If the EAS device does have a current active custom message alert, that alert will appear on the right side of the page in red.

If the **NET Decode Custom Message Forwarding** is enabled, more options appear.

Allow message stop from master NET message originator
This option allows the EAS device that sent a custom message via EAS NET to control when the alert is stopped on the receiving EAS device. If this is not enabled, the user would manually stop the alert on the receiving EAS device (if it is before the alert is done).

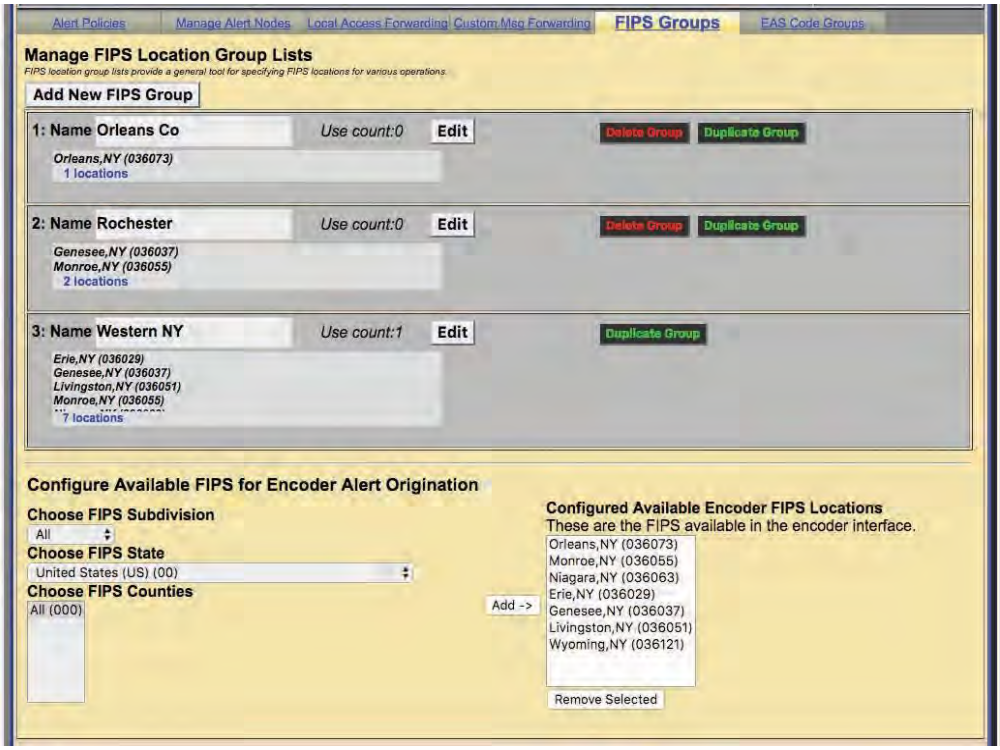
Text Message to Speech Options
This drop down menu gives the EAS device the ability to use a text-to-speech engine on EAS NET decoded custom alerts. There are three options:

- Never use message text-to-speech
- Use message text-to-speech only if Audio not present
- Always use message text-to-speech. Ignore Audio if present.

Auto-Forward NET decoded Custom Messages
This option gives the EAS device the ability to auto forward decoded EAS NET custom messages, even if the EAS device is in Manual Forwarding Mode.

FIPS Groups

The **FIPS Groups** sub-tab screen was first introduced within V3.0 software. Throughout the user interface there are numerous places to enter FIPS Location Codes. In an effort to eliminate redundant operations and reduce errors, FIPS code Groups were created. Users can create and modify groups of FIPS Codes in one central area and use those groups throughout the web interface. This screen is also where a list of available encoder FIPS code locations is established. The **FIPS Group** sub-tab has two sections; **Manage FIPS Location Group Lists** section and the **Configure Available FIPS for Encoder Alert Origination** section.



Manage FIPS Location Group Lists Screen

Manage FIPS Location Group Lists

This section of the screen displays a list of existing FIPS Groups and enables users to add, edit, duplicate and delete FIPS Groups. A brand new EAS device will not have any configured FIPS code groups - they will need to be added on this screen.

Add New FIPS Group

To create a new FIPS Group click the **Add New FIPS Group** button. A new FIPS group will appear at the top of the FIPS Location Group Lists and will have an auto-generated name, starting with a series of numbers and ending in '_FIPS'. This group will have no defined FIPS codes and will need to be edited.

Individual FIPS Groups contain the following information and action buttons:

Name

Name of the FIPS Group.

Use Count

Number of times this FIPS Group is used throughout the web interface.

FIPS Codes List

Displays the first four FIPS codes used in the group, along with a number of FIPS code locations contained in the group.

Edit

This button opens the edit FIPS Group interface. Here FIPS codes are added and removed in the group and the group name can be edited.

Duplicate Group

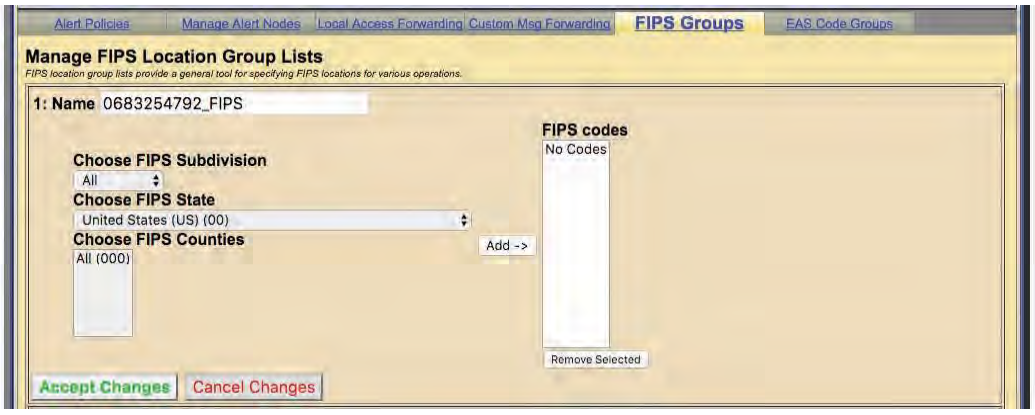
Clicking this button will create a duplicate FIPS Group and place it below the original. It copies the existing group name and adds '.CPY' at the end.

