Alert

The same **Stop Active Message** button is available for the active alert displayed in the **Alert Events > Active** and **Alert Events > Incoming/Decoded** screens.

Send Alerts **Alert Events** **System** **Setup**

General Alerts One-Button Alert **Custom Message**

Password for user 'Admin' is older than 180 days!

Custom Message Options NOTE: Changes made on this page effective IMMEDIATELY

Load Custom MSG Template: None **Delete Template** **Save Template As:** _____

Send Custom Message

Sending originated custom message with EAS ID 5910!
Remaining event duration: 13 mins 140720550-420750 secs
Test Text Test
Playing message for the first time.
Message will payout for 3 more times unless manually stopped.
Next play at Mon Jan 8 10 24 48 2024 EST
STOP Active Message

Incoming/Decoded Screen – Active CEM Alert

Custom Text Translation for CEM

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.

Optional Station ID criteria

A station ID filter code can be entered in the **Optional Station ID criteria** text field below the **Custom**

CEM Text Translation text field. This will limit action of local access forwarding to those CEM alerts decoded from the **Local Access Forwarding** configuration sub-tab. 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. Click the **Submit Decoder Channels** button once selection(s) have been made. 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. There are five radio buttons to select:

- Play CEM alert with custom translation once
- Repeat CEM alert payout for the defined EAS duration (or until stopped)
- Repeat CEM alert payout until stopped
- Repeat CEM alert payout for a specific duration (or until stopped)
- Repeat CEM alert payout for a fixed number of times (or until stopped)

Each option has one or more sub-options to refine the play-out repetition period and audio. These sub-options are located in the box below the selector radio buttons.

Number of repetitions

For this sub-option, use the text field to enter the number of times the CEM alert is to be replayed.

Time

The **Time in min:secs between end of payout and replay period** interface for Message Display Control options that cause repetition for certain time durations can set the replay period to the time in minutes and seconds between the end of play-out and replay. Use the text boxes to set the desired minutes and seconds.

Audio control/Audio repetition control

The pull-down menu allows selection of none, full, or part of the EAS audio message during the first and repeat payouts.

Custom Message Duration

The **Custom Message Duration in minutes:seconds (30 secs up)** Message Display Control option allows the length of time the CEM is to be replayed. Use the text boxes to set the desired minutes and seconds. This setting defaults to 30 seconds.

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.



Custom Msg Forwarding Screen

NET Decode Custom Message Forwarding

When enabled, this 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.

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.

When **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 pull-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** and **Configure Available FIPS for Alert Origination**.

FIPS Groups Sub-Tab

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 the 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 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?** Select either:

- Yes, delete group.
- No, cancel group deletion!

Edit FIPS Location Group Lists Interface

To edit a new or existing FIPS Group, click the corresponding **Edit** button. Users 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 Groups. Highlight the text and enter a descriptive name for this group of FIPS codes.

Choose FIPS Subdivision

This pull-down menu shows 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:

1. Select one of the **FIPS Subdivisions** options (North, Northeast, West, etc.)
2. Select a **FIPS County**
3. Click the **Add ->** button to add that subdivision to the **FIPS codes** list.
4. Repeat the above steps to add multiple subdivisions of a single county to the **FIPS codes** list. For example, both North Orleans, NY and Northeast Orleans, NY FIPS codes can be added.

Caution: Check to make sure **All** is selected in the **Choose FIPS Subdivision** pull-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.

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 **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 **Choose 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 Selected

FIPS codes 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.

Configure Available FIPS for 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 **FIPS Groups** sub-tab. The interface operates similarly to the edit FIPS group interface.



Configure Available FIPS for Alert Origination Section

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:

1. Select one of the **FIPS Subdivisions** options (North, Northeast, West, etc.)
2. Select a **FIPS County**
3. Click the **Add ->** button to add that subdivision to the **Configured Available Origination FIPS Locations** list.
4. Repeat the above steps to add multiple subdivisions of a single county to the **Configured Available Origination FIPS Locations** list. 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 **Configured Available Origination FIPS Locations** 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.

Configured Available Origination FIPS Locations

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 **Configured Available Origination FIPS Locations** list area.

Remove Selected

FIPS code can be removed from the **Configured Available Origination FIPS Locations** 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: **Manage EAS Code Group Lists** and **Configure Available EAS Types for Alert Origination**.

Manage EAS Code Group Lists
 EAS group lists provide a general tool for specifying EAS code entries for various operations.

Add New EAS Group

1: Name: NY State Codes Use count: 0 Edit Duplicate Group Delete Group
 NYW - BLIZZARD WARNING
 CSM - CIVIL EMERGENCY MESSAGE
 EAM - NATIONAL EMERGENCY ACTION NOTIFICATION
 JFA - FLASH FLOOD WATCH
 10 codes

2: Name: Tests Use count: 0 Edit Duplicate Group Delete Group
 JWP - PRACTICE/TEST WARNING
 EAM - NATIONAL EMERGENCY ACTION NOTIFICATION
 NIC - NATIONAL INFORMATION CENTER
 NPT - NATIONAL PERIODIC TEST
 RMT - REQUIRED MONTHLY TEST
 RWT - REQUIRED WEEKLY TEST
 4 codes

3: Name: Weather Use count: 0 Edit Duplicate Group Delete Group
 ATW - AVALANCHE WARNING
 BZW - BLIZZARD WARNING
 FLA - FLOOD WATCH
 HWA - HIGH WIND WATCH
 SWR - SEVERE THUNDERSTORM WARNING
 TOR - TORNADO WARNING
 8 codes

Manage EAS Code Group Lists Section

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 EAS 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 the 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. The group name can be edited here as well.

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 an EAS Code Group 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?** Select either: **Yes, delete group.** or **No, cancel group deletion!**



EAS Code Groups Sub-Tab with Weather Group open for editing

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 generated 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 code. 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 watch codes
- **Add Tests** – contains all the test codes
- **Add Advisories** – contains all the advisory codes

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 **EAS codes** list area.

Remove Selected

EAS codes 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 an 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 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 **Configured Available Origination EAS codes** list for this group. Make a selection by clicking on the desired code. 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 Origination 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 Origination EAS codes** list area.

Remove Selected

EAS codes can be removed from the **Configured Available Origination EAS codes** list by selecting the

item and clicking the **Remove Selected** button.

Station Setup

The **Station** navigation tab under the **Setup** tab is where station alert originations and alert forwarding settings are located. The origination settings primarily focus on Required Weekly Test settings. The **Station** tab included two standard sub-tabs:

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 station's 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 MultiStation2 or 5.

Send Alerts **Alert Events** **System** **Setup**

Main **Station** Alert Agent Demo/Practice Audio Video/CG Net Alerts Email GPIO Printer Alert Storage Network Time Users

Global Options Simultaneous Station Override 1: Station 1 2: Station 2 3: Station 3 4: Station 4 5: Station 5

[Station 0: DuetNet](#) [Global Auto-Forward Mode](#)

☐ Block Origination and Manual Forwarding during in progress alert announcement
☐ Use separate EAS Station IDs for Origination and Forwarding

Alert Origination

Set One-Button Required Weekly Test (RWT) Duration: 0 Hours 15 Mins

☐ Forwarded alerts halt creation of random Required Weekly Tests (RWT)
☐ Automatically Manage random Weekly Test removal upon airing of alerts
☐ Allow Required Weekly Test to include audio
☒ Front Panel Button generates Required Weekly Test (RWT)
☐ Segmented Alert Origination

Alert Forwarding

Auto Forwarding Active
 NOTE: Each station can override global auto-forward enabled mode, but NOT global manual mode.

☒ Enable Auto-Forward Mode.

☐ Auto-Forward Mode Timer 1 ☐ Auto-Forward Mode Timer 2

Start Time: 00:00 End Time: 23:59 [Weekday](#) Start Time: 00:00 End Time: 23:59 [Weekend](#)

☐ Front Panel Button press releases held alert
☐ Include Required Weekly Test (RWT) original audio during forwarding
☐ Segmented Manual Alert Forwarding

Forwarding Serial Protocols are: XB0B4.CEM5.CEM5.CEM5.CEM5. [Follow link to configure.](#)

Station Setup Screen - MultiStation Mode

Global Options

The **Global Options** sub-tab is divided into two main sections: **Alert Origination** and **Alert Forwarding**. There are two check boxes at the top of the page which allow for additional customization.

Block Origination and Manual Forwarding during in progress alert announcement

Check this box 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 Participant IDs for Origination and Forwarding

This check box enables the user to configure a different EAS Participant ID for the Origination Settings and the Forwarding Settings. These settings are found within the **Setup > Station > Station (1-5)** screen. A valid Plus Package License Key is required.

Alert Origination

This section of the screen allows the user to set One-Button Weekly Test Duration, forward alerts, automatically manage Weekly Test removal, allow weekly tests to include audio, and segment alert origination.

The screenshot shows a window titled "Alert Origination". Inside, there is a label "Set One-Button Required Weekly Test (RWT) Duration:" followed by a text input field containing "0" and a dropdown menu showing "15" with a downward arrow, followed by the text "Hours" and "Mins". Below this are five checkboxes with their corresponding labels: "Forwarded alerts halt creation of random Required Weekly Tests (RWT)", "Automatically Manage random Weekly Test removal upon airing of alerts", "Allow Required Weekly Test to include audio", "Front Panel Button generates Required Weekly Test (RWT)" (which is checked), and "Segmented Alert Origination".

Alert Origination Screen

Set One-Button Weekly Test Duration

Input the duration of the RWT in hours and minutes. The default time is 15 minutes.

Forwarded Alerts halt creation of random Required Weekly Tests (RWT)

Automatically Manage random Weekly Test removal upon airing of alerts

Random Weekly Tests (RWT) remain scheduled regardless of other alerts that air. Check to enable.

Allow Required Weekly Test to include audio

This controls whether the originated Weekly Test (RWT) can be constructed with an audio message. The default is disabled.

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 generates Required Weekly Test (RWT)

Check this box to initiate an RWT using the front panel button.

Segmented Alert Origination

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. Default is disabled.

Alert Forwarding

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 banner at the top of this section indicates the current forwarding state. It will display either "Manual Forwarding Active" (highlighted yellow) or, if the **Enable Auto-Forward Mode** check box is checked, "Auto Forwarding Active" (highlighted green). The same information is also displayed on the individual Station pages.

To enable or disable the Auto-Forward Mode, use the **Enable Auto-Forward Mode** check box beneath the banner.

Alert Forwarding

Manual Forwarding Active
 NOTE: Each station can override global auto-forward enabled mode, but NOT global manual mode.

☐ Enable Auto-Forward Mode.

☐ Auto-Forward Mode Timer 1 ☐ Auto-Forward Mode Timer 2

Start Time: End Time: Start Time: End Time:

☐ Use EAS-Net originating unit station ID when forwarding an EAS-Net received alert
☐ Send EAS-Net source time zone when forwarding an EAS-Net received alert without retranslation
☒ Front Panel Button press releases held alert
☒ Include Required Weekly Test (RWT) original audio during forwarding
☐ Segmented Manual Alert Forwarding

Forwarding Serial Protocols are: OFF. Follow link to configure.

Alert Forwarding Settings Section- Manual Forwarding Active

Manual Forwarding Mode

When manual forwarding is active, the web interface or GPI input contact closures must be used to actively forward any unforwarded alerts from the **Alert Events > Incoming/Decoded** screen.

Alert Forwarding

Auto Forwarding Active
 NOTE: Each station can override global auto-forward enabled mode, but NOT global manual mode.

☒ Enable Auto-Forward Mode.

☒ Auto-Forward Mode Timer 1 **ACTIVATED!** ☐ Auto-Forward Mode Timer 2

Start Time: ☐ Daily ☒ Weekday ☐ Weekend
 End Time: ☐ Daily ☒ Weekday ☐ Weekend

☐ Front Panel Button press releases held alert
☐ Include Required Weekly Test (RWT) original audio during forwarding
☐ Segmented Manual Alert Forwarding

Forwarding Serial Protocols are: XB064.CEMS.CEMS.CEMS.CEMS. Follow link to configure.

Alert Forwarding Settings Section- Auto Forwarding Active

Auto-Forward Mode

During Auto-Forward mode, the EAS device forwards alerts without review or intervention, provided they pass the currently configured Auto-Forwarding criteria.

Forward Mode Timers

All licensed versions feature two Auto-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 on 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 it will go back to Manual mode.

In the screenshot below, Auto-Forward Mode is active from midnight to 6:00am on weekdays and from midnight to 8:00am on Saturday and Sunday.

Alert Forwarding

Manual Forwarding Active
NOTE: Each station can override global auto-forward enabled mode, but NOT global manual mode.

☐ Enable Auto-Forward Mode.

☒ Auto-Forward Mode Timer 1 Not Activated ☒ Auto-Forward Mode Timer 2 Not Activated

Start Time: 0 : 00 Hrs : Mins ☐ Daily ☒ Weekday ☐ Weekend
End Time: 6 : 00 Hrs : Mins

Start Time: 0 : 00 Hrs : Mins ☐ Daily ☐ Weekday ☒ Weekend
End Time: 8 : 00 Hrs : Mins

[Accept Time Changes](#) [Cancel Time Changes](#)

☐ Front Panel Button press releases held alert
☐ Include Required Weekly Test (RWT) original audio during forwarding
☐ Segmented Manual Alert Forwarding

[Forwarding Serial Protocols are: XROB4.CEMS.CEMS.CEMS.CEMS. Follow link to configure.](#)

Alert Forwarding Settings Section- Manual Forwarding Active with Timers

Main

When MultiStation mode is **not** enabled, the **Main** screen provides controls to set the basic values to construct an EAS alert. It contains four sections: **Station**, **Origination**, **Required Weekly Test (RWT)**, and **Forwarding**.

Main Station Alert Agent Demo/Practice Audio Video/CG Net Alerts Email GPIO Printer Alert Storage Network Time Users

Global Options **Main**

Station

Timezone: Eastern Set Origination/Forwarding Station IDs below

Primary Alert Language: English
Extended Alert Languages: English Spanish
☐ Disalt serial/audio/video/stream play out for non-national alerts

GPI Alert Hold: Do not use GPI Alert Hold Optionally designate GPI inputs to hold alerts (until closure or during closure).

[Decoder Languages Duplicate Handling Unstable Policies - Goto Alert Policies page.](#)

Origination

Origination EAS Station ID: Onefret

EAS Origination (ORG) Code: EAS-Broadest Station/Cable System
CIV-Civil Authority
WWS-National Weather Service

☒ Use custom text for origination (ORG) code string
Custom Origination (ORG) Code: A BROADCASTER The phrase "HAS ISSUED" follows this string in the translation
Translation

Non-national alert play scheduling: As soon as possible (default)
Play:

Required Weekly Test (RWT)

Optional Pre-Alert Audio: No Audio Optional. Played before the EAS header audio.
Announcement
Post-Alert Audio Announcement: No Audio Optional. Played after the EAS EOM audio.

EPS Group: weekly_test_1
1, Orleans, NY (036072)

☐ Automatic Random Required Weekly Test Generation

Forwarding

[Manual Global Forward Mode](#)

Forwarding EAS Station ID: Onefret

☐ Retransmit EAS alert text using forwarding station ID and timezone

[Goto Alert Agent Settings page](#) [Goto Alert Agent Policies](#)

Main Sub-Tab Screen

Station**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 alerts through non-streaming Net Alert interfaces. Applies to both Origination and Forwarding.

GPI Alert Hold

Optionally designate GPI inputs to hold alerts (until closure or during closure). This pull-down menu contains three options:

- Do not use GPI Alert Hold
- Designated GPIs Hold alert while Closed
- Designated GPIs Hold alert while Open

When using the last two options, a list of GPIs is available for selection.



Main Sub-Tab – Origination Section

Origination**Origination EAS Participant 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 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. Select the EAS Origination code for your system from the listed options:

- EAS – Broadcast station or cable system
- CIV – Civil authorities
- WXR – National Weather Service
- PEP – Primary Entry Point System (United States Government)

Use custom text for origination (ORG) code string

This setting defaults to 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 this box allows a custom translation to be used instead.