Delete Group

Users wanting to delete a FIPS Group can click this button. This button is only available to groups not being used throughout the web interface. (See **Use Count** above.) Once the Delete Group button is clicked, a confirmation screen will appear asking: **Are you sure you want to delete the selected FIPS group?**

User may select either:

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



Edit FIPS Group Section

To edit a new or existing FIPS Group, click the corresponding **Edit** button. User have the ability to change the name and add/remove FIPS codes within this group. The following fields, pull-downs, and buttons are available:

Name
The EAS device automatically generates a name for new FIPS Group. Highlight the text and enter a descriptive name for this group of FIPS codes.

Choose FIPS Subdivision
A pull-down menu showing the subdivision setting of the chosen FIPS County. A selection of **All** should be used unless the county is to be subdivided. To subdivide a county:

- Select one of the FIPS Subdivisions options (North, Northeast, West, etc.)
- Select a FIPS County
- Click the **Add** button to add that subdivision to the **FIPS codes** list.

Multiple subdivisions of a single county can be added to the **FIPS codes** list by repeating the above steps. For example, both North Orleans, NY and Northeast Orleans, NY FIPS codes can be added.

Choose FIPS State
This pull-down contains a list of US States, territories and pre-defined FIPS regions. Select the desired item and the EAS device will populate the **Choose FIPS Counties** with the FIPS codes available for that area in numeric order.

Choose FIPS Counties
This area is populated with individual FIPS codes based on the selection made in the **Choose FIPS State** pull-down menu. It is from this area that FIPS codes are added to the **FIPS codes** list for the group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection.

FIPS Codes
This area represents a list of FIPS codes used in the group. Only FIPS codes found in this area will be used for processing wherever this FIPS group is selected. FIPS codes are added to this list by selecting the desired codes from the FIPS Counties list and clicking the **Add ->** button. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->
Clicking this button will add the selected **FIPS Counties** to the **FIPS codes** list area.

Remove Selection
FIPS code can be removed from the **FIPS codes** list by selecting the item and clicking the **Remove Selected** button.

Accept Changes
This button will finalize any additions, edits, and/or deletions made while editing a FIPS code group. Once clicked, the Edit FIPS group section of the interface will be removed and the screen will return to its normal state.

Cancel Changes
Pressing this button will cancel any changes made to the FIPS group and return this screen to its normal state.

Caution
Check to make sure **All** is selected in the **Choose FIPS Subdivision** drop-down menu. Selecting another option in this menu will sub-divide the selected **FIPS Counties** and may result in EAS alerts being missed. Double check that subdividing a county will trigger the proper alerts.

Configure Available FIPS for Encoder Alert Origination
The **Send Alerts** tab is where users configure and send alerts from the EAS device. A list of FIPS codes for available locations where these alerts may be sent is configured in the lower section of the screen. The interface operates similarly as the edit FIPS group interface:

Choose FIPS Subdivision
A pull-down menu showing the subdivision setting of the chosen FIPS County. A selection of **All** should be used unless the county is to be subdivided. To subdivide a county:

- Select one of the FIPS Subdivisions options (North, Northeast, West, etc.)
- Select a FIPS County
- Click the **Add** button to add that subdivision to the **FIPS codes** list.

Multiple subdivisions of a single county can be added to the **FIPS codes** list by repeating the above steps. For example, both North Orleans, NY and Northeast Orleans, NY FIPS codes can be added.

Choose FIPS State
This pull-down contains a list of US States, territories and pre-defined FIPS regions. Select the desired item and the EAS device will populate the **Choose FIPS Counties** with the FIPS codes available for that area in numeric order.

Choose FIPS Counties
This area is populated with individual FIPS codes based on the selection made in the **Choose FIPS State** pull-down menu. It is from this area that FIPS codes are added to the **FIPS codes** list for the group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection.

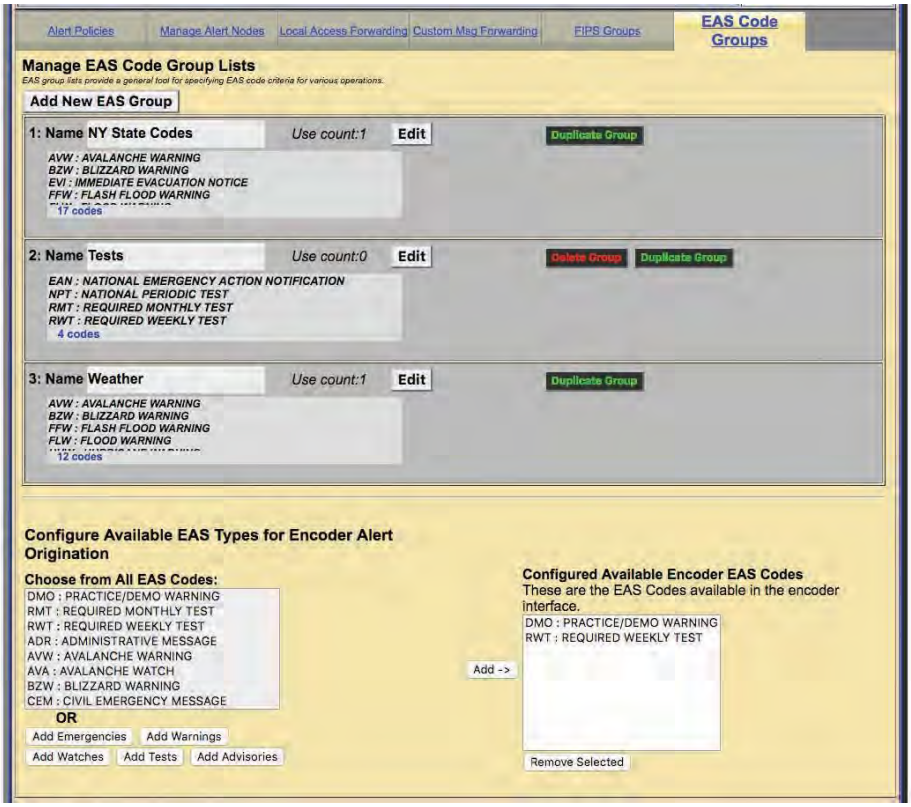
FIPS Codes
This area represents a list of FIPS codes used in the group. Only FIPS codes found in this area will be used for processing wherever this FIPS group is selected. FIPS codes are added to this list by selecting the desired codes from the FIPS Counties list and clicking the **Add ->** button. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->
Clicking this button will add the selected **FIPS Counties** to the **FIPS codes** list area.