Custom Origination (ORG) Code Translation

When custom text is enabled, a text entry box is displayed in which you can enter the organization name issuing the alert.

In the screenshot above, custom text is enabled and 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

Sets 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 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.

Required Weekly Test (RWT)

Optional Pre-Alert Audio Announcement: No Audio (Optional. Played before the EAS header audio.)

Post-Alert Audio Announcement: No Audio (Optional. Played after the EAS EOM audio.)

FIPS Group: weekly_test_fips (1. Orleans, NY (036073))

☐ Automatic Random Required Weekly Test Generation

Main Sub-Tab – Required Weekly Test (RWT) Section

Required 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** sub-tab (Allow Required Weekly Test to include audio check box).

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

The pull-down list contains created FIPS Codes Groups. Click to select the desired FIPS Codes Group. The FIPS codes within a group will display below the pull-down once a selection is made.

Automatic Random Required Weekly Test Generation

This 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 and end time, in hours and minutes.

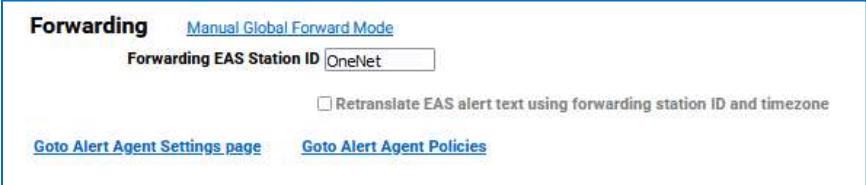
On days

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 the first time is greater than the second time, the alert will be scheduled at a random time from 0 hrs (midnight) to the second time or the 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.

The screenshot shows a software interface for the 'Forwarding' section. At the top, there is a tab labeled 'Forwarding' and a link 'Manual Global Forward Mode'. Below this, there is a text field labeled 'Forwarding EAS Station ID' containing the text 'OneNet'. Underneath the text field is a checkbox labeled 'Retranslate EAS alert text using forwarding station ID and timezone', which is currently unchecked. At the bottom of the section, there are two links: 'Goto Alert Agent Settings page' and 'Goto Alert Agent Policies'.

Main Sub-Tab – Forwarding Section

Forwarding

Forwarding EAS Participant 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.

Retranslate EAS alert text. Use forwarding station ID and timezone

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)

The 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.

Send Alerts **Alert Events** **System** **Setup**

Main **Station** Alert Agent™ Demo/Practice Audio Video/CG Net Alerts Email GPIO Printer Alert Storage Network Time Users

Global Options **Simultaneous Station Override** 1:Station 1 2:Station 2 3:Station 3 4:Station 4 5:Station 5

Override Station 5 Stations: 0 Enabled

Timezone: Eastern Set Origination/Forwarding Station IDs below

Primary Alert Language: English ▼

Extended Alert Languages: English, Spanish

☐ Omit serial/audio/video/stream play out for non-national alerts

GPI Alert Hold: Do not use GPI Alert Hold ▼ Optionally designate GPI inputs to hold alerts (until closure or during closure).

[Decoder Languages, Duplicate Handling, Update Policy, etc - Goto Alert Policies page.](#)

Origination

Origination EAS Station ID: OneNet

EAS Origination (ORG) Code: EAS-Broadcast Station/Cable System, CIV-Civil Authority, WXR-National Weather Service

☒ Use custom text for origination (ORG) code string

Custom Origination (ORG) Code: A BROADCASTER The phrase "HAS ISSUED" follows this string in the translation

Non-national alert play scheduling: As soon as possible (default) ▼

Required Weekly Test (RWT)

Optional Pre-Alert Audio Announcement: No Audio ▼ Optional. Played before the EAS header audio.

Post-Alert Audio Announcement: No Audio ▼ Optional. Played after the EAS EOM audio.

FIPS Group: weekly_test_fips ▼

1. Orleans, NY (036073)

☒ Automatic Random Required Weekly Test Generation

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: 0 : 00 and Time: 0 : 00

Mon : Mon Tue : Tue Wed : Wed Thu : Thu Fri : Fri Sat : Sat

On days checked days are candidates for RWT, unchecked days are omitted (effective immediately).

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Forwarding [Manual Global Forward Mode](#)

Forwarding EAS Station ID: dasdec

☒ Retranslate EAS alert text using forwarding station ID and timezone

☒ Use custom ORG text substitution if alert ORG Code is EAS

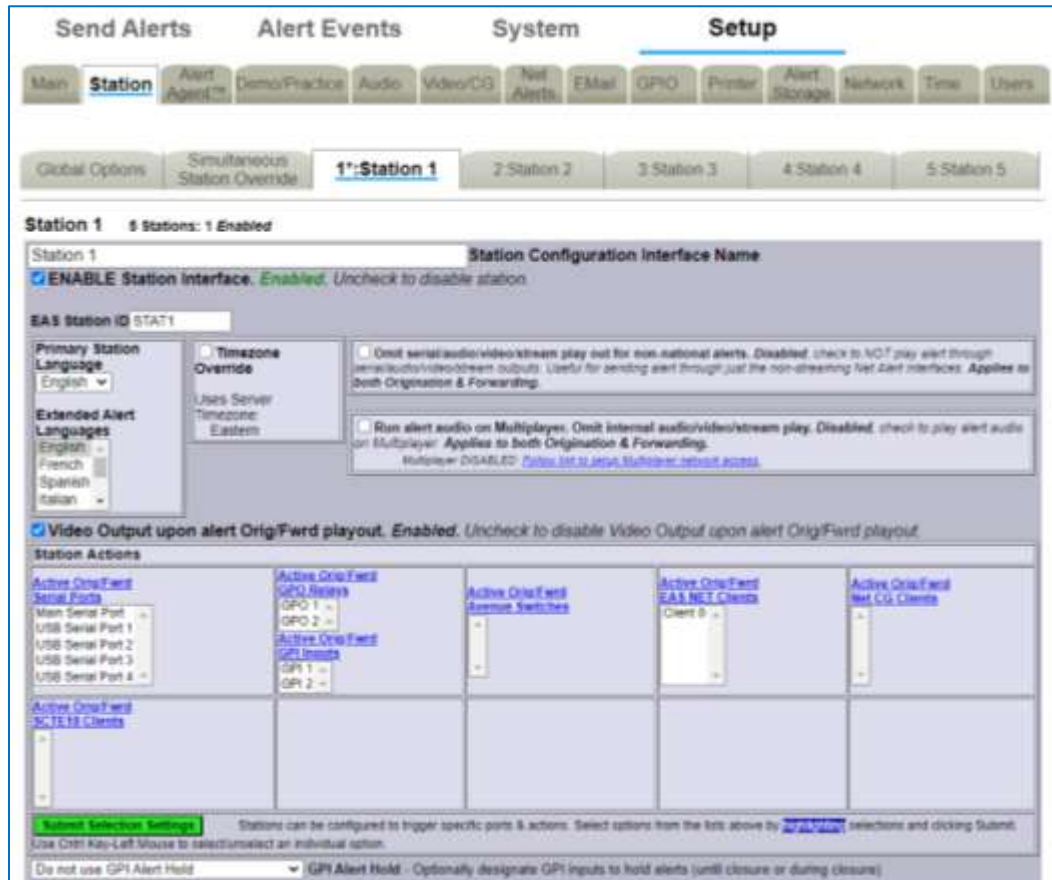
Custom Forwarding EAS ORG Code substitution: THIS BROADCASTER The phrase "HAS FORWARDED" will follow this string in the translation.

[Goto Alert Agent Settings page](#) [Goto Alert Agent Policies](#)

Simultaneous Station Override Screen

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 **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. **Required Weekly Test (RWT)** settings are only available in this sub-tab if every station sub-tab is disabled.



Station Sub-Tab Configuration Screen – Top Portion

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 a configuration for each channel individually. All **Station** sub-tabs contain three sections: Station Configuration, Origination Settings, and Forwarding Settings.

Station Configuration

Station Configuration Interface Name

This text field 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/disables the station interface for this sub-tab. Checking it will make the following

configuration settings active:

EAS Participant 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.

Timezone Override

MultiStation mode allows stations in differing time zones to be configured in the same EAS unit. The default setting is the same time zone that was configured in the **Setup > Time** screen. To change to a different time zone, check the box and select the desired time zone from the **Region** and **Zone** pull-down menus. Click the **Submit Timezone Setting** button to save the setting.

Primary Station Language

Use this pull-down menu 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 an alert through serial/audio/video/stream outputs. Useful for only sending alerts 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 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 Settings** button. Multiple selections can be made by using the CTRL key when making selections.

Station Sub-Tab Screen – Origination Settings

Origination Settings

The Origination settings are exactly the same as in the **Simultaneous Station Override** sub-tab, 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** button. 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.



Station Sub-Tab Screen – Forwarding Settings

Forwarding Settings

The Forwarding settings are exactly the same as in the **Simultaneous Station Override** sub-tab, with the exception of the **Forwarding Audio Output Devices** settings.

Forwarding Audio Output Devices

A list of available forwarding audio output 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** section.

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** screen. (See [Chapter 6 - Incoming/Decoded](#) 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, as well as FIPS codes and audio for the DMO alert.

The screenshot shows the 'Setup' tab of the software interface. The 'Demo/Practice' sub-tab is active. The main configuration area includes:

- Allow DEMO Decode/Forwarding Test:** Enabled, unchecked to Disable. Below this, it says 'Set FIPS locations for One-Button DEMO Test. For each Location, Select a FIPS, then Add Selected FIPS'. A list of FIPS codes is shown: Oregon.NY (030073), New York (036000), Genesee.NY (036037), and Livingston.NY (036051). The 'New York (036000)' entry is highlighted in orange. An 'Add Selected FIPS' button is at the bottom of the list.
- Current FIPS locations for One-Button DEMO Decode/Forwarding Test:** A table showing 'All' in a dropdown menu and 'New York (036000)' in a text field, with a 'Remove' button.
- Roll EAS station IDs three times:** Enabled, unchecked to Disable. A note states: 'You are limited to 3 Demo alerts per minute.' Below this are two checkboxes: 'Preempt an in-progress alert announcement as a test' (unchecked) and 'When DMO event is forwarded, forward live and bypass criteria (like an EAN,NPT), to simulate national live alert operation' (unchecked).
- Select Alert Audio Message:** This optional audio is played after the EAS header and attention signal audio, and before the EOM audio. The dropdown menu is set to 'No Audio'.
- EAS Origination (ORG) Code:** A list with 'EAS-EAS Participant', 'GPH-Grail Authority', and 'WOUR-National Weather Service'.

At the bottom, there is a link: 'To Run Demo alert goto Alert Events Incoming/Decoded Alerts.' and a footer: 'Please Refresh Top Start First DEMO Disable Demo/Practice Audio Out by Weather Set test (used where) Update (FIPS) EASMET CAP Alerts test by Demo All OK! Digital Alert Systems, Inc. All rights reserved. 2005'.

Demo/Practice Configuration Screen

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 offline during practice.

Allow DEMO Decode/Forwarding Test

When enabled, the **Add Demo Decoded Alert** button is available on the **Alert Events > Incoming/Decoded** 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 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 (Central Pacific Ocean 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 Participant IDs three times

When checked, the EAS Participant ID will roll three times. If left unchecked, the EAS Participant 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) to simulate national live alert operation

When enabled, a national live alert will be simulated. This setting requires Administration-level permission to enable. All other users will see grayed text.

Select Alert Audio Message

This pull-down menu 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 and preview audio files go to Setup Audio Outputs** is provided to go to the **Setup > Audio > Audio Outputs** screen. Here users can upload and listen to the available audio files (See the [Audio Setup](#) section of this document).

EAS Origination (ORG) Code

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.

A hyperlink labeled **To Run Demo alert go to Alert Events Incoming/Decoded Alerts** is provided to go to the **Incoming/Decoded** screen within the **Alert Events** tab. Demo/Practice alerts may be added and forwarded from this location.

Net Alerts Setup

There are up to seven 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. This option only appears when the license is installed.
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 unicast or multicast an MPEG2 video/audio details page. Added support for D2D audio only streaming. 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.

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 > Main > Main/License**. (See the [Setup > Main > Main/License section](#) of this document) License keys may be purchased from Digital Alert Systems.

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**.

DVS168

The DVS168 sub-tab provides an interface to a single DVS-168 client. If the DVS168 sub-tab is available, use this screen to enable this protocol for forwarding and/or sending alerts.

The screenshot shows the 'DVS168' sub-tab interface. At the top, there are tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs: 'Main', 'Station', 'Alert Agent™', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts' (selected), 'Email', 'GPIO', 'Printer', 'Alert Storage', 'Network', 'Time', and 'Users'. Below these, there are buttons for 'DVS168', 'CAP Decode', 'DVS644 (SCTE18)', 'Stream MPEG', 'Net CG', 'Net Switch', and 'Net GPIO'. There are also 'Accept' and 'Cancel' buttons. The main content area has two checked options: 'Alert Forwarding to DVS168/EARS device. Enabled. Uncheck to disable.' and 'Encoder Originated Alerts Sent to DVS168/EARS device. Enabled. Uncheck to disable.' Below this is a section titled 'Configure DVS168/EARS Client Connection (client network connection values apply to both Origination and Forwarding)'. It contains a 'DVS168/EARS client 1 connection info' box with fields for 'DVS168/EARS FTP User', 'Set DVS168/EARS FTP Password (Not set)', 'DVS168/EARS Server IP Address', 'DVS168/EARS Server Port (default is 4098)', 'Audio File Sample Size' (16 Bits/Sample), and 'Audio File Sample Rate' (16000 Sample/sec). There is also a checkbox for 'Send alert text for Live alerts (EAN,NPT). Disabled. NOT sending alert text for EAN,NPT is the Normal Model! Check to FTP the alert text to DVS168/EARS device. Used to for Evertz DVS168 compatible equipment.' and a note about 'Forced EAT-EOM mode: Send DVS168 EAT-EOM at end of EAN,NPT live alerts (provides Cisco DNCS an end force tune command).'

DVS168 Sub-Tab Screen

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 option is checked.

Encoder Originated 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.

Configure DVS168/EARS Client Connection

Once forwarding and/or sending have been enabled, four information fields must be configured to identify the DVS-168/EARS host. (See the above screenshot.) Enter the DVS168/EARS FTP User and DVS168/EARS FTP Password, the DVS168/EARS Server IP address, the DVS168/EARS Server Port, select an Audio File Sample Size, and the Audio File Sample Rate (default is 16000 Sample/sec).

All FIPS codes trigger

Alerts with all FIPS codes can be forwarded by placing a check mark in the All FIPS codes trigger check box. Alerts with any FIPS locations will trigger the DVS168/EARS device. Alerts for specific FIPS areas can also be filtered/passed through the protocol.

Remove the check mark from the All FIPS codes trigger check box 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 DVS168 client.

All EAS codes trigger

Alerts with all EAS codes can be forwarded by placing a check mark in the All EAS codes trigger check box. Alerts with any EAS code will trigger DVS168/EARS send. Digital Alert Systems Version 5.1 Software User's Guide Revision 1.0 139

Remove the check mark from the All EAS codes trigger check box 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

The EAS Net sub-tab provides an interface to a single DVS-168 client. If the **DVS168** sub-tab is available, use this screen to enable this protocol for forwarding and/or sending alerts. There are three sections on the EAS NET sub-tab: EAS NET Decoding, EAS NET Web audio streaming, and EAS NET Clients.

EAS NET Sub-Tab

EAS NET Decoding

EAS Net Decoding is included with the EAS NET license key.

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 differences depending on the chosen EAS NET protocol:

- **SSH STDIN Only**- does not offer the 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.

There is only one check box to enable EAS NET decoding. 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** 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.

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 screenshot below.

EAS NET Web audio streaming. Changed Settings are not effective until Accept Changes is pushed.

☒ **EAS_NET Web (HTTP) Alert Audio streaming during alerts.** Enabled. Uncheck to disable.