Remove Selection
FIPS code can be removed from the **FIPS codes** list by selecting the item and clicking the **Remove Selected** button.

EAS Code Groups

EAS Code Groups were first introduced with V3.0 software. There are numerous places to enter EAS codes within the web interface. EAS Code Groups were created to eliminate redundant operations and reduce errors. The EAS Code Groups sub-tab is divided into two sections. The **Manage EAS Code Group Lists** section provides controls to add, edit, duplicate and delete these groups. The **Configure Available EAS Types for Encoder Alert Origination** section is where users establish a list of available encoder EAS codes.



EAS Code Groups Sub-Tab

Manage EAS Code Group Lists

The top section of this screen shows a list of configured EAS Code Groups and enables the user to add, edit, duplicate and delete these groups.

Add New EAS Group

To add a new EAS Group, first click the **Add New FIPS Group** button. A new EAS group will appear at the top of the EAS Code Group Lists and have an automatically generated name starting with a series of numbers and ending in '_EAS'. This group will have no defined EAS codes and will need to be edited.

EAS Code Groups contain the following information and action buttons:

Name

The name of the EAS Code.

Use Count

Number of times this EAS Code is used throughout the web interface.

EAS Codes List

Displays the first four EAS codes used in this group along with a number of EAS codes contained in this group.

Edit

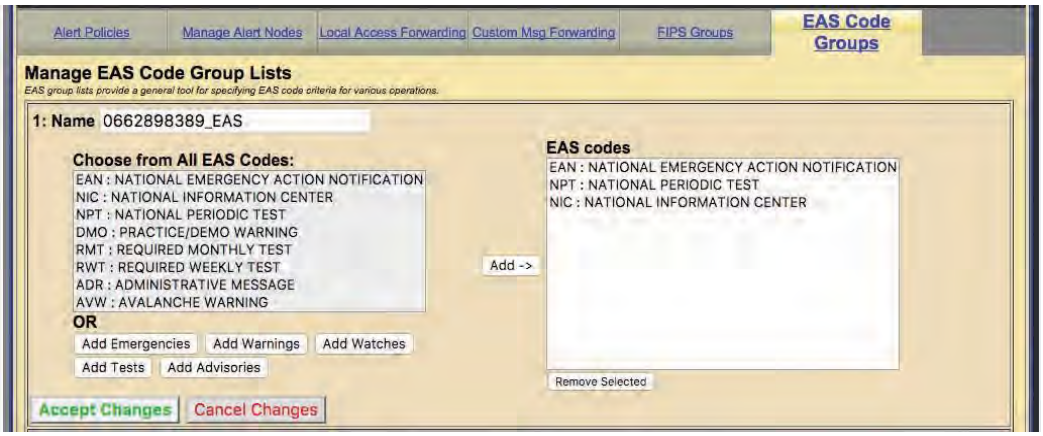
This button opens the edit EAS Code interface where EAS codes are added and removed within this group and where the group name can be edited.

Duplicate Group

Clicking this button will create a duplicate EAS Code Group and place it below the original. The duplicate group copies the existing group name and adds '.CPY' to the end of it.

Delete Group
Users wanting to delete a EAS Code can click this button. This button is only available to groups not being used throughout the web interface. (see Use Count) Once the Delete Group button is clicked, a confirmation screen will appear asking: **Are you sure you want to delete the selected EAS Filter group?** User may select either:

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



Edit EAS Code Group Section

Attention
EAN, NPT, and NIC codes are automatically added to new or empty EAS Code Groups to insure they are utilized when filtering in any area of the web interface. These national codes may be removed in instances where they are not needed.

To edit a new or existing EAS Code Group, click the corresponding **Edit** button. The user will have the ability to change the name and add/remove EAS codes within this group. The following fields, pull-downs, and buttons are available:

Name
An automatically generate name is found in the **Name** field. Highlight the text in this field and enter a descriptive name for this group of EAS codes.

Choose from All EAS Codes:
This area contains all the EAS codes. It is from this area (and the **Quick Add** buttons just below) that EAS codes are added to the **EAS codes** list for this group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection. Both a mouse scroll (while the mouse hovers over this area) and keyboard up/ down arrows will allow users to scroll the entire list of codes.

Quick Add Buttons
These five buttons, located just below the **Choose from All EAS Codes**: area, will quickly add their respective codes to the EAS codes list – foregoing the use of the **Add ->** button. The five Quick Add buttons are:

- **Add Emergencies** – contains all emergency related codes
- **Add Warnings** – contains all the warning codes
- **Add Watches** – contains all the watches codes
- **Add Tests** – contains all the test codes
- **Add Advisories** – contains all the advisory codes

EAS Codes
This area displays a list of EAS codes used in the group. Only EAS codes found in this area will be used for processing wherever this EAS group is selected. EAS codes are added to this list by selecting the desired codes from the **Choose from All EAS Codes** list and clicking the **Add ->** button. Alternatively, clicking the Quick Add buttons will add the associated codes to this area. Items are removed from this list by selecting the item(s) and clicking the **Remove Selected** button.