Stream address of 1st network interface: <http://192.0.0.214:8000/liveeas.ogg>

For streaming Live alerts (EAN,NPT) audio to a remote DASDEC™ or OneNet™ EAS Net decode channel, the required settings in this interface are OGG format, no EAS header and EOM sequences, and Live alerts only; the preferred settings are no auto-delay, 0 sec delay, 1 seconds start silence, 1 second ending silence. Also, make sure EAS NET interfaces are configured to send audio files if only Live alerts stream audio.

☐ Audio streaming on all alert types. Disabled. Streaming is only enabled for Live alerts (EAN,NPT). Check to enable streaming for all alerts.

☒ OGG/Vorbis ☐ MP3 Audio Stream Format (remote EAS NET Decoder requires OGG/Vorbis)

16000 Sample/sec ▼ Streamed Audio Output Sample Rate This setting should equal the target server.

☐ Pre-alert audio/alert header/attention inclusion at start of audio stream. Disabled. Check to enable.

☐ Auto stream startup delay by duration of Alert header sequence. Disabled. Check to enable.

***Alert message audio, if available, is always included in the stream.

☐ Alert EOM audio streaming. Disabled. Check to enable.

5 Delay time before stream start (0-90 seconds). Auto stream startup delay adds to this duration. Set long enough to compensate for remote encoder latency.

3 Starting silence duration before audible audio (0-90 seconds). This can also be used for some latency compensation.

1 Ending silence duration, after audible audio finishes, until stream is ended (0-120 seconds).

EAS NET Web Audio Streaming Enabled 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 types** can be enabled to allow all alert types to have audio streaming. Make sure to use this option to test live audio for any remote EAS device/EAS NET decoder.

Audio Stream Format

You can select either the **OGG/Vorbis** or **MP3** audio radio button, including streaming audio to a remote EAS device/EAS NET decoder.

Streamed 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 from the pull-down menu. Choices are 16000, 32000, 44100, and 48000 samples/sec.

Pre-Alert audio/alert header/attention inclusion at start of audio stream**Audio stream startup delay by duration of Alert header sequence****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 before audible audio****Ending silence duration, after audible audio finishes, until stream is ended**

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.

EAS NET Clients

Two check boxes are displayed for enabling EAS_NET during alert forwarding and origination. A third check box can enable EAS_NET during alert decoding.

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.

EAS NET Clients Section – Top Portion

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 the **Delete this EAS_NET interface** button.

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 be 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).

Various information fields must be configured to identify and correctly communicate with 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.

Enable Client Interface

This check box enables or disables the EAS NET client.

EAS NET Event Send Options

To decode the EAS NET Event Send Options requires the Decoded Alerts Master Switch.

Use the pull-down menu to select EAS NET Event Send options.

EAS NET Event Send Options (decode send options require Decoded Alerts Master Switch)

- ☐ Disabled. Client syncs EAS NET alert info send with alert audio payout.
- ☐ ET compatible equipment that requires sync with alert audio payout via GPI control or Extended Status Play control. Prior send is required!
- ☒ EAS NET Client forwards Live alerts (EAN,NPT). Uncheck to disable Live alert forwarding.

EAS NET Event Transfer Protocol

Secure Copy ☐ Remote EAS NET Host Port

☐ Follow Network > Security HTTPS setting for local URI references. Presently local URI references will only use http://
First (Main) Ethernet w/ Local network device (provides return IP address).

EAS NET Event Send Options Pull-Down Menu

☐ **EAS NET only at Fxwd or Only (sent Decade send)** ☐ **EAS NET Event Send Options** (decade 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 OPI 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:

Remote Host Address
(name if DNS enabled or dot address)

22 **Remote EAS NET Host Port**

☐ **Follow Network->Security HTTPS setting for local URI references.** Presently local URI references will only use http.

Local network device (provides return IP address)

☒ **Automatic internal connection test every 5 minutes.** Enabled.

(allow any config changes before using Test button)

(if sending to CALDEC, preferred user name is dsladmin_netel)

[Follow this link to find SSH Public Encryption Key.](#)

Current Schema Default

See schema for target paths and names of data files.

EAS NET Event Send Options Screen

Send EAS Net Prior to alert audio playout

Use this check box to enable EAS NET alert info to send prior to alert audio playout.

Live alerts (EAN,NPT) EOM Options

Use this check box to enable this EAS NET client to forward Live alerts, or uncheck to disable Live alert forwarding. This section of the EAS NET screen provides a pull-down menu with the following two options:

- Forced EAT-EOM Mode

- Basic EOM mode

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).

Basic EOM mode: Send DVS168 EOM at end of EAN,NPT live alerts.

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 (Save any config changes before using Test buttons)

☐ Alert file FTP. Check to disable alert file FTP to DVS168/EARS device.

LIVE Alert (EAN,NPT) EOM options

Event Data IP Control Options

This section of the screen allows the user to control the Event IP information entered into the system.

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 (Save any config changes before using Test buttons)

☐ Alert file FTP. Check to disable alert file FTP to DVS168/EARS device.

Event Data IP Control Options Section

Remote EAS NET Host IP Address

Enter the remote EAS NET Host IP address into this field.

Remote Host Address

Use to Name if DNS enabled or dot.decimal.

Remote EAS NET Host Port

Enter the port number of the remote EAS NET Host port.

Automatic Internal Connection test every 5 minutes

Use this checkbox to enable the system to automatically test the internal connection every 5 minutes.

Test Connection

SAVE any configuration changes BEFORE using the Test connection button!

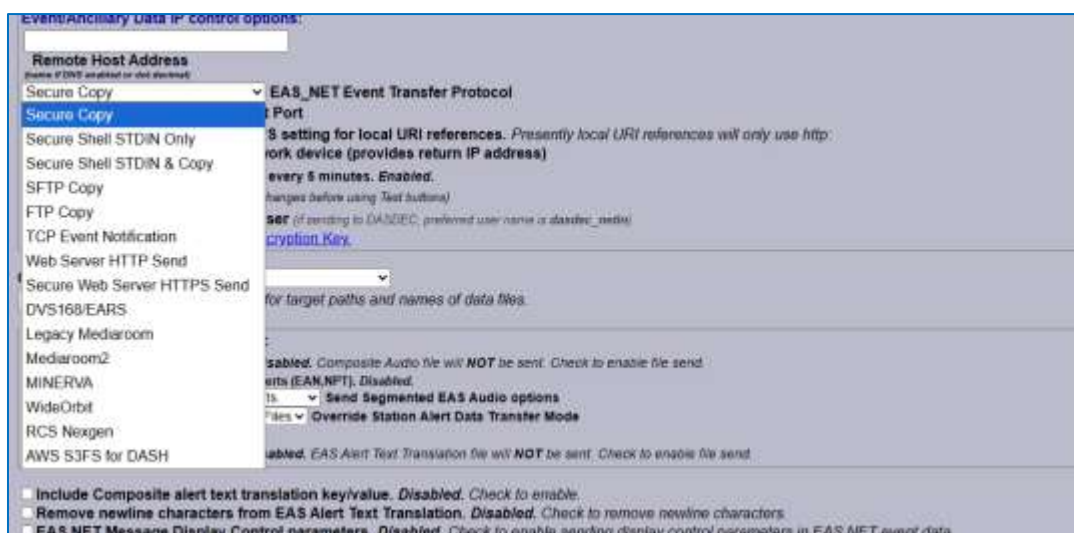
Click the check-box to test the connection.

EAS_NET User

Enter the EAS_NET User in the provided text box. If sending to DASDEC, the preferred username is dasdec_netin.

EAS_NET Event Transfer Protocol

This pull-down menu will display the event transfer protocol options (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 a password, others use encryption keys. Most provide for optional data file connections.



EAS_NET Event Transfer Protocol Screen Mid-Section

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 the **Secure Shell STDIN Only (SSH)** protocol above. The event file is sent as in that protocol, 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.
- **SFTP Copy – Secure File Transfer Protocol (SFTP)**
- **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 **Non-Passive, regular FTP port connection** 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 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.

- **Web Server HTTP Send**
- **Secure Web Server HTTPS Send**
- **IPAWS Open 2**
- **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.
- **AWS S3FS for DASH** – EAS_NET Event Transfer Protocol needs to be set to AWS S3FS for DASH. This will make the heartbeat options appear.

Setting Local URI References

Use the **Setup > Net Alerts > EAS NET** screen to set local URI references.

Send Alerts Alert Events System **Setup**

Main Station Alert Agent™ Demo/Practice Audio Video/CG **Net Alerts** EMail GPIO Printer Alert Storage Network Time Users

Password for user 'Admin' is valid for 180 days!

EAS NET CAP Decode DVS644 (SCTE18) Stream MPEG Net CG Net Switch Net GPIO

☐ Common Alert Protocol (CAP)
 ☐ PureCAP™ - Source CAP File
 ☐ PureCAP™ Plus - Embedded Source CAP File
 ☐ Advanced Emergency Alerting Table (AEAT) Container

☐ EAS NET only at Privet 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.*

Event/Ancillary Data IP control options:

Remote Host Address
(leave if DNS enabled or disdecimal)
☐ Secure Copy ☐ EAS NET Event Transfer Protocol
 22 Remote EAS NET Host Port

☒ Follow Network->Security HTTP5 setting for local URI references. *Presently local URI references will only use http.*
☐ First (Main) Ethernet ☐ Local network device (provides return IP address)

☒ Automatic internal connection test every 5 minutes. *Enabled.*
 (Save any config changes before using Test buttons)

EAS NET User (if sending to DASDEC, preferred user name is dasdec_user)
[Follow this link to find SSH Public Encryption Key.](#)

Current Schema SFTP-test

[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.*

[Back](#) [Refresh](#) [See Red](#) [Stat](#) [Send](#) [GPIO](#) [OnLog](#) [SessionLog](#) [Audio Out to Radio \(MP\)](#) [NetNet Usenet Policy \(Global\)](#) [GPIO \(EASNET CAP Alerts Sent to Decode All\)](#) [RWT](#)
 Digital Alert Systems, Inc. All rights reserved. 2020

Setting Local URI References

Follow Network > Security HTTPS setting for local URI references

Use this check-box to follow the Network > Security HTTPS setting for local URI references. Presently local URI references will only use HTTP.

Local network device (provides return IP address)

Use the pull-down menu to select the appropriate Ethernet device: First (Main) Ethernet, 2nd Ethernet, 3rd Ethernet, 4th Ethernet.

CAP field string:

- CAP (sender) field string (set to name of sender or agency, no whitespace, if empty hostname@IPADDR is substituted).
- CAP (source) field string (set to name of sender, if empty EAS Station name is substituted).
- CAP (senderName) field string (set to name of alerting agency, if empty EAS Station name is substituted, for NWEM must be formatted as "name,city,state").

To set local URI references:

1. Click on **Follow Network > Security HTTPS settings for local URI references**.
2. Click on **Setup > Network > Security**.
3. In the **Web Interface Security** section of the screen, click on **Check to only allow HTTPS secure access to this platform. Effective Immediately!**
4. Click on **Enhanced HTTPS SSL Strength. Effective Immediately!**
5. Select the **Web Interface SSL (HTTPS) Certificate** from the pull-down menu.

Setting **AWS S3FS for DASH** in the **EAS_NET Event Transfer Protocol** to display the heartbeat options. DASHS3FS provides an option for date/time \$(macro) expansion in GM (UTC) time

3rd Party Ancillary Data File Control Options

Use the pull-down menu to select the EAS NET Data File Transfer Protocol from the following menu options:

- Secure Copy
- SFTP Copy
- FTP Copy
- TCP Copy
- None

EAS_NET Host Data File IP Address

This field is optional, however, if undefined main EAS NET Host IP address used.

Remote EAS NET Host Data Port

Enter the port number for the remote EAS NET data port.

Remote Host User

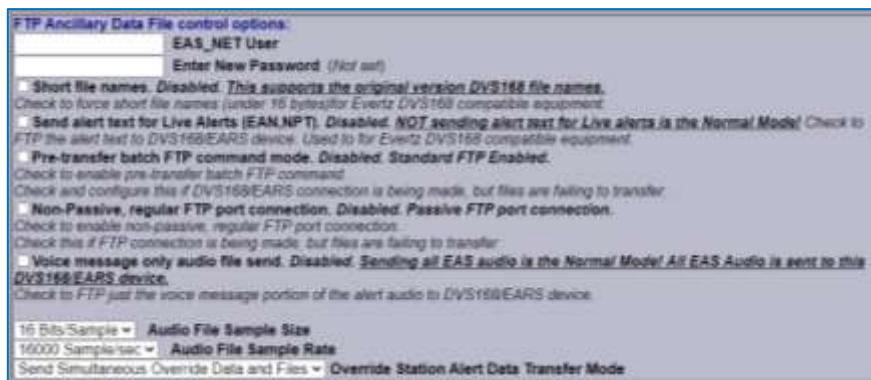
Follow this link to find SSH Public Encryption Key.

Add Digital Signal to Sent CAP Alert

Use check-box to enable/disable the add the digital signal to the sent CAP Alert. This requires a PEM Certificate.

Remote EAS NET Host Port

This field displays the port on the remote EAS NET host where the EAS NET event info is sent.



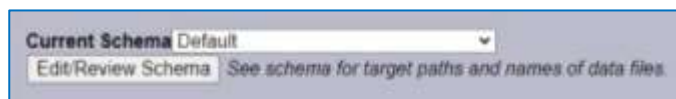
FTP Ancillary Data File Control Options Section

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.



Current Schema Section

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.

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 Source
 weekly_test_fips
 Others,NY (316070)
 United States (000000)
 2 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 Source
 all

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 a single asterisk (*) meaning any station ID, up to 8 character each, requires each source
 EAS station ID with a letter, eg. 123456789 to the last 7 (240 station specified 2474
 0123456). The (*) character matches all 101 and 2400000.

Do not use GPI triggers GPI Trigger - Optionally designate GPI inputs/status required to use this net interface.

Note: system paths and names in EAS_NET can include text substitution patterns.
 \$DD\$ is replaced with the alert ID. \$EAS\$ is replaced with the 1 letter alert EAS code. \$EASID\$ is replaced with the Simultaneous Override
 Encoder Station ID name. \$EASID\$ is replaced with the Multicaster Encoder Station ID name. \$EASID\$ is replaced with the alert Station
 number. For example, 1.5 for Multicasting, 20000 For Audio-Only only. \$DAY\$ is replaced by the Audio-File extension. (eg. use 12 for 12PM, 3PM
 and 5PM). \$TIME\$ is replaced with the current year. \$MM\$ and \$DD\$ are replaced with the current month and day. (\$MM\$ and \$DD\$ are
 replaced with a leading 0 if < 10). \$MM\$ (\$DD\$) are replaced with the current hour,minute, and seconds (each with leading 0 if <
 10). \$LANG\$ is replaced by language name.

Accept Changes Cancel Changes

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 screenshot this option is disabled. Select 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 code group from the **FIPS Group** pull-down menu. That group of FIPS codes is 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 the **Accept Changes** button to save the configuration.

DVS168/EARS Devices

DVS168/EARS can be selected as an option in the **EAS_NET Event Transfer Protocol** pull-down menu. See the screenshot below. Like the other EAS NET protocols, the **Remote EAS NET Host IP Address** and **Remote EAS NET Host 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 User** and **EAS_NET Password** value must also be entered for a standard client configuration. However, there is an option to disable the FTP send. Use the **Alert File FTP** check box to enable/disable this function. 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.

EAS NET DVS168/EARS Client Section

Two other options unique to the DVS168 protocol are also provided.

- **Voice message only audio file send:** Use this check box to send just the EAS alert audio message, instead of the EAS FSK header and EOM audio, and attention audio. Before using this option, it is important to make sure your local EAS plan allows the FSK audio to be discarded.
- **DVS168 4-byte Duration Format:** Alert duration data format, typically in minutes. Some DVS-168 interpreters have coded this differently. The pull-down menu provides two other interpretations, Hours:Minutes and Seconds.

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 Factor**, 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. A control message is then 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 Nationwide Test 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-tab: Common Alerting Protocol (CAP) decode and CAP server configuration.

CAP Decode Sub-Tab

Common Alerting Protocol (CAP) decode

This check box enables or disables CAP decoding for the EAS device. When enabled, all of the available options for CAP Decoding are visible. Checked is enabled, unchecked is disabled.

This section of the screen provides hyperlinks to the following information:

- See all CAP messages
- See all EAS from CAP messages
- See errored CAP messages

View Global CAP options

This section of the web interface deals with logging and XML file handling. Checked is enabled, unchecked is disabled.

Logging Options

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 troubleshooting purposes.

CAP Server Configuration

CAP Server Configuration Section

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 CAP Client Interface

Duplicate CAP Client Interface

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 to enable the configured or new client to become active to EAS NET CAP Alerts.

CAP Poll Protocol

This pull-down menu provides a list of the CAP Poll Protocol options.

CAP Poll Protocol Pull-Down Menu

Choose between HTTP, HTTPS, SSH and the IPAWS Open 2.0 option from the pull-down menu.

- **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.
- **CAP Canada IP Get** – All CAP alerts polled are delivered using HTTPS protocol. Canada CAP decoder uses HTTPS for CAP file download.
- **CAP Caribbean Get** – Protocol used when located in the Caribbean.

Under each of these 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 these 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 IPAWS 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 the Server Network Configuration section at **Setup > Network** to change your DNS options or use the hyperlink.

URL path

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 wait 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.

Connect to IPAWS CAP Server

To quick connect to the FEMA CAP Server, create a new client and follow the options in the screenshot that follows the procedure.

1. Navigate to the **Setup > Net Alerts > CAP Decode**
2. Ensure DNS is enabled (**Setup > Network > Configuration**)
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** text field (i.e. IPAWS)
5. Select **IPAWS Open 2.0 Get** from the **CAP Poll Protocol** pull-down menu.
6. Enter the following data 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-04-14-2024.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu.
8. Select the desired FIPS Group from the **FIPS Group** pull-down menu.

(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 if the EAS device is connected. Green text under the **Poll CAP from IPAWS Open 2.0 Server** section header should read, in green, **✓ Connected**.

CAP server configuration

2 **DNS is Enabled** (192.0.0.11) 3

4 **IPAWS CAP Select CAP input client
There are 4 user allocated client interfaces (max is 10).
Decode Channel: 'CAP4'

5 IPAWS Open 2.0 Get CAP Poll Protocol

10 Poll CAP from IPAWS Open 2.0 Server.
Waiting for connection status.

6 https:// apps.fema.gov / ipawsopeas_service/rest/update
CAP IPAWS server host address URL path
(DNS must be enabled; eg apps.fema.gov) (Do NOT begin with http(s)://webate.net/. Just the path (eg: cap/alerts.xml), without a leading / character. If a dynamic date and time is required in the URL, see notes below.)

7 View Advanced Options (unchecked to remove view).
Pin Type: Preassigned IPAWS Pin (selected), User configurable Pin, No Pin
Use Secure connection: Enabled (checked), Unchecked to use non-secured connection.
Ignore SSL certificate checking: Presently SSL certificates must verify. Check to ignore certificate.
Optional Text to append to URL:
Accept unsigned alerts: Enabled (checked), Unchecked to reject unsigned alerts.
Accept unverifiable signed alerts: Enabled (checked), Unchecked to reject unverifiable signed alerts.
XML Digital Signature Certificate Authority (CA) Name (upload below): IPAWS_Valid-until-04-14-2024.c (selected), CA Information, Delete CA file

8 Poll Interval in seconds: 60
Assigned Station ID: IPAWSCAP
Log blocked CAP alerts: Enabled (checked), Unchecked to disable.
Adhere to Strict IPAWS CAP to EAS translation: Enabled (checked), Unchecked to disable.
Process CAP <status>Test messages as <status>Actual. For lab testing purposes only!
Process CAP <status>Exercise messages as <status>Actual. For lab testing purposes only!
CAP Text Message to Speech when CAP alert audio not available: Disabled (checked), Check to enable.
CAP alerts with any FIPS codes will be converted to EAS. Disabled. Screen to specific FIPS Codes (EAN,NPT with FIPS 000000 override). Check to enable all FIPS codes.
FIPS Group: weekly_test_fips (selected), Orleans,NY (036073) 1 locations
CAP alerts with any EAS code will be converted to EAS. Disabled. Only specific EAS Codes processed (EAN,NPT always processed). Check to enable all EAS Codes.
EAS Group: All (selected)
Allow CAP SAME EAS code extensions to be converted to EAS. Disabled. Only FCC recognized EAS Codes processed. Check to add extended EAS Codes.
Screen EAS/CAP alerts by COG addresses. Disabled. All alerts are processed. Check to specify COG addresses.

9 Accept Changes Cancel Changes

Connect to IPAWS CAP Server Settings Screen

Connect to NAAD CAP Server (CAP Canada) (Cap Canada must be enabled)

To quick connect to the Canadian **National Alert Aggregation and Dissemination** (NAAD) system server, create a new client and follow the options below, similar to those in the above screenshot.

1. Navigate to the **Setup > Net Alerts > CAP Decode**
2. Ensure DNS is enabled (**Setup > Network > Configuration**)
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 **streaming.alertready.ca** in the **CAP Canada NAAD server host address** text field.
7. Enter **8443** in the **CAP server host port number** text field
8. Enter **cap.alertready.ca** in the **NAAD previous alert download host name** text field.
9. Select **Pelmorex-digicert-verisign-symantic-ENVCan-CA.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu.

10. Click the **Accept Changes** button.
11. Check to see if the EAS device is connected. Green text under the **Poll Canada CAPCP from NAAD IP Server** section header should read **✓ Connected**.

Note: The system has been updated to use https for CAP Canada CAP decoder file download.

Bahamas and Anguilla

The **CAP Poll Protocol** in the preceeding screen capture provides a pull-down menu option for Bahamas and Anguilla.

Added FIPS mapping for Bahamas and Anguilla. (**Setup>Net Alerts>CAP Decode**).

The Bahamas uses the same EAS code LAE in alerts to support filtering and downstream equipment triggering.

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 Alert 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 DVS644/SCTE18 clients. In the screenshot below, the Encoder Originated Alerts 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 allows the audio to be delayed so as to synchronize the audio and video content. The Audio Delay setting is found in **Setup > Audio > Audio Outputs** at the bottom of the screen – **Alert Audio Delay**.

DVS644/SCT18 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 DVS644 (SCTE18) Client Interface

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.

Duplicate DVS644 (SCTE18) Client Interface

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.

Delete this DVS644 (SCTE18) Interface

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.

Client Interface Configuration

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.

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 Address
5050 Remote Host Port
0 Multicast TTL (0..200)

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

☐ **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 = 0 seconds.
0 Duration Extension Time (seconds).
Alert Duration == Audio Duration + Extension Time
(max total is 120 seconds)

☐ **NPT initial duration 120 secs.** Disabled.
Will be 0 like EAN.

☒ **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.

Accept Changes Cancel Changes

DVS644/SCTE18 Client Interface Configuration Section

Various information fields must be configured to identify and correctly communicate to the DVS644/SCTE18 client. The basic fields are the **Remote Host Unicast or Multicast IP Address** and **Remote Host Port**. Enter these addresses according to the specific DVS644/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 is a standard MPEG2 Transport Stream. Use the check box 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 it can be set lower if needed.

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 DVS644/SCTE18 message is made.

The DVS644/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 TVs. The ultimate target for the DVS644/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 Video/Audio OOB ID** or the **Details InBand Major/Minor 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 InBand 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 Counter Options

Each MPEG2 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 MPEG2/SCTE18 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 MPEG2/SCTE18 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 not reset Continuity Counter

The CC will always increment appropriately and will not be forced to a value of zero (0).

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. Enabled. Uncheck to disable.				
Add Exception Channel Entry				
1. VROC_1	☒ In-band, Enabled. Uncheck to enable Out-of-Band	8	1	Remove
2. VROC_2	☒ In-band, Enabled. Uncheck to enable Out-of-Band	9	2	Remove
3. VPEC_1	☒ In-band, Enabled. Uncheck to enable Out-of-Band	10	1	Remove
4. VPEC_2	☒ In-band, Enabled. Uncheck to enable Out-of-Band	10	2	Remove
5. VPEC_3	☒ In-band, Enabled. Uncheck to enable Out-of-Band	10	3	Remove
6. VSNAP_1	☒ In-band, Enabled. Uncheck to enable Out-of-Band	13	1	Remove
7. VSNAP_2	☒ In-band, Enabled. Uncheck to enable Out-of-Band	13	2	Remove
8. VSNAP_3	☒ In-band, Enabled. Uncheck to enable Out-of-Band	13	3	Remove
9. VVCI_1	☒ In-band, Enabled. Uncheck to enable Out-of-Band	21	1	Remove
10. VVCI_2	☒ In-band, Enabled. Uncheck to enable Out-of-Band	21	2	Remove
11. VVCI_3	☒ In-band, Enabled. Uncheck to enable Out-of-Band	21	3	Remove

Exception Channel List Section

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 4E)
 Audio/Video Stream Source ISMPv3 IP Address (optional)
☐ Input Port options. Disabled. Check to enable Input Port Options.

MPEG Audio Sync Private Descriptor Section

MPEG Audio Sync Private Descriptor (Tag=0xE1)

Check to enable the MPEG Audio Sync Private Descriptor - a special private descriptor for syncing an 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 (Tag=0xE8)

Check to enable the NDS Tune Private Descriptor method - a special private descriptor for syncing an 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.

The screenshot shows a configuration window titled "Set Alert type priority selection". It includes a list of priority levels on the left: Low:3 (Advisories), Low:3 (Tests), Low:3 (Watches), Medium:7 (Warnings), High:11 (Emergencies), and Highest:15 (National Test). Below this is a checkbox for "NPT initial duration 120 secs. Disabled. Will be 0 like EAS". On the right, there are several checkboxes: "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 Repeat Control", "Alert Message Transmission Duplication Count (1-30)", "Additional Start Delay Time (seconds)", "Start Delay == (Audio Delay if enabled) + Additional Time DVS644/SCTE 18 message send delay time = 3 seconds", "Duration Extension Time (seconds)", and "Alert Duration == Audio Duration + Extension Time (max total is 120 seconds)". At the bottom, there are two checkboxes: "All FIPS codes trigger. Enabled. All FIPS locations will trigger DVS644/SCTE 18/CEAM device. Uncheck to choose specific triggering FIPS" and "All EAS codes trigger. Enabled. Alerts with any EAS code will trigger DVS644/SCTE 18 send. Uncheck to choose specific triggering EAS Codes". At the very bottom are "Accept Changes" and "Cancel Changes" buttons.

Set Alert Type Priority/FIPS & EAS Code Triggers Section

Set 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 incremented (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 SCTE18 to send multiple language translations to the SCTE18 connected device.

Alert Text Control

This pull-down menu programs when the alert text section of the DVS644/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** text 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 DVS644 client at a specific IP address, the DVS644/SCTE-18 MPEG2 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 screenshot this option is enabled. Click 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 codes trigger** is disabled, select a FIPS Group 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 DVS644/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 screenshot this option is enabled. Click 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 codes trigger** is disabled, select an EAS Group from the pull-down menu. If the EAS codes of an active forwarded/originated alert match any included in the EAS Group, the alert will be sent using the DVS644/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 **Forwarded Alerts stream** and/or the **Encoder Originated Alerts stream** check boxes to enable/disable the use of streaming MPEG clients when alerts are forwarded and/or originated.

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. Pop-up Help is available on this page.

The screenshot shows the 'Stream MPEG' configuration page. At the top, there is a navigation bar with tabs: Main, Station, Alert Agent™, Demo/Practice, Audio, Video/CG, **Net Alerts**, EMail, GPIO, Printer, Alert Storage, Network, Time, and Users. Below this is a sub-navigation bar with tabs: EAS NET, CAP Decode, DVS644 (SCTE18), **Stream MPEG**, Net CG, Net Switch, and Net GPIO. The main content area contains several settings:

- ☐ Forwarded Alerts stream MPEG. *Disabled. Uncheck to disable.*
- ☒ Encoder Originated Alerts stream MPEG. *Enabled. Uncheck to disable.*
- * Video output must be Enabled!
- * Click Accept Changes to store modified values
- * **Multistation Active.** Specific stations can disable Streaming MPEG by disabling Video Output
- * [No audio playout delay. Click to edit.](#)

Configuration fields include:

- Screen Resolution: 640x480
- Video Bitrate: 2000kbps
- Video Framerate: 30 FPS
- Font size: 32
- PAT/PMT (in Decimal, default is 1): 101
- PMT PID (in Hex, default is 42): 64
- Audio Stream PID (in Hex, default is 45): 45
- Video Stream PID (in Hex, default is 44): 44
- Test MPEG out: Select Streaming MPEG client
- Audio Codec: MP2
- Audio Bitrate: 128Kbits/sec
- MPEG Audio Sample rate: System rate (48000: Audio Samples/Sec. [Follow link to edit.](#))

Total Bitrate: 2394kbps. See the manual for bitrate calculation details.

Stream MPEG

Note: The addition of the MPEG Audio Sample rate selector pull-down menu with the following selections:

This close-up shows the 'MPEG Audio Sample rate' pull-down menu. The menu is open, displaying the following options:

- System rate
- 16K samples/sec
- 32K samples/sec
- 44.1K samples/sec
- 48K samples/sec

MPEG Audio Sample Rate Selections Pull-Down Menu

Streaming MPEG requires very few configuration fields. A **Remote Host Unicast or Multicast IP Address** must be set, along with a port. The **Multicast TTL** value must be set high enough to ensure the multicast data is sent past all the LAN routers between the EAS device and the destinations. Also, as with the EAS NET and DVS644 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 Alerts** check boxes to enable/disable the use of Net CG clients when alerts are forwarded and/or originated.

Addition/duplication/deletion, configuration, and enable/disable for each client interface is handled just like other Net Alert interfaces described in previous sections.

Net CG Sub-Tab

Client Interface Name

This text field 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 radio button for the CG that pertains to your situation. The 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. Check 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 IDs 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

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.

ENABLE Client Interface

Check this box to enable the interface for the card/module located within the defined Avenue frame slot.

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.

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 Participant 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 Participant 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 characters each. Separate each source EAS Participant ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS Participant identifiers STAT1 or STAT2).

Hub Controller/Net GPIO

This sub-tab is a standard feature on an 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:

- Digital Alert Systems – R190A Hub Controller (four relays)
- Digital Alert Systems – R197 Audio Switch
- Digital Alert Systems – R198 AES Audio Switch
- Titus - W300
- WebRelay X401
- 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.

Net GPIO Sub-Tab

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.

Listen for any Net GPI 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.

Note: Only enable this option when an input from a Net GPIO unit is required.

Add 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 Client Interface** button to create a new interface configuration.

Duplicate NetGPIO Client Interface

To duplicate an existing client interface, select the **Duplicate NETGPIO Client Interface** button. A different name will be automatically generated. This is the best way to create many client interfaces that are mostly the same except for the IP address.

Delete this NetGPIO interface

To delete a client configuration, select the client and click on **Delete this GPIO interface**.

Close EAS Audio Relay, Open EAS Audio Relay

These buttons provide manual overrides intended for test purposes. Pressing either button will either close or open any audio relays programmed for audio payout. This will control both the internal relays and the Net Controller/Net GPIO relays programmed for audio payout.

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 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

The actions can be tied to alert FIPS Groups, EAS Groups, and specific EAS Participant 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 Participant 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 Participant ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS Participant identifiers STAT1 or STAT2).

When you finish making changes, click the **Accept Changes** button to save the configuration.

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 status 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 to the right of the Platform Name in 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.