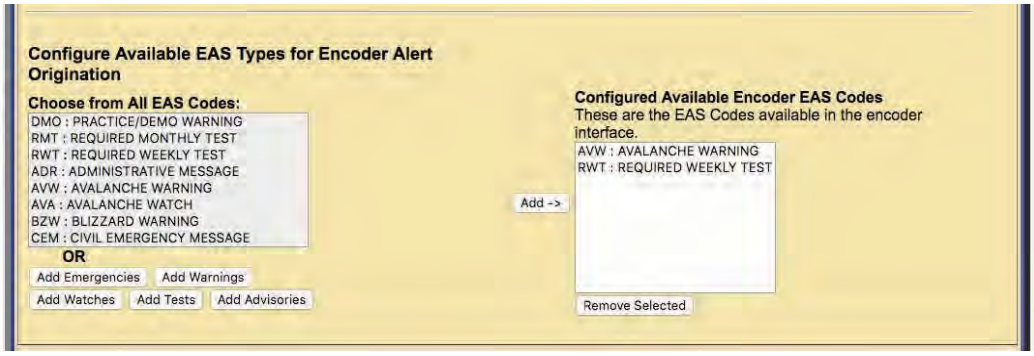
Add ->
Clicking this button will add the selected **Choose from All EAS Codes** to the **Configured Available Encoder EAS codes** list area.

Remove Selection
EAS code can be removed from the **EAS codes** list by selecting the item and clicking the **Remove Selected** button.

Accept Changes
This button will finalize any additions, edits, and/or deletions made while editing a EAS code group. Once clicked, the Edit EAS code group section of the interface will be removed and the screen will return to its normal state.

Cancel Changes
Pressing this button will cancel any changes made to the EAS code group and return this screen to its normal state.

Configure Available EAS Types for Encoder Alert Origination
The **Send Alerts** tab is where users can configure and send alerts from the EAS device. A list of EAS codes for available locations where these alerts may be sent is configured in the lower section of this screen. The interface operates similarly as the edit EAS code group interface.



Configure Available EAS Types for Encoder Alert Origination Section

Choose from All EAS Codes:
This area contains all the EAS codes. It is from this area (and the **Quick Add** buttons just below) that EAS codes are added to the **EAS codes** list for this group. Make a selection by clicking on the desired item. Multiple selections can be made by using the CTRL key when clicking items after the first selection. Both a mouse scroll (while the mouse hovers over this area) and keyboard up/ down arrows will allow users to scroll the entire list of codes.

Quick Add Buttons
These five buttons, located just below the **Choose from All EAS Codes**: area, will quickly add their respective codes to the EAS codes list – foregoing the use of the **Add ->** button. The five Quick Add buttons are defined above.

Configured Available Encoder EAS Codes
This area represents a list of available EAS codes when sending alerts. Only EAS codes found in this area will be available to the user. EAS codes are added to this list by selecting the desired codes from the **Choose from All EAS Codes** list and clicking the **Add ->** button or by using the **Quick Add** buttons. Items are removed from this list by selecting the item and clicking the **Remove Selected** button.

Add ->
Clicking this button will add the selected **Choose from All EAS Codes** to the **Configured Available Encoder EAS codes** list area.

Remove Selection
FIPS code can be removed from the **EAS codes** list by selecting the item and clicking the **Remove Selected** button.

STATION SETUP

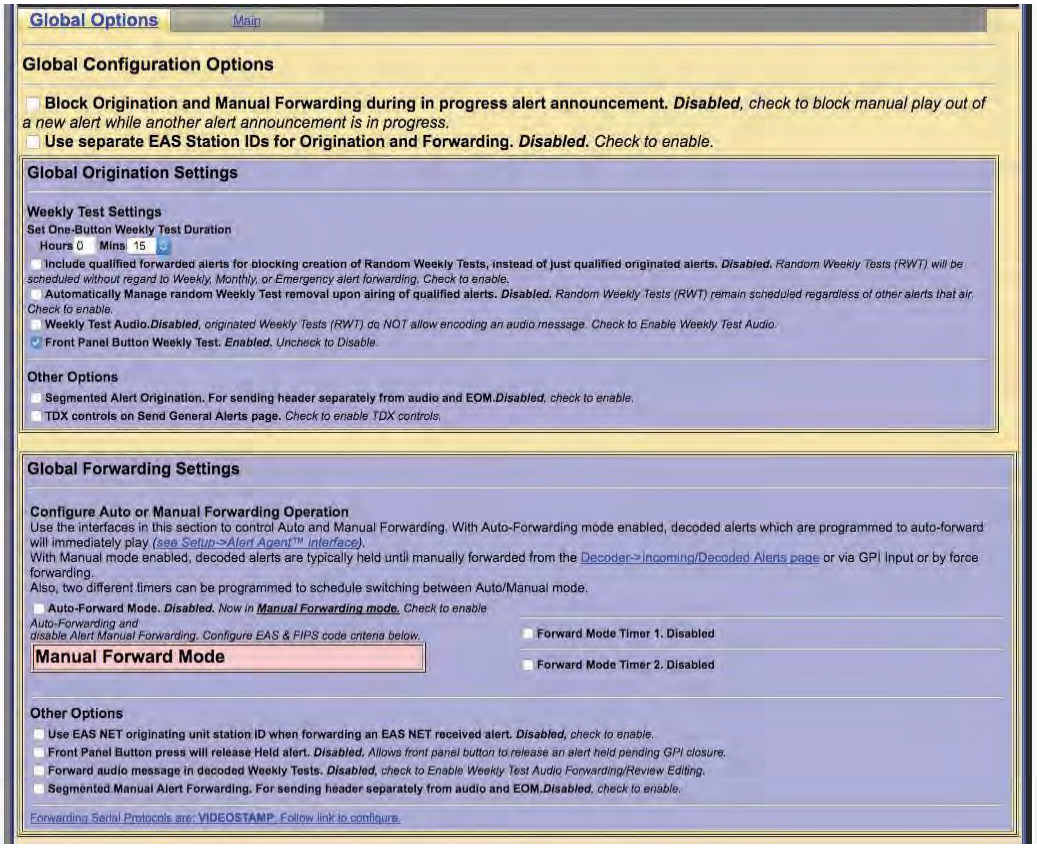
The **Station** radio button within the **Setup** tab is where station alert originations and alert forwarding settings are located. The origination settings primarily focus on Required Weekly Test settings. There are two standard sub-tabs: **Global Options** and **Main**.