Main GPIO

The **Main GPIO** web interface contains the following sections:

- **DASDEC Server GPIO Table**
- **Programmable GPIO Input Actions/Output Relay**
- **DASDEC Server Expansion GPIO Input/Output Tables** (*when configured with an Expansion GPIO option*)
- **Network GPIO Table** (*if a network-attached GPIO unit is configured*)

Send Alerts **Alert Events** **System** **Setup**

Main Station Alert Agent™ Demo/Practice Audio Video/CG Net Alerts EMail **GPIO** Printer Alert Storage Network Time Users

Main GPIO Expansion GPIO Multiplayer GPIO

DASDEC™ Server GPIO Table				
Front Panel Button Press Current Status:Open (OFF)	GPI Input 1: Trigger Weekly Test (RWT) Current Status:Open (OFF)	GPI Input 2: Forward Active pending RMT with original audio Current Status:Open (OFF)		
GPI Output 1: Closed during EAS Audio Current Status:Open (OFF)	GPI Output 2: Closed during EAS Audio Current Status:Open (OFF)	Main audio passthrough Disabled: Internal Audio On.	Main AES audio passthrough Disabled: Internal AES audio On.	

Close EAS Audio Relay Open EAS Audio Relay

Programmable GPIO Input Actions (Dry contact)

GPI Input 1:
Issue Weekly Test (RWT) upon closure

GPI Input 2:
Forward active RMT with original decoded audio

GPIO Pending Alert Activation Criteria Configuration
Choose FIPS and EAS codes that control which active pending alerts trigger the GPIO Output 1 and 2 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 any forward action eg. "Forward active decoded EAS upon closure".

FIPS Group: All Locations EAS Group: All

Programmable GPIO Output Relay (Dry contact, max 2 Amps@30VDC)

GPI Output 1 Relay is closed:
During EAS Audio Playback
FIPS Group: All Locations EAS Group: All

GPI Output 2 Relay is closed:
During EAS Audio Playback
FIPS Group: All Locations EAS Group: All

☐ EAS NET/Multistation option for National Alerts EAS/NPT: delay EAS Audio GPIOs until voice audio. Only use for special EAS NET applications.Disabled, check to enable.

Setup > GPIO > Main GPIO Setup Screen

DASDEC 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 playback.

Programmable GPIO Input Actions/Output Relay

The programmable options in this section are **GPI Input 1**, **GPI Input 2**, **GPI Output 1 Relay**, and **GPI 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.

GPI Input 1

A pull-down menu allows GPI 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

The same pull-down menu options from GPI Input 1 are available for GPI Input 2. A pull-down menu allows GPI Input 2 to be programmed to do one of the options above.

GPI 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 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) (X)
- During EAS Video Payout
- During Main Serial Port EAS Payout
- 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)

GPI Output 1 Activation Filter Configuration

Choose the **FIPS Group** and/or **EAS Group** that will control which alerts trigger the applicable programmed GPI 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.

GPI Output 2 Activation Filter Configurations

Choose the **FIPS Group** and/or **EAS Group** that will control which alerts trigger the applicable programmed GPI 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 a **FIPS Group** and **EAS Group** to control which active pending alerts trigger the GPI 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 GPI 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 GPI 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 GPI Output 1 Relay or GPI Output 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 Inputs Table			
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 : Light Front Panel Alert LED white closed Current Status:Open (OFF)

DASDEC™ Server Expansion GPIO Outputs Table			
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 Expansion GPIO Status** check box will appear on this screen and there will be a sub-tab labeled **Expansion GPIO** within the **Setup > GPIO** navigation tab. 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 GPIO** 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** sub-tab. (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** navigation tab. 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 Screen

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 GPI Input 1 selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Input Action** pull-down menu.

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 GPI 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 payout 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** navigation tab. MultiStation and MultiPlayer options require a valid Plus Package license key.

Multiplayer GPIO Screen

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 GPI 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 GPI 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 programmed to EAS audio payout.

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, download the Multiplayer Quick Start Guide from the Digital Alert Systems website.

The screenshot displays the 'Programmable Multiplayer GPIO Outputs' web interface. At the top, there are two buttons: 'Close EAS Audio Relay' and 'Open EAS Audio Relay'. Below these buttons is a table with 8 rows, each representing a relay. The rows are labeled as follows:

- MP Port 1: Relay 1
- MP Port 1: Relay 2
- MP Port 2: Relay 1
- MP Port 2: Relay 2
- MP Port 3: Relay 1
- MP Port 3: Relay 2
- MP Port 4: Relay 1
- MP Port 4: Relay 2

Each row contains a 'Relay is closed' pull-down menu and a 'Current Status: Open (OFF)' button.

Programmable Multiplayer GPIO Outputs

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 emailed 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 will enable the automatic printout of EAS alerts as they occur. Using this approach means that each alert will print on an individual page. This printing means is reviewed in this section.

Connecting to a Network Computer or Via USB

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. From the CUPS homepage, click on the **Administration** tab at the top of the page. Click the **Add Printer** button and 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.

To connect to a printer via USB, plug the printer into a USB port located on the back of the EAS device. On the **Setup > Printer** navigation tab, 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**. Print a test page to make sure the printer works.

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.

The screenshot shows the 'Printer' configuration window. At the top, there are tabs for 'Send Alerts', 'Alert Events', 'System', and 'Setup'. Under 'Setup', there are sub-tabs: 'Main', 'Station', 'Alert Agents', 'Demo/Practice', 'Audio', 'Video/CG', 'Net Alerts', 'Email', 'GPIO', 'Printer' (selected), 'Alert Storage', 'Network', 'Time', and 'Users'. Below the tabs are 'Accept' and 'Cancel' buttons. The main content area shows the 'CUPS Printer system' is 'Enabled'. Under 'Printer Configuration', there is a description and a link to 'CUPS Printer Administration/Configuration'. Below this are seven checkboxes for various printer output options. At the bottom, there are 'Accept Changes' and 'Cancel Changes' buttons, and a 'Print Test Page' button. A 'Printer Status' window is open at the bottom, showing system logs.

Send Alerts **Alert Events** **System** **Setup**

Main Station Alert Agents Demo/Practice Audio Video/CG Net Alerts Email GPIO **Printer** Alert Storage Network Time Users

Accept Cancel

☒ CUPS Printer system. **Enabled**. Uncheck to Disable.

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 Monthly Printout of EAS Event Report.
☒ Weekly and Monthly EAS Event Report is Categorized. **Enabled**. Uncheck to Disable.

☐ Send data as Postscript to printer. **Disabled**. Check to enable.

Accept Changes Cancel Changes

Print Test Page

Printer Status

```
scheduler is running
system default destination: HP2300L
device for HP2300L: socket://10.0.0.52:9500
HP2300L accepting requests since wed Jan 27 13:40:17 2021
printer HP2300L is idle. enabled since wed Jan 27 13:40:17 2021
```

Printer Configuration Screen

Printer Configuration

There are seven check box options available. Check to enable/disable each option. 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 that includes 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 that includes 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, 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 Changes** button to save changes to this page.

When a printer is configured, the expired alert status reports displayed on the **Alert Events > Active, 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 alert timed cleanup.** Enabled. Decoded alerts will be saved for the following number of days, then moved to a holding area for 14 days, then alerts is deleted and header archived. Uncheck to Disable Decoded alert cleanup.
Decoded alerts save period (180 or more days) 730

☒ **Forwarded alert timed cleanup.** Enabled. Forwarded alerts will be saved for the following number of days, then moved to a holding area for 14 days, then alerts is deleted and header archived. Uncheck to Disable Forwarded alert cleanup.
Forwarded alerts save period (180 or more days) 730

☒ **Originated alert timed cleanup.** Enabled. Originated alerts will be saved for the following number of days, then moved to a holding area for 14 days, then alerts is deleted and header archived. Uncheck to Disable Originated alert cleanup.
Originated alerts save period (180 or more days) 730

☒ **CAP file timed deletion.** Enabled. CAP files will be saved for the following number of days, then deleted (no holding period). Uncheck to Disable CAP file deletion.
CAP files save period (180 or more days) 730

☐ **Archived header file timed deletion.** Disabled. Check to Enable Archived file deletion after a specific time period.

☐ **Op Log and Web Session Log file timed deletion.** Disabled. Check to Enable Log 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.** Enabled. See Delete button on each expired alert event. Check to Enable

☒ **Rebuild Event Display Cache Files on Startup.** Enabled.

Storage Space Table for core partition

Category	Value	Percentage
Total	204800000	100%
Used	6553600	3%
Available	198246400	97%

Alert Storage Setup Screen

Note: An option to force clean encrypted disks has been added to the interface.

Alert Storage Management configuration

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 150MB). 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 150 MB. If the EAS device available storage space drops below 150 MB, 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.



Force Options on the Setup > Alert Storage Screen

Note: Mouse-overs display an explanation of functional for each Force button.

Chapter 4: Alert Events Tab

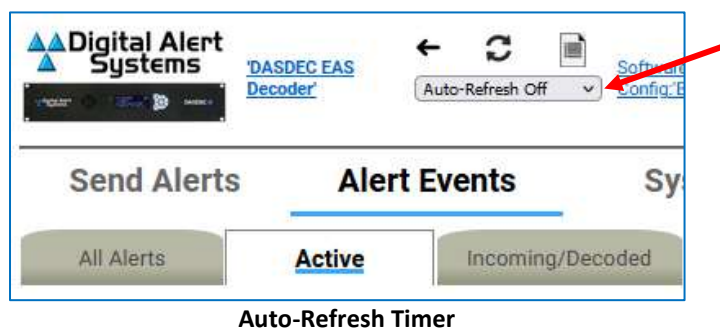
The **Alert Event** tab has six sub-tab options. Incoming alerts are automatically displayed on the Alert Events page. Each sub-tab is described below.

Sub-Tab	Description
All Alerts	Displays a list of scheduled Originated Alerts, current Active Alerts, and expired Alerts. EAS alert logs can be printed and/or saved.
Active	Displays the status of Incoming and Active Decoded alerts. Unacknowledged alerts can be forwarded and Demo Decoded alerts can be added from this screen.
Incoming/Decoded	Displays the status of Incoming and Active Decoded alerts, and 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 status of Active Forwarded alerts and Expired Forwarded Alerts. EAS alert logs can be printed and/or saved.
Originated/ Forwarded Alerts	Displays a list of Scheduled Originated Alerts, current Active Originated/Forwarded Alerts, and expired Originated/Forwarded Alerts. EAS alert logs can be printed and/or saved.
Originated Alerts	Displays a list of Scheduled Originated Alerts, current Active Originated Alerts, and expired Originated Alerts. EAS alert logs can be printed and/or saved.

Each sub-tab 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 above the **Alert Events** tab in the screen header) allowing the page to be re-displayed every 15, 30, or 60 seconds. Use this option to stay informed of the EAS device decoding activity and decoded events status.



Auto-Refresh Timer

Decode Activity Table

The **Active**, **Incoming/Decoded**, and **Forwarded Alerts** sub-tabs 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. The **Decode Activity** hyperlink takes users to the **Setup > Audio > Decoder Audio** screen.



Decode Activity Table

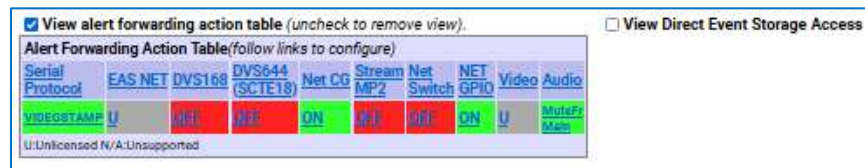
Station ID and Global Forwarding Mode

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.

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.

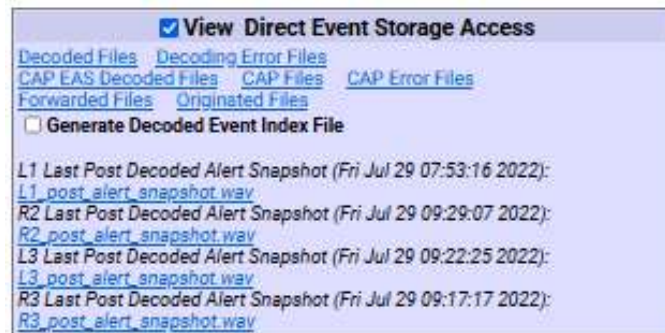


View Alert Forwarding Action Table

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 for analysis.

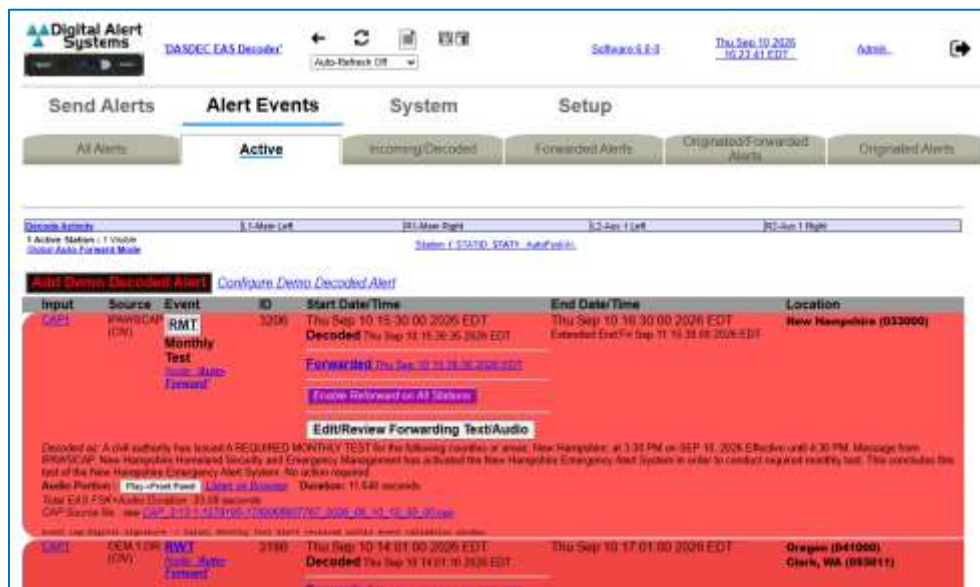


Direct Event Storage Access Table

The **Generate Decoded Event Index File** check box 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)”.

Active

This screen shows the status of Incoming and Currently Active Decoded Alerts. The **Active** screen monitors new and incoming EAS alert activity. Broadcasters who manually forward alerts should stay logged into the EAS device to view the **Active** screen with the auto-refresh option enabled.



Active Alerts Screen

The **Active** screen displays the status of all incoming alerts “received” by the EAS device and contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Direct 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 **Incoming/Decoded** section.

All other interfaces on this web page are described in the **Incoming/Decoded** section that follows.

Incoming/Decoded

Incoming/Decoded 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, Direct Event Storage Access table, active decoded EAS alerts, and expired decoded EAS alerts.

The screenshot displays the 'Incoming/Decoded' interface. At the top, there are tabs for 'All Alerts', 'Active', 'Incoming/Decoded' (which is selected), 'Forwarded Alerts', 'Originated/Forwarded Alerts', and 'Originated Alerts'. Below the tabs, there's a 'Decode Activity' section with filters for 'L1 Alert Left', 'R1 Alert Right', 'L2 Alert Left', and 'R2 Alert Right'. The main content area shows an active alert for 'Decoded (EAS)' with ID 1591, starting on Tue Jan 31 11:20:00 2023 EST and ending on Tue Jan 31 11:35:00 2023 EST. The location is Central Pacific Ocean (009000). The alert text is 'TTS ENGLISH: Alert on Broadcast - 15.3 secs'. Below the alert text are buttons for 'Forward Alert', 'Edit/Review Forwarding Text/Audio', and 'Acknowledge Pending Alert'. At the bottom, there are two sections: 'View alert forwarding action table' and 'View Direct Event Storage Access'. The 'View alert forwarding action table' section shows a table with columns for Serial, Protocol, CAS, Net, IVN, Net, Stream, Net, Net, Video, and Audio. The 'View Direct Event Storage Access' section shows a list of decoded files and a link to generate a decoded event index file.

Incoming/Decoded Screen with Active Alert

The **Incoming/Decoded** screen displays status of all incoming and decoded alerts “received” by the EAS device and contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Direct 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

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 **Forward Alert** and **Edit/Review Forwarding Text/Audio** 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

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 [Demo/Practice Setup](#)).

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.

Currently Active Decoded Alerts

These alerts are below the **Add Demo Decoded Alert** button and display 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.

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 screenshot 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.

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.

Edit/Review Decoded Alert for Forwarding

Input	Source	Event	ID	Start Date/Time	End Date/Time	Location
Device (EAS)	Device	1592	Tue Jan 31 11:49:00 2023 EST	Tue Jan 31 12:04:00 2023 EST	Central Pacific Ocean (60kms)	

Decoded as: A broadcast or cable system has issued A PRACTICE/DEMO WARNING for the following counties or areas: Central Pacific Ocean at 11:49 AM on Jan 31, 2023 Effective until 12:04 PM. Message from Device.

Decoded EAS String:

Forwarding Alert Text Translation: Length: 100. View decoded alert text.

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 = 198

Optional Pre-Alert Audio Announcements (played before EAS Header audio)

Optional Post-Alert Audio Announcements (played after EAS EOM audio)

Original alert audio can be replaced. Make selection.

Original Audio

EASINTRO.wav

EASOUTRO.wav

EASpreMsg.wav

EASpostMsg.wav

No audio message for this alert.

Record Audio File

Total EAS ESK+Audio Duration: 10.04 seconds

OK Cancel

Upload Audio .WAV file to DASDEC™ Server.

Browse... No file selected.

Upload .WAV file

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 the 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.

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.



Blocked Alert Example

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.



Enable Reforward Example

Expired Decoded Alerts

Using the pull-down menu in the Expired Decoded Alerts section allows you to choose which expired alerts to view. The expired alerts are divided into three categories:

- 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)

Select the types of expired alerts to be viewed. Each of the listed alerts contains a hyperlink that can be used to review the specific expired alert.

Input	Source	Event	ID	Start Date/Time	End Date/Time	Location
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1595	Tue Jan 31 12:14:00 2023 EST	Tue Jan 31 12:29:00 2023 EST	Jackson, OR (541829)
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1593	Tue Jan 31 12:02:00 2023 EST	Tue Jan 31 12:17:00 2023 EST	Santa Barbara, CA (949992)
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1592	Tue Jan 31 11:49:00 2023 EST	Tue Jan 31 12:04:00 2023 EST	Central Pacific Ocean (949996)

Expired Alerts Section

The Deleted Expired 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 screenshot below shows the most commonly used option **View Expired Alerts**. The other two options present the same interface.

Set the Date Range

The Expired Decoded Alerts list shows past decoded alerts for any range of dates. Once the type of expired alert to be viewed is selected, use the pull-down menu located below it to view the date range options and select the best option. A user defined date range is available, enabling custom start and end dates (year, month, day). The screenshot shows an example of the expired alerts list for a selected range of dates.

Input	Source	Event	ID	Start Date/Time	End Date/Time	Location
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1595	Tue Jan 31 12:14:00 2023 EST	Tue Jan 31 12:29:00 2023 EST	Jackson, OR (541829)
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1593	Tue Jan 31 12:02:00 2023 EST	Tue Jan 31 12:17:00 2023 EST	Santa Barbara, CA (949992)
IRWIS CAP	JACKCOEM (OVN)	WWT South_Rule Forward	1592	Tue Jan 31 11:49:00 2023 EST	Tue Jan 31 12:04:00 2023 EST	Central Pacific Ocean (949996)

View Expired Alerts- User Defined Range

Whatever a View Expired Alert option 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 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 date range 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.

Get Text Version

A text version of the expired alerts is available. Select the option **Get 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 **Categorize alerts in text version** check box. Otherwise, the text version will be organized by date of alert.

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.

If a printer is enabled, a **Print** button will display to the right of the link **Get 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 are displayed in a table. This includes the time the alert was decoded and the time the alert was forwarded, as well as if it was forwarded.

Forwarded alerts are displayed on the **Forwarded Alerts** or **Originated/Forwarded Alerts** screens.

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 Expired Decoded Alerts section. 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 Alerts list, 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 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.

Active & Incoming/Decoded: MultiStation Mode

The active decoded alerts display supports MultiStation mode. You can view the active (enabled) stations on the right side of the page below the Decode Activity 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 screenshot below shows one active, unacknowledged decoded alert, with five available enabled station targets, and thus five **Forward Alert** buttons, one per station. A single **Acknowledge Pending Alert** and **Edit/Review Forwarding Text/Audio** button is provided to cover MultiStation mode.



Active Decoded Alerts – MultiStation Mode

A severe EAS alert may need to be forwarded faster than in sequence to each enabled station. In that case, a separate button labeled **Forward Once Simultaneously on 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.

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 (unchecked to remove view).

Alert Forwarding Action Table (follow links to configure)

Station	Serial Protocol	EAS NET	DVS168	DVS644 (SCTE18)	Net CG	Stream MP2	Net Switch	NET GPIO	Video	Audio
Station 1	OFF	U	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1
Station 2	OFF	U	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1
Station 3	OFF	U	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1
Station 4	OFF	U	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1
Station 5	OFF	U	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1

U: Unlicensed N/A: Unsupported

Alert Forwarding Action Table- MultiStation Mode

After an alert is forwarded to a station, the **Forward Alert** button is replaced by the **Enable Reforward** 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 displays an active decoded alert after forwarding to the fifth station.



Active Decoded Alerts – MultiStation Mode w/Enable Reforward button

Below is an example of the changes to the alert display after using the other **Forward Alert** buttons. The screenshot shows the active decoded alert status after forwarding to the first, second, third, fourth, and fifth enabled station, and after forwarding to all stations once (using the **Forward Once Simultaneously on 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).



Active Decoded Alerts – MultiStation Mode w/All Forward Alert Buttons Used

Forwarded Alerts

Forwarded Alerts contain the same detailed alert information about Forwarded Alerts as previously discussed in the **Active** section. They are organized alike, without the options for the Alert Forwarding Action table, Play audio alarm, and the Direct 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 screenshot below shows the active Forwarded Alerts display after the same decoded alert was forwarded to all stations using the **Forward Once Simultaneously on All Stations** button (top RWT 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.

Security Station		300 Main Left		300 Main Right		300 Sub 1 Left		300 Sub 1 Right			
3 Active Stations - 3 Visible		Station 1: STATION1 - Auto-Forwarded		Station 2: STATION2 - Auto-Forwarded		Station 3: STATION3 - Auto-Forwarded		Station 4: STATION4 - Auto-Forwarded			
Global Auto-Forward Mode		Station 5: STATION5 - Auto-Forwarded		Station 6: STATION6 - Auto-Forwarded		Station 7: STATION7 - Auto-Forwarded		Station 8: STATION8 - Auto-Forwarded			
Input	Source	Event	ID	Start Date/Time	End Date/Time	Location					
1001	STATION1 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 1 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											
1002	STATION2 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 2 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											
1003	STATION3 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 3 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											
1004	STATION4 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 4 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											
1005	STATION5 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 5 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											
1006	STATION6 (CIV)	WEAT	1611	Wed Feb 1 09:49:00 2023 EST	Wed Feb 1 17:49:00 2023 EST	Wright, MN (027171)					
Forwarded To Station Station 6 Wed Feb 1 10:50:04 2023 EST											
A civil authority has issued a REQUIRED WEEKLY TEST for the following counties or areas: Wright, MN, at 9:49 AM on FEB 1, 2023 Effective until 5:49 PM. Message from HWASCAP TEST TEST TEST This is a test from the Wright County Sheriff's Office TEST											
Total EAS FOR Audio Duration: 10:04 seconds											

Forwarded Alerts- MultiStation Mode

Originated/Forwarded Alerts

The **Originated/Forwarded Alerts** screen displays the status of all alerts “sent” from the EAS device and contains the following three sections:

- 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 [Station Setup](#)).

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 and contains the following three sections:

- 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.

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 [Station Setup](#)).

Currently Active Originated 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 Alerts

This section displays the total number of expired and currently active originated 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.

All Alerts

The **All Alerts** screen is typically used to view or print all activity for a selected date range and contains 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.

View Expired Alert

As with the other event status views, you may choose to view:

- View Expired Alerts
- Expired Alerts Pending Deletion
- 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.

Get Text Version

Click the **Get Text Version** link to generate a printable text version of the alert(s).

Print

Use the **Print** button to send the text version of the alert(s) to the printer.

Categorize alerts in text version

Click the checkbox to categorize text alerts.

Show event details

Click the checkbox to show event details.

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 EAS device
2. Go to **Alert Events**
3. Select one of the following sub-tabs, depending on which type of logs are desired:
 - Incoming/Decoded
 - Forwarded Alerts
 - Originated/Forwarded Alerts *(This is the typical selection for FCC logging purposes)*
 - Originated Alerts
 - All Alerts
4. Scroll down and find the Expired Decoded Alerts section and make sure **View Expired Alerts** is selected in the pull-down menu.
 - The blue area displays the EAS logs that have been processed within the time period selected.
 - The total number of records is shown (next to the pull-down) along with the date range. These EAS records are sorted from earliest to (at top of the list) to the latest dates

Input	Source	Event	ID	Start Date/Time	End Date/Time	Location
IRAWS CAP (CAP)	Decoder: WIC IRAWSCAP (CIV)	REQUIRED WEEKLY TEST	1597	Tue Jan 31 12:24:00 2023 EST	Tue Jan 31 13:24:00 2023 EST	Washoe, NV (832831)
		Forwarded Tue Jan 31 12:42:01 2023 EST				
		A civil authority has issued A REQUIRED WEEKLY TEST for the following counties or areas: Washoe, NV at 12:24 PM on JAN 31, 2023 Effective until 1:24 PM. Message from IRAWSCAP: Test test test. This is a weekly test of the Emergency Alert System. Test test test.				
		Duration: 15.213 seconds				
		Audio Portion: Play from File Listen on Stream				
IRAWS CAP (CAP)	Decoder: WIC IRAWSCAP (CIV)	PRACTICE/DEMO WARNING	1579	Tue Jan 31 07:43:00 2023 EST	Tue Jan 31 07:58:00 2023 EST	Central Pacific Ocean (859800)
		Forwarded Tue Jan 31 07:43:30 2023 EST				
		A broadcast or radio system has issued A PRACTICE/DEMO WARNING for the following counties or areas: Central Pacific Ocean, at 7:43 AM on JAN 31, 2023 Effective until 7:58 AM. Message from Decoder: Test This is a State Wide Required Weekly Test of the Emergency Alert System originating from the Pennsylvania Emergency Management Agency, Harrisburg. This is only a test.				
		Duration: 15.376 seconds				
		Audio Portion: Play from File Listen on Stream				

Alert Events Screen - Select Expired Alert View Section

5. Use the time period pull-down menu to further refine the records displayed.
6. Once the desired list is displayed, clicking the **Get 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 forwarded alerts:
-----
Server: 'DASDEC EAS Decoder' @ 192.0.0.212
DASDEC-3EN '/dasdec_forwarded_events/' Alert Report at 'Wed Feb 1 13:00:16 2023 EST'
From 'Sun Dec 4 00:00:00 2022 EST' to 'Thu Feb 2 00:00:00 2023 EST'
-----
1578: RWT REQUIRED WEEKLY TEST 'CAP1'(Dasdec ) ORG=CIV
      'Tue Jan 31 07:01:00 2023 EST' to 'Tue Jan 31 09:01:00 2023 EST'
      Forwarded : 'Tue Jan 31 07:41:27 2023 EST'
      Pennsylvania(042000)

1579: DMO PRACTICE/DEMO WARNING 'DEMO'(Dasdec ) ORG=EAS
      'Tue Jan 31 07:43:00 2023 EST' to 'Tue Jan 31 07:58:00 2023 EST'
      Forwarded : 'Tue Jan 31 07:43:30 2023 EST'
      Central Pacific Ocean(859800)

1597: RWT REQUIRED WEEKLY TEST 'CAP1'(Dasdec ) ORG=CIV
      'Tue Jan 31 12:24:00 2023 EST' to 'Tue Jan 31 13:24:00 2023 EST'
      Forwarded : 'Tue Jan 31 12:42:01 2023 EST'
      Washoe, NV(832831)

3 events for this time period.