The standard **Station** sub-tabs are described as follows:

Sub-Tab	Description
Global Options	Configuration of global origination (Required Weekly Tests) and forwarding settings. Auto-Forward Mode settings are found here.
Main	Station specific ID, language settings in addition to origination and forwarding settings

When using **MultiStation** mode, the web interface displays additional sub-tabs, one for each station and a simultaneous station override sub-tab. Using these additional settings, the EAS device can handle each stations' ID, languages, origination, and forwarding settings separately.

Sub-Tab	Description
Global Options	Configuration of global origination (Required Weekly Tests) and forwarding setting. The Auto-Forward Mode settings are found here.
Simultaneous Station Override	Simultaneous ID, language settings in addition to origination and forwarding settings
Station 1 - 5	Station specific ID, language settings in addition to GPIO handling, origination and forwarding settings. The number of station sub-tabs will depend on license key – with MultiStation 2 or 5.



Station Setup Screen

Global Options

Block Origination and Manual Forwarding during in progress alert announcement
Check to block manual play-out of a new alert while another announcement is in progress. If left unchecked, the alerts will play sequentially.

Use separate EAS Station IDs for Origination and Forwarding
Enables the user to configure a different **EAS Station ID** for the Origination Settings and the Forwarding Settings. These settings are found within the **Setup > Station > Main** screen. A valid Plus Package License Key is required.

Global Origination Settings

This section of the screen has two distinct parts: **Weekly Test Settings** and **Other Options**.

Weekly Test Settings

Set One-Button Weekly Test Duration
Input the duration of the RWT in hours and minutes. The default time is 15 minutes.

Include qualified forwarded alerts for blocking creation of Random Weekly Tests, instead of just qualified originated alerts.

Random Weekly Tests (RWT) will be scheduled without regard to Weekly, Monthly, or Emergency alert forwarding. Check to enable.

Automatically Manage random Weekly Test removal upon airing of qualified alerts

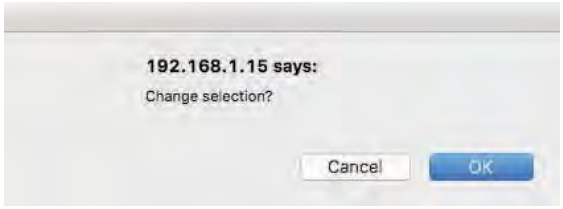
Random Weekly Tests (RWT) remain scheduled regardless of other alerts that air. Check to enable.

Note
The minimum duration of any EAS alert is 15 minutes. This time setting represents the duration of the alert itself, and does not reflect the amount of time the alert is broadcast.

Weekly Test Audio
Default is disabled. This controls whether the originated Weekly Test (RWT) can be constructed with an audio message. The audio message is configured within the **Weekly Test Settings** inside the **Origination Settings** section of the **Setup > Station > Main** screen labeled **Optional Alert Audio Announcement**. – this option requires a valid Plus Package license key.

Front Panel Button Weekly Test
Check this box to initiate an RWT using the front panel button.

A confirmation page has been added when making changes to FIPS Groups and the Audio File selectors within the **Required Weekly Test** settings due to the importance of these settings.



Other Options

All these other options require a Plus Package License Key

Segmented Alert Origination
Default is disabled. This controls whether the option for segmented alert origination is available on the **Send Alerts> General Alerts** screen. Segmented alert origination is when the alert header and attention signal are played with a pause for live audio voice dub. A separate button allows the play-out of audio files and EOM. (In EAS, the End of Message (EOM) is signaled by the final three FSK audio bursts.)

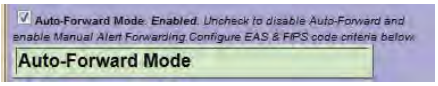
TDX controls on Send general EAS page
Check to enable TDX controls (requires a TDX license key) found within the **Send Alerts > General Alerts** screen. Requires a valid TDX license key.

Global Forwarding Settings

Configure Auto or Manual Forwarding Operation
One essential decision that an EAS participant must make is whether to run an EAS decoder in Auto-Forward mode or Manual Forwarding mode. This section provides the controls over these two options.

The text box on the left side of this section indicates the current forwarding state. It will display either “Auto-Forward Mode Enabled” or “Manual Forward Mode”. The same information is also displayed on the Alert Events > Incoming Alerts pages. To set the Auto-Forward Mode or the Manual Forward Mode look to the check box to on the right side of this section.

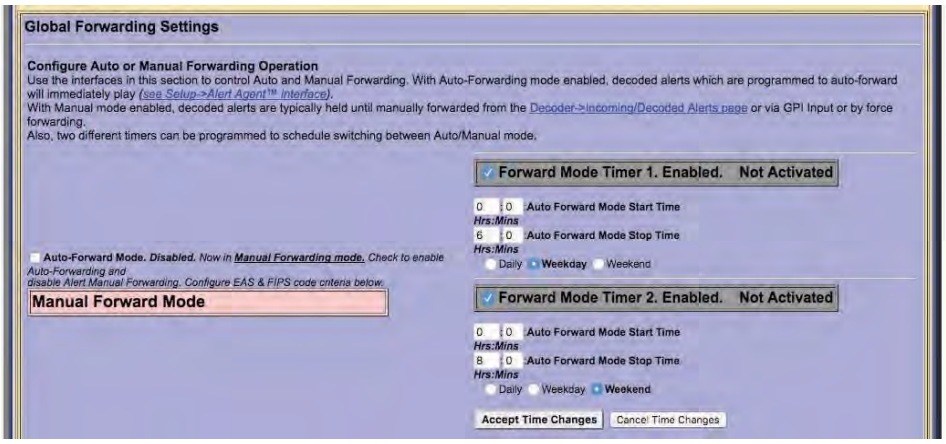
Auto-Forward Mode
Check the first check box to enable Auto-Forwarding. Uncheck to select Manual Forwarding. A large button that says “Manual Forward Mode” or “Auto Forward Mode” will be displayed.



Note
Emergency National Activation (EAN) and National Periodic Test (NPT) alerts always forward automatically.

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

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



Global Forwarding Setting with Timers enabled

Forward Mode Timers

All licensed versions feature two Forward Mode Timers that can be enabled independently to automatically switch the EAS device between Manual and Automatic Forwarding modes. The timers can be set to run on a daily basis, or just on weekends or weekdays. Each timer has a time setting for enabling Auto-Forwarding and later disabling Auto-Forwarding. Active timers override the check box for setting Auto/Manual Forward Mode. The timers allow a station to schedule auto-forwarding when unmanned and manual forwarding at other times. For both timers, the start and stop time fields need to be modified by the system administrator to configure when the EAS device will go into Auto-Forward mode and when will go back to Manual mode. In the screen shot above, Auto-Forward Mode is active from midnight to 6:00am on Weekdays and from midnight to 8:00am on Saturday and Sunday.

Other Options

Use EAS NET originating unit station ID when forwarding an EAS NET received alert

Check to enable.

Front Panel Button press will release Held alert

Allows front panel button to release an alert held pending GPI closure.

Forward audio message in decoded Weekly Tests

If a decoded Required Weekly Test (RWT) has audio, it will be forwarded. This is uncommon, but can occur. When disabled, decoded RWT alerts with audio will discard the audio portion of the RWT during forwarding.

Segmented Manual Alert Forwarding

If enabled, manual forwarding will provide buttons to send the alert header and attention signal separately from audio and EOM. This provides an opportunity to dub in live audio. Uncheck to disable.

Main

The screen provides controls to set the basic values to construct an EAS alert and contains three sections; general station settings, Origination Settings, and Forwarding Settings.

EAS Station ID
Type up to 8 characters in this text field to identify the Station ID. This code is included in all originated alerts, both manually forwarded and automatically forwarded alerts.

Uses Server Timezone:
Displays the configured time zone. To change this setting, go to **Setup > Time**.

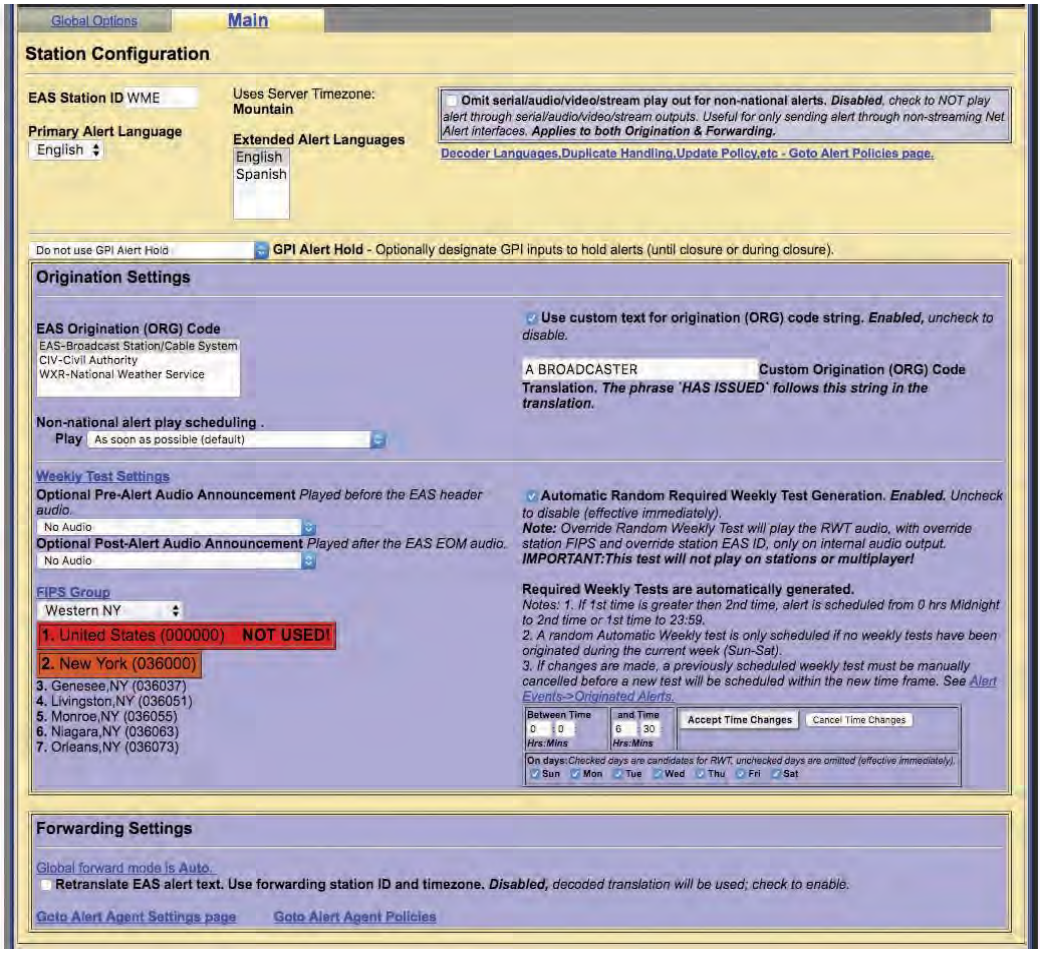
Primary Alert Language
This pull-down menu is used to select the primary alert language. A list of available languages is displayed.