*****
3 total events found for this time period.
*****
```

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 5: 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 sub-tabs.

Sub-Tabs	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, 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.

Note: Due to the need for immediate action during origination, **Send Alert** 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.

For 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, as well as to prepend or append text to the standard translation or even fully substitute the translation for custom text.

General Alerts

The **General Alerts** 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 Alerts** 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.

- Set Destinations
- Set Event
- Set Duration, Date and Time

- Set Locations(s)
- Set ENGLISH Message Contents
- Set ENGLISH Audio
- Send Alert

Send Alerts

Alert Events

System

Setup

General Alerts

One-Button Alert

Custom Message

5 Active Stations : 5 Visible

Station 1' STATID: STAT1

Station 2' STATID: STAT2

Station 3' STATID: STAT3

Station 4' STATID: STAT4

Station 5' STATID: STAT5

Override

Origination

code:EAS

Set Event-->Event_Time&Duration-->Locations-->Message-->Audio-->SEND

1. Set Event

Alert EAS Code

RWT : REQUIRED WEEKLY TEST

2. Set Duration, Date and Time

Event Duration

Hours 0 Mins 15

Use current time for the effective Start Time for alert. Enabled.

3. Set Location(s)

Northeast Erie,NY (336029)

Northeast Genesee,NY (336037)

Northeast Orleans,NY (336073)

SELECTED FIPS Location Codes

Need to Add FIPS Codes

<< Use interface to left to select FIPS from the available pool.

Add Selected FIPS->

Content Language English

4. Set ENGLISH Message Contents

Alert NOT Ready to send

5. Set Primary ENGLISH Audio

Optional Pre-Alert Audio Announcement

No Audio

Record Audio File

EAS Broadcast Audio Content (optional)

Local audio content

Weekly Test EAS Broadcast Audio is Not Enabled

Optional Post-Alert Audio Announcement

No Audio

Goto --> Setup Audio Output Levels

6. Send Alert

Alert NOT Ready to send::Specify FIPS

Reset

View alert action table.

Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

General Alerts Section

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. Use this pull-down menu to view the available options, then select/click the desired option.



General Alerts Screen - Template Management Section

Loaded EAS Templates can be modified prior to being sent. Recall the saved template, make the desired changes, and send the Alert.

Delete Template

The process of deleting EAS Templates is a three-step process. First, load the desired template from the **Load EAS 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 Message** screen.

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 to the right of this button and click the **Save Template As:** button. The template will be saved and available in the **Load EAS 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 Participant 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 generally will 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.



General Alerts - Set Event Section

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 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 that are 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.



General Alerts - Set Duration, Date and Time Section

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.

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**.

4. Set Location(s)

Available FIPS Codes	SELECTED FIPS Location Codes
- Orleans, NY (036073) - Genesee, NY (036037) - Livingston, NY (036051) - Monroe, NY (036055) - Niagara, NY (036063)	Current FIPS locations for Alert 1. All Orleans, NY (036073) Remove

General Alerts – Set Location(s) Section

To set the FIPS location(s) for the alert code, select from the list of available FIPS codes. 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 the **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.

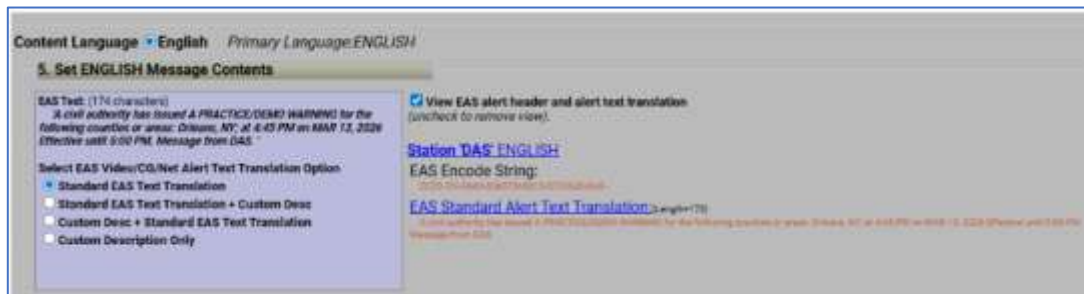
There is special color coding of state-wide codes in the **SELECTED FIPS Location Codes** frame. The state-wide codes are colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but not very common.

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 grayed 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 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.



General Alerts – Message Contents Section

Note: Additional languages (beyond English and Spanish) are available with a valid OmniLingual™ license key.

Set [Selected Language] Message Contents

Valid Plus Package and EAS NET™ license keys will display the **Select EAS Video/CG/Net Alert Text Translation Option** frame. Use the radio buttons to select one of four combinations of Standard Translation and Custom Translation. For selections with custom translations, a text entry field is displayed where the text can be entered.

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 EAS Text Translation
- Standard EAS Text Translation + Custom Description
- Custom Description + Standard EAS 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 the setup screen, allowing you to make changes as needed.

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

6. Set ENGLISH Audio

Optional Pre-Alert Audio Announcement
No Audio

EAS Broadcast Audio Content (optional)
Text to Speech from text content

*Note: Advanced Text to Speech not available, using basic Text to Speech.
Advanced Text to Speech installed but with 2 unlicensed voices.*

Make Draft TTS Audio File

Use Simultaneous Override Alert Text Select Station EAS alert text for draft TTS

An EAS Participant has issued A SEVERE THUNDERSTORM WARNING for the following counties or areas: Orleans, NY; at 7:54 AM on SEP 11, 2026 Effective until 8:09 AM. Message from WYRK.
Text size: 182 characters

Optional Post-Alert Audio Announcement
No Audio

[Goto --> Setup Audio Output Levels](#)

General Alerts – Set Primary Audio Section

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.

6. Set Primary ENGLISH Audio

Optional Pre-Alert Audio Announcement
EAS2750.wav
Duration: 5.297 seconds Rate: 48000 samples/sec Mono
[Listen on Browser](#)
Play in Front Panel Play in Web Play in Preview Out
Delete Selected
Record Audio File

EAS Broadcast Audio Content (optional)
Local audio content
[Resample to output rate \(configured output sample rate\) to avoid play out slowdown!](#)

Optional Post-Alert Audio Announcement
No Audio

[Goto --> Setup Audio Output Levels](#)

General Alerts – Optional Pre-Alert Audio Announcement Section

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
- Remote URI audio content
- Text to Speech from text content

Local Audio Content

The Local audio content option 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 pull-down menu.

The audio file duration (in seconds) and sample rate are displayed below the selection. There might also be a **Resample File** button – as described above.

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**, and **TDX URL**. These control the addition of TDX alert details.

Audio Playout Options:

Numerous playout 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**)

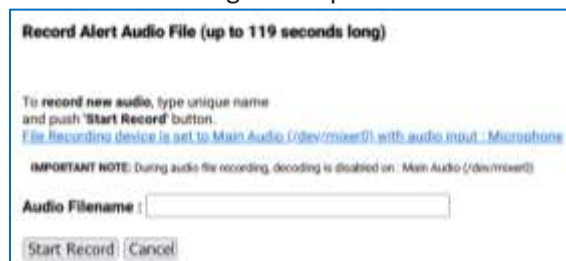
Audio Management Options:

Included in this section are three buttons to assist with managing audio files within the EAS device:

- Record Audio File
- Upload Audio File
- Delete Selected

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** screen to change the input source.



Record Alert Audio File Interface

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

When this button is clicked, an **Upload Audio .WAV file** interface appears. 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

This button is available when an audio file is selected and will immediately delete the selected file when clicked.

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.

General Alerts - Remote URI Audio Content Selection

Two pull-down menus and a text entry box will appear once this option is selected: Audio Type, URI Type, and EAS Audio URI address.

Audio Type

Select one of the following options from the pull-down menu:

- **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:

Select one of the following options from the pull-down menu:

- **http://** - HyperText Transfer Protocol
- **https://** - HyperText Transfer Protocol Secure

URI Address Text Entry Field

Enter the URI address for the desired audio file in the text field.

Use the **Auto-download upon send** check box to download the desired audio file for logging purposes.

Text to Speech from text content

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.

General Alerts- Text to Speech from Text Content Selection

There are three available buttons and a hyperlink available:

- **Make Draft TTS Audio File** button – 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 playout options in this section. A new TTS file will need to be created each time any of the alert settings are modified.
- **Play->Front Panel** button – click this button to play the audio file out the internal front panel speaker.
- **Play->Preview Out** button – click this button to play 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– click the hyperlink to play the selected audio file within the web-browser.

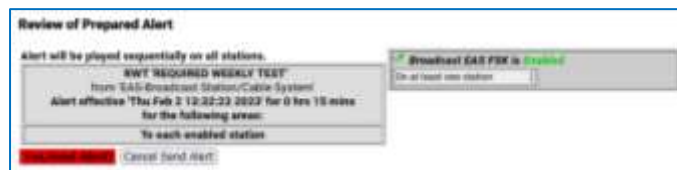
Optional Post-Alert Audio Announcement

Similar to the pre-alert announcement, this pull-down menu provides options to allow 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 Send Alert 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 Screen

Once 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 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 **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.



Send Alert Screen

Reset

The entire alert setup process can be restarted by clicking the **Reset** button, located to the right of the red **Send Alert** button.

View Alert Action Table

When the **View 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.

☒ View alert action table (unchecked to remove view).

Alert Origination Action Table(follow links to configure)

Station	Serial Protocol	EAS NET	DVS644 (SCITE18)	Net CG	Stream MP2	Net Switch	NET GPIO	Video	Audio
Station 1	OFF	ON	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1

U:Unlicensed N/A:Unsupported

☐ Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

View Alert Action Table Section

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 **Alert Origination Action Table** above changes to say the Serial Protocol is bypassed.

General Alerts: 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)**.

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 the 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).

Alert Origination Action Table(follow links to configure)

Station	Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP2	Net Switch	NET GPIO	Video	Audio
Station 1	OFF	ON	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1
Station 2	OFF	OFF	OFF	OFF	OFF	OFF	OFF	U	Front Main Aux1

U:Unlicensed N/A:Unsupported

☐ Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

Alert Origination 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.

One-Button Alert Screen

There are three ways to send reconfigured one button test alerts:

- Click the **Send Preconfigured Weekly Test!** button on the **One-Button Alert** screen
- Press the front panel button once, wait a second, press it again
- Initiating a contact closure on a configured GPIO Input

In all cases the alert is sent immediately with the current clock time as the effective alert start time. No confirmation dialog is presented.

The **One-Button Alert** 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:

- Setup Audio Output Levels
- Wrong FIPS?
- Front Panel Button Weekly Test Enabled

The **View EAS alert header and alert text translation** check box and the **Alert Origination Action Table** operate 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 screenshot below.

General Alerts

One-Button Alert

Custom Message

2 Active Stations: [Station 1 - EAS - STAT1](#)

2 Visible: [Station 2 - EAS - STAT2](#)

CAREFUL: Run Weekly Test button(s)

IMMEDIATELY play alert without confirmation!

Run Weekly Test sequentially on all stations

OR Bypass stations and play alert once (using simultaneous override configuration)

Run Weekly Test once simultaneously on all stations

OR

Run Weekly Test on Station "Station 1"

Run Weekly Test on Station "Station 2"

Effective Duration: 15 minutes

Override locations: [weekly_test_files](#)

1, Orleans,NY (036073)

Station "Station 1" locations: [weekly_test_files](#)

1, Orleans,NY (036073)

Station "Station 2" locations: [weekly_test_files](#)

1, Orleans,NY (036073)

☒ View alert action table (uncheck to remove view)

Alert Origination Action Table/Follow links to configure)

Station	Serial Protocol	EAS.NET	W/S&AA (GCTE)US	Net.EG	DRSnet MP3	Net Switch	NET COPS	Video	Audio
Station 1	NET	On	On	On	On	On	On	Y	Front Menu Run 1
Station 2	NET	On	On	On	On	On	On	Y	Front Menu Run 1

U/Unlicensed N/A/Unupported

☐ Serial Interface Bypass: Disabled. Check to Bypass Use of Serial Interface.

☒ View EAS alert header and alert text translation (uncheck to remove view).

Station "Station 1" ENGLISH

EAS Encode String:
ZCZC-CAG-4W15362734073-034103W-03AT1-

EAS Standard Alert Text Translation (Length=188)
"In broadcast or cable system has issued a 15362734073 1537 for the following location or area: Orleans, NY at 5:59 AM on FEB 2, 2023 Effective until 6:14 AM. Message from 21211"

Total EAS FSK+Audio Duration: 10.84 seconds

Station "Station 2" ENGLISH

EAS Encode String:
ZCZC-CAG-4W15362734073-034103W-03AT2-

EAS Standard Alert Text Translation (Length=188)
"In broadcast or cable system has issued a 15362734073 1537 for the following location or area: Orleans, NY at 5:59 AM on FEB 2, 2023 Effective until 6:14 AM. Message from 21212"

Total EAS FSK+Audio Duration: 10.84 seconds

Station "Override" ENGLISH

EAS Encode String:
ZCZC-CAG-4W15362734073-03WY03W-03AT0-

EAS Alert Text Translation w/ Custom Origination String (Length=176)
"In broadcast or cable system has issued a 15362734073 1537 for the following location or area: Orleans, NY at 5:59 AM on FEB 2, 2023 Effective until 6:14 AM. Message from 03AT0"

Total EAS FSK+Audio Duration: 10.84 seconds

☒ View alert action table (uncheck to remove view)

Alert Origination Action Table/Follow links to configure)

Station	Serial Protocol	EAS.NET	W/S&AA (GCTE)US	Net.EG	DRSnet MP3	Net Switch	NET COPS	Video	Audio
Station 1	NET	On	On	On	On	On	On	Y	Front Menu Run 1
Station 2	NET	On	On	On	On	On	On	Y	Front Menu Run 1

U/Unlicensed N/A/Unupported

☐ Serial Interface Bypass: Disabled. Check to Bypass Use of Serial Interface.

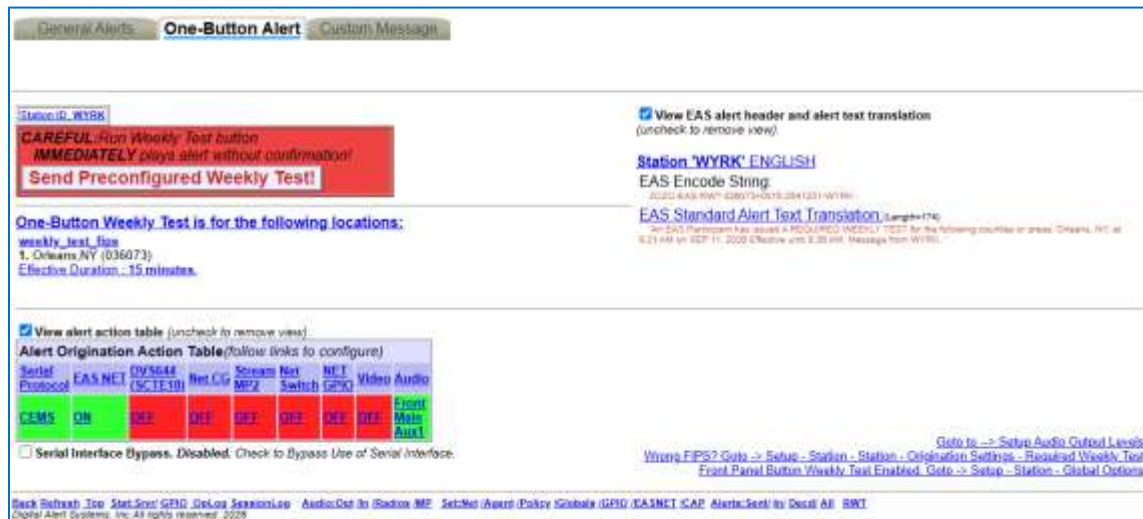
Go to => Setup Audio Output Levels

View EPG? Go to => Setup - Station - Station - Origination Settings - Run and Weekly Test

Front Panel Button Weekly Test Enabled, Go to => Setup - Station - Global

Options

One-Button Alert – MultiStation Mode



Single Station 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 the **Simultaneous Station Override** sub-tab used for any un-configured station.

The screenshot 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 button 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

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 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 Tab when MultiStation is enabled

The Custom Messaging 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 to DASDEC Server** controls.

General Alerts
One-Button Alert
Custom Message

Custom Message Options
NOTE: Changes made on this page effective IMMEDIATELY.

Load Custom MSG Template: None
Delete Template
Save Template As:

Send Custom Message
No Active custom messages at this time.

Message Type Control
Non EAS custom message

Message Display Control
Repeat custom message payout for a fixed number of times (or until stopped)
Number of repetitions: 1
Time in min:secs between end of payout and replay.
Mins : 00 Secs
Play audio message with every display repetition
Audio repetition control

Set Message Max Active Duration
Hours 0 Mins 15

Custom Text Message
THIS MESSAGE IS FROM THE CITY OF ALTUS EMERGENCY MANAGEMENT OFFICE AND IS SENT AT THE REQUEST OF ADMINISTRATION. As drought conditions continue and levels at Tom Steed Reservoir remain below 70%, Altus City Management has officially declared Stage 2 Water Conservation Restrictions are in effect for //
Custom text size = 299.
Read text file: None
Delete Text File
Save Text to File

Audio Messages
Optional Pre-Alert Audio Announcement
No Audio
Local Audio File
Select Alert Audio Message
No Audio
Optional Post-Alert Audio Announcement
No Audio
[Goto to --> Setup Audio Output Levels](#)

☒ View action and GPI binding table (unchecked to remove view).
Alert Origination Action Table(follow links to configure)

Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP2	Net Switch	NET GPIO	Video	Audio
CEMS	ON	OFF	OFF	OFF	OFF	OFF	OFF	Front Main Aux1

☐ Serial Interface Bypass. Disabled. Check to Bypass Use of Serial Interface.

Message template not selected above.
☐ Stop GPI triggered messages upon contact open.Disabled

Upload Audio .WAV file to DASDEC™ Server.
Choose File No file chosen
Upload .WAV file

[Back](#) [Refresh](#) [Top](#) [Stat.Srvr/](#) [GPIO](#) [OpLog](#) [SessionLog](#) [Audio.Out](#) [In](#) [Radio](#) [MP](#) [Set.Net](#) [Agent](#) [Policy](#) [Global](#) [GPIO](#) [EASNET](#) [CAP](#) [Alerts.Sent](#) [In](#) [Decd](#) [All](#) [RWT](#)
Digital Alert Systems, Inc.All rights reserved. 2020

Custom Messaging Screen

Template Management

The first section of this screen allows for quick and easy access to stored message templates. The following controls are available:

Custom Message Options
NOTE: Changes made on this page effective IMMEDIATELY.

Load Custom MSG Template: None
Delete Template
Save Template As:

Send Custom Message
No Active custom messages at this time.

Custom Message - Template Management Section

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.

To load a Custom Message Template, use the pull-down menu to 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

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 Message** screen. Click the **No, cancel** button to abort the deletion process and return to the **Custom Message** screen.

Save Template As:

Custom Message 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 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.

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 if an EAS or non-EAS message is being sent.

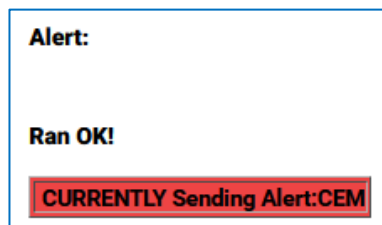


Review of Prepared Alert Screen

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.

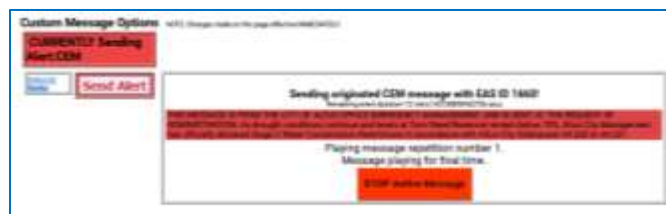
If for any reason the message is not configured properly, use the **Cancel Send Message/Alert** button, make the necessary changes, and begin the send message/alert process again. Otherwise, click the **Yes, Send Message/Alert!** button to send the configured message/alert.