Extended Alert Language
A list of available languages is displayed within this box. Select one language by clicking it. Multiple languages may be selected by using the CTRL key when making additional selections.

Omit serial/audio/video/stream play out for non-national alerts
Check to NOT play alert through serial/audio/video/stream outputs. Useful for only sending alert through non-streaming Net Alert interfaces. Applies to both Origination & Forwarding.

GPI Alert Hold
Optionally designate GPI inputs to hold alerts (until closure or during closure). When using the last two options, a list of GPI's is available for selection.

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



Main Sub-tab Screen

Origination Settings

EAS Origination (ORG) Code

The ORG code is a standard part of the EAS audio protocol. It is placed in the EAS alert message when the encoder originates an EAS alert. The same code is used for forwarded alerts. MultiStation operation allows this value to be overridden per station definition. This code categorizes the type of organization sending the EAS. Use the selection menu to choose the EAS Origination code for your system:

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

Custom text for origination (ORG) code string

Default is disabled. The origination codes are given a standard text translation when an encoded EAS alert is sent to a video display. When an EAS origination code is used, the alert text will start with the phrase “A Broadcast or Cable System has issued.” Checking the Custom Text option allows a custom translation to be used instead.

In the screen shot above, Custom Text is enabled. When enabled, a text entry box is displayed in which you can enter the organization name issuing the alert for Custom Origination (ORG) Code Translation. In the screen shot, the phrase, "A BROADCASTER" has been entered as the custom text. The EAS translation text will use this phrase instead of the generic "A Broadcast or Cable System." The phrase "HAS ISSUED" follows the custom organization name in the alert translation.

Non-national alert play scheduling

Set the play scheduling for the originating alert. The options are as follows:

- **As soon as possible** (default) – after the incoming alert message is decoded, it is played - beginning at the start time of the alert message.
- **As late as possible** – after the incoming alert message is decoded, it is held and then played just before the end of the valid alert time period.
- **Top of next minute interval** (MM:00) – the alert 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.

Weekly Test Settings

Optional Pre-Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played prior to the EAS header audio.

Optional Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played following the EAS header audio and the attention two-tone signal. Only available if option is enabled within the **Setup > Station > Global Options** (**Weekly Test Audio** check box)

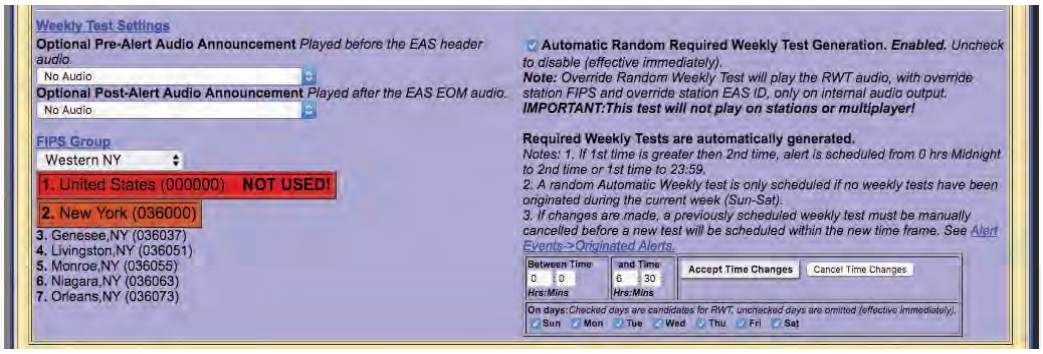
Optional Post-Alert Audio Announcement

The pull-down menu for this option displays the available audio files that can be played after the EAS end of message (EOM) audio.

FIPS Group

Make a selection from the pull-down list to designate the desired FIPS Codes Group.

Notice the color coding of the United States code (000000) in red and the state-wide code (New York in the below example) in orange. The EAS device will block the use of the United States FIPS code and any 'wildcarded' state codes when originating alerts along with including the text "NOT USED". The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but likely not very common.



Weekly Test Settings Section

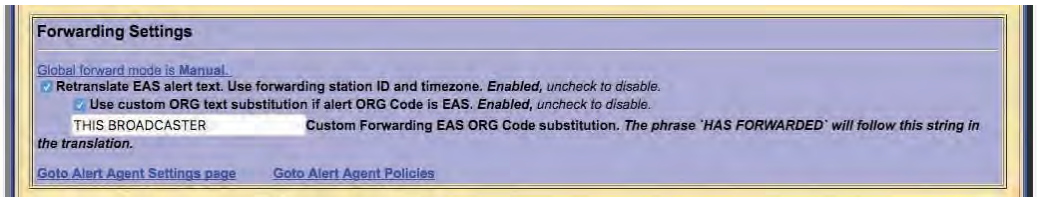
Automatic Random Required Weekly Test Generation
The check box allows you to enable Required Weekly Tests to be automatically generated at a random time within a pre-selected time frame for specifically selected days. If enabled, controls are displayed that allow setting the time period and the days for which the test will be scheduled.

Between Start Time and End Time
Enter start time, then end time, in hours and minutes.

On days
Check the days the Required Weekly Test could be generated. The RWT will not occur on a day that is unchecked.