The Custom Messaging 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.



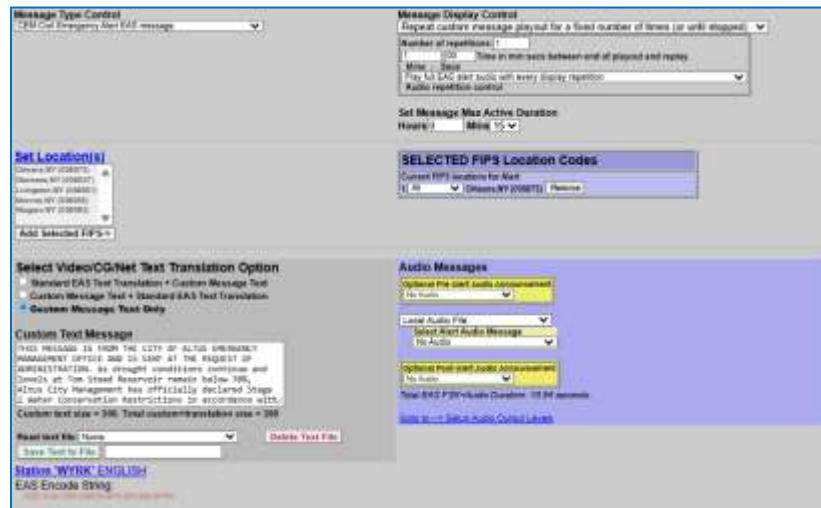
Confirmation Screen

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.



Custom Message Screen with Active Message/Alert

Below the **Send Custom Message/Send Alert** button is a gray background section for composing messages/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, that 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 Alert Text Translation**.



Custom Messaging 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.

Select the desired **Message Type** by clicking the menu once and selecting the desired type by clicking again on that selection.

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 abductor's 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 in the U.S. are said to "adhere closely to": 1. Law enforcement must confirm that an abduction has taken place. 2. The child's whereabouts are unknown and they are assumed to be at risk of serious injury or death. 3. There must be sufficient descriptive information of child, captor, or captor's vehicle to issue an alert 4. The child must be under 18 years of age
---	---

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)

Choose the desired **Message Display Control** by selecting the desired type from the pull-down menu.

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 field. These interface changes are self-explanatory.

Audio Repetition Control

Due to the tight relationship between video and audio, the **Audio repetition 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 with every display repetition
- 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 repetition control** pull-down menu. These include:

- 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

Set Message Max Active Duration

Every message/alert contains an active duration. This time is useful in several ways. It is used to calculate the 'Effective until...' time displayed in an EAS alert. Also, 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 **Set 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 **Set 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 time and date as the 'Effective until...' within the EAS alert. See the example alert text below.

'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, 2022 Effective until 8:41 PM OCT 27, 2022. 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 use 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 **SELECTED FIPS Location Codes** 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** section.

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.

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.

The screenshot shows a window titled "Select Video/CG/Net Text Translation Option". It contains three radio buttons: "Standard EAS Text Translation + Custom Message Text" (selected), "Custom Message Text + Standard EAS Text Translation", and "Custom Message Text Only". Below this is a section titled "Custom Text Message" with a text area containing the following text: "THIS MESSAGE IS FROM THE CITY OF ALTUS OFFICE EMERGENCY MANAGEMENT AND IS SENT AT THE REQUEST OF ADMINISTRATION. As drought conditions continue and levels at Tom Steed Reservoir remain below 70%, Altus City Management has officially declared Stage 2 Water Conservation Restrictions in". Below the text area, it says "Custom text size = 340. Total custom+translation size = 340". At the bottom, there is a "Read text file:" label with a pull-down menu showing "None", a red "Delete Text File" button, and a green "Save Text to File" button next to an empty text input field.

Custom Message – Custom Text Message Section

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** section 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 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 to DASDEC Server** section at the bottom of this screen. (see below for more detailed information on loading audio .wav files)



Custom Message - 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 on the **Optional Pre-Alert Audio Announcement** pull-down menu and selecting the desired item from that list.

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 the 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 utilizing the **Optional Post-Alert Audio Announcement** pull-down menu and selecting the desired item from that list.

When configuring EAS alerts, the total duration of the EAS alert is displayed just below this pull-down menu and labeled **Total EAS FSK+Audio Duration**:

The interface also contains a hyperlink to the **Setup Audio Output Levels** screen 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.



Custom Message – Alert Origination Action & GPI Binding Tables

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.

The GPI Binding Table (to the right of the **Alert Origination Action Table**) displays the GPI(s) configured to trigger the selected **Custom MSG Template**. A **Custom MSG Template** must be selected (at the top of the screen) in order to see what GPI(s) are configured to trigger that specific **Custom MSG Template**, otherwise the table will display **Message template not selected above**. Load each **Custom MSG Template** to view what GPIs 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 to DASDEC Server

The interface at the bottom of this screen allows .wav and .mp3 audio files to be uploaded into the EAS device for playback from the EAS device.



Custom Message - Upload Audio .WAV file Section

To upload a file, click the **Browse** button to locate the file on the local computer, then click the **Upload .WAV file** button. MP3 files are automatically converted into a WAV file. 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 interface screen or simply navigate using the tabs at the top of the user interface.

Any GPI may be assigned to a template – including internal and external/networked GPIs. More than one GPI may be assigned to a single template, however a single GPI may not be assigned to multiple templates.



Main GPIO - GPI Setup Screen

At the top of the GPI Setup screen is the **DASDEC Server GPIO Table**. In the above screenshot, the table displays **GPI Input 1** as being assigned to the **Test Template** custom message template. To configure this relationship:

1. Locate the GPI Input 1 pull-down menu on the left side of the interface.
2. Click the pull-down menu to view the available options.
3. Select **Run Custom Message** at the bottom of the pull-down menu.
4. Another pull-down menu will appear titled **Custom MSG**:
5. 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 6: 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 navigation tabs:

Navigation Tab	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 as decoders, GPIOs, network(s), Operating Systems, USB, CPU, PCI, IO devices, and email.
Logs	EAS device kept extensive logs for web sessions, operation, OS, security, boot, and email.
Debug Logs	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** navigation tab displays basic information about the DASDEC, End User License, About EAS, EAS Message Protocol, and EAS Codes. Each sub-tab is described below.

Sub-Tab	Description
About DASDEC	Displays basic system information about the EAS device, 64-bit 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

About DASDEC

Presents information about the installed 64-bit operating system, software version, install date and build date. This screen additionally displays information about Digital Alert Systems and the EAS device. The **WCPO DASDEC OAS** in the Header at the top of each screen is a hyperlink to the **Setup > Main > Main License** screen.



Help – About DASDEC Sub-Tab

End User License

A copy of the Digital Alert Systems End User License Agreement is displayed in this sub-tab.

About EAS

This sub-tab contains general information regarding the Emergency Alert System. This includes its purpose, operation, management, your responsibilities as a broadcaster, and the future of EAS and DASDEC/One-Net.

EAS Message Protocol

This sub-tab 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 is contained in this sub-tab. This list coincides with available EAS Codes throughout the web interface.

Status

The **Status** navigation tab 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 it displays.

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, and 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. support for a single hub extender, and optimized matching for specific USB devices
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.

The screenshot displays the 'Status > Main' screen of the DASDEC software. The interface includes a navigation bar at the top with tabs for 'Main', 'GPIO', 'Network', 'Operating System', 'USB', 'CPU', 'PCI', 'IO', and 'Email'. The 'Main' tab is currently selected. The main content area shows the following information:

- Platform ID:** PROEEADTYU9KW/NSJM19/
- Server Name:** DASDEC EAS Decoder
- System Uptime:** 11:51:08 up 14 days, 14 min, 0 users, load average: 0.12, 0.10, 0.11
- Decoder and Other Server Status:** A table listing decoders (L1, R1, L2, R2) with columns for Active status, Input Level, and Mixer. All decoders are active with input levels around 35-40 and are connected to mixers (dev/mixer0 or dev/mixer2).
- 3 Radio Tuner's:** A section showing three FM radio frequencies: 1. FM 102.5 MHz (0%), 2. FM 94.5 MHz (0%), and 3. FM 107.1 MHz (0%).
- DASDEC Server GPIO Table:** A table at the bottom showing the status of various GPIO inputs and outputs. For example, 'Front Panel Button Press' is 'Current Status: Open (OFF)', 'GPI Input 1: Run Msg/Text Template' is 'Current Status: Open (OFF)', 'GPI Input 2: Unused' is 'Current Status: Open (OFF)', and 'Main audio passthrough' is 'Internal audio: ON'.

Status > Main Screen

Logs

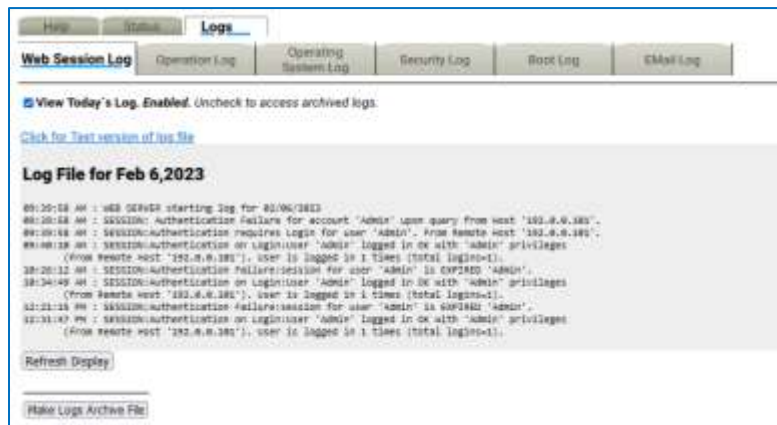
The **Logs** navigation tab has six sub-tab options: **Web Session Log**, **Operation Log**, **Operating System Log**, **Security Log**, **Boot Log**, and **Email Log**.

Sub-Tab	Description
Web Session Log	Displays user access to the EAS device.
Operation Log	Shows the EAS device operation log, including EAS event information.
Operating System Log	Presents the last 500 lines of current and previous backup logs.
Security Log	Presents the last 500 lines of security logs.
Boot Log	Presents the last 500 lines of boot logs.
Email Log	Presents the last 500 lines of email logs.

Web Session Log

The **Web Session Log** sub-tab presents time stamped information about user access to the unit. It shows exactly who and when a user logged on or attempted to log on to 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.



Logs - Web Session Log Sub-Tab

Log files a day old or more can be deleted using the **Delete** button. The page can be refreshed by using the **Refresh Display** button at the bottom of the page to show new information.

Operation Log

The **Operation Log** sub-tab 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

The **Operating System Log** sub-tab presents the last 500 lines of the current and previous backup of the Linux System Log.

Security Log

The **Security Log** sub-tab presents the last 500 lines of the Linux System Security Log.

Boot Log

The **Boot Log** sub-tab presents the last 500 lines of the Linux System Boot Log.

Email Log

The **Email Log** sub-tab presents the last 500 lines of the Linux System Email Log. Also, it has a list of the Email Submission Queue and the Email Send Queue.

Debug Logs

The **Debug Logs** sub-tab is only available when the **Debug Log Interface** check box is enabled within the **Setup > Main > Options** screen. These logs provide customer service engineers with a better view of what is happening within the EAS device. For each of these sub-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-categories. When debugging is no longer needed, make sure to uncheck the **Debug Log Interface** check box.

Appendix

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 ensure 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 to dangerous conditions. Over seventy percent of all EAS and EBS activations have been 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 the 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 <http://www.fcc.gov/emergency-alert-system>. The FCC provides handbooks in 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. 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.

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 option requires 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 have 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 an 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 an 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 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:

www.digitalalertsystems.com/application-notes.

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):

(a) 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.

(1) 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.

(2) 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.

(3) The message may be audio, video, or text.

(b) 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.

(c) 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 the Originator Code table below.

EEE- This is the Event code and indicates the nature of the EAS activation. The codes are specified in the Event Code tables below. 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. 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.

The Only Originator (ORG) Codes:

Originator Description	Originator Code
Code Broadcast station or cable system	EAS
Civil authorities	CIV
National Weather Service	WXR
Primary Entry Point System (United States Government)	PEP

Event (EEE) codes that are presently authorized

The following tables include 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)
National Emergency Message	EAN (National only)	Emergency	:00
Nationwide Test	NPT (National only)	Test	:00
National Information Center (deprecated in 12/2023))	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	EWV	Warning	:15
Evacuation Immediate	EVI	Emergency	:15
Fire Warning	FRW	Warning	:15
Flash Flood Warning	FFW	Warning	:15

Nature of Action	Event Code	Type	Delay (:mm)
Flash Flood Watch	FFA	Watch	:15
Flash Flood Statement	FFS	Advisory	:15
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	Advanced Emergency Alert. A key component of ATSC 3.0 - the next generation broadcasting standard. 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. 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), Caribbean Barbados (CAP) and the United States (IPAWS-OPEN).
CAT-5 Cable	Category 5 cable. 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.
CIDR	Classless Inter-Domain Routing (CIDR) notation used to support single-character “?” wildcard.
CG	Character Generator. 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. 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	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	Federal Communications Commission. An independent U.S. government agency overseen by Congress that 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	Federal Information Processing Standards codes. Geographic codes developed that establish six-digit numeric values for US states, counties, subdivision of counties, and other predefined geographic boundaries.
FSK	Frequency-shift keying. 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. 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 reference to data the reader can directly follow either by clicking or hovering over. Can point to a whole document or to a specific element within a document. Typically displayed in blue, underlined text: FIPS Groups .
IP Address	Internet Protocol address. 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).
IPAWS	Integrated Public Alert and Warning System
LED	Light-emitting diode. 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	Moving Picture Experts Group. 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. 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. 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	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. 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 in the early 1940s for internal connection of the pickup to the chassis in home radio-phonograph consoles.
RJ45 Connector	Also known as 8 position 8 contact (8P8C). 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	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 set top boxes that are sold to retail consumers, 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.
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 connectors 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. 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. The analog computer display standard found within the 15-pin D-subminiature VGA connector.
Web Browser	Commonly referred to as a browser. 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, Microsoft Edge, Mozilla Firefox, and Opera.
XLR Connector	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.

Unauthorized Third Party Software/Firmware/Hardware

The DASDEC™/One-Net™ is a specialized appliance, not a general server product. Any modifications may cause issues with the proper functioning of the device, including disabling features, removal of security features, application instability, degradation of performance, and potential incompatibility with future software updates.

THE INSTALLATION OF ANY THIRD-PARTY PRODUCTS – HARDWARE OR SOFTWARE - OTHER THAN THOSE AUTHORIZED BY DIGITAL ALERT SYSTEMS (DAS) VOIDS ALL WARRANTIES.

Violating the warranty means DAS does not promise to support any repair, service, or replacement of a device having such third-party applications installed. DAS makes no warranty, implied or otherwise, regarding the performance or reliability of any third-party products (hardware or software).

The customer fully assumes all risks related to voiding equipment support, including any costs for repair and/or replacement, and non-compliance with any applicable regulatory rules should the third-party software interfere with the intended function and operation of the product.

Return to Factory Policy

Materials returned to Digital Alert Systems must have a Return Material Authorization number. To obtain an RMA number, contact Customer Service at 585-765-2254 or fax 585-765-9330. Customers have 30 days to determine that the product ordered fills their needs and performs as described in the applicable literature. Units returned for approved repair or credit must be in the original packaging, including all parts and paperwork, plus be in very good physical condition. If not, the customer is billed for the cost to refurbish the unit and for missing accessories and merchandise. No products may be returned for exchange or credit after 12 months from the shipment date. Digital Alert Systems reserves the right to repair or replace units under warranty.

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-III, 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. **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.