Time Configuration Notes

- When configuring the time period, if first time is greater than the second time, the alert will be scheduled at a random time from 0 hrs. Midnight to second time or first time to 23:59. If the first time period is less than the second, the alert will be scheduled at a random time between the first and the second time entry.
- A random Automatic Weekly test is only scheduled if no weekly tests have been originated during the current week (Sun-Sat).
- If changes are made, a previously scheduled weekly test must be manually cancelled before a new test will be scheduled within the new time frame. Go to **Alert Events > Originated Alerts** to view and/or cancel any scheduled originated alerts.



Forwarding Settings

Retranslate EAS alert text. Use forwarding station ID and time zone
To retranslate the EAS alert text, check the box. When not checked the decoded translation will be used.

Use custom ORG text substitution if alert ORG Code is EAS
When checked a text field appears for a custom originator code (ORG). Enter the desired EAS ORG code.

Simultaneous Station Override (MultiStation Mode)

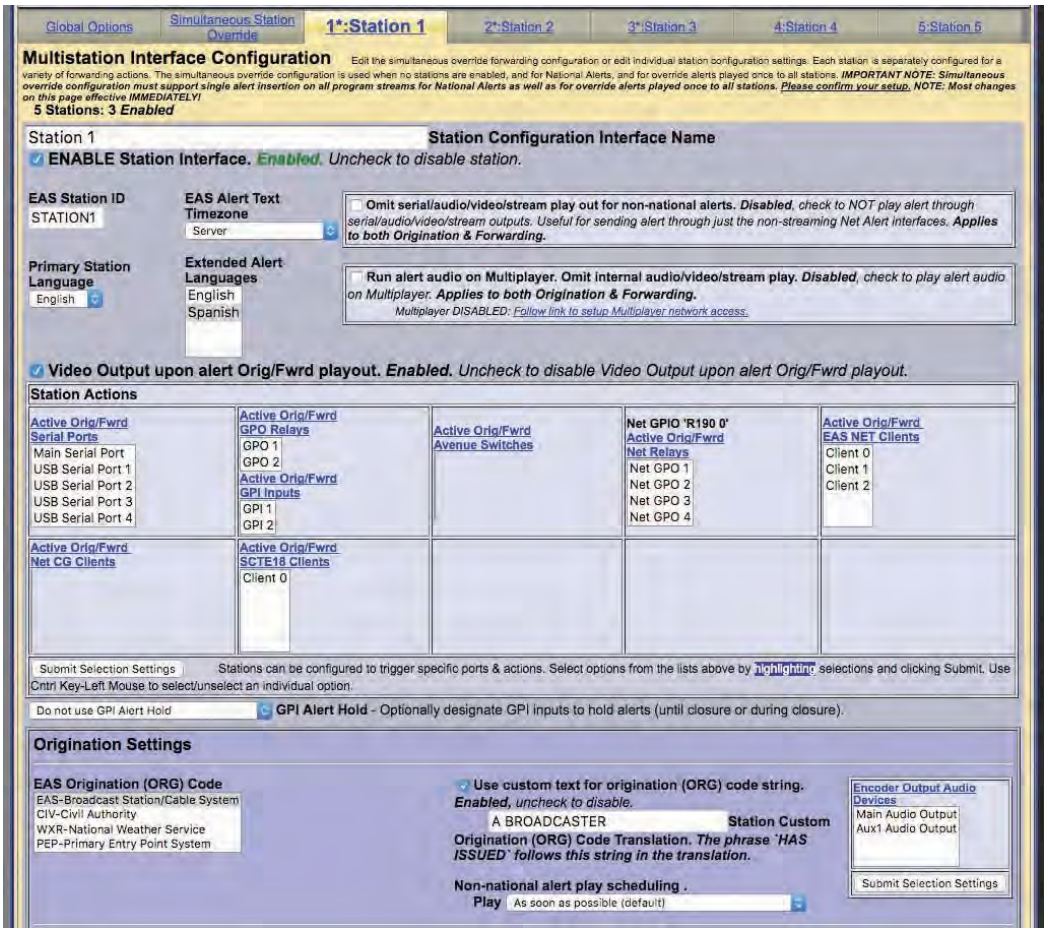
MultiStation mode option enables one EAS device to provide complete EAS coverage for up to five co-located stations or program streams with individual station ID's and logging. GPIO's can be set for each stream according to Station ID, FIPS and/or Event Code. A good portion of the MultiStation specific settings are configured within the **Setup > Station** screens. After the MultiStation license key is installed, the **Main** sub-tab is re-titled **Simultaneous Station Override** and one 'Station' sub-tab is added for each station. A MultiStation 2 will add **Station 1** and **Station 2** sub-tabs while MultiStation 5 will add **Station 1**, **Station 2**, **Station 3**, **Station 4**, and **Station 5** sub-tabs.

Simultaneous Station Override Sub-Tab

The **Simultaneous Station Override** sub-tab has the same controls as the **Main** sub-tab did. The simultaneous override configuration settings are used when no stations are enabled, for national alerts, and for override alerts played once to all stations. **Weekly Test Settings** are only available in this sub-tab if every station sub-tab is disabled.

Station 1 – 5 Sub-Tabs (MultiStation Mode)

Station sub-tabs are displayed when a valid MultiStation license key is enabled. MultiStation 2 will add 2 station sub-tabs and MultiStation 5 will add 5 station sub-tabs. Each Station sub-tab has the exact same controls as the others – enabling users to make configuration for each channel individually. All Station sub-tabs screens contain three sections: general station settings, Origination Settings, and Forwarding Settings.



Station 1 Sub-Tab

The majority of the Station sub-tab configuration settings are described in the Main Sub-tab (above). The following descriptions will highlight specific differences.

Multistation Interface Configuration

Station Configuration Interface Name

Text field that labels the Station sub-tab. The purpose of this name is to label the sub-tab and is not used or included in any EAS alerts messages. Each Station sub-tab starts with a number (1-5) and colon (:) along with a default name of 'Station' followed by a number. In the above example the Station Configuration Interface Name is 'Station 1' and is displayed on the sub-tab as '**1*:Station 1**'. The asterisk (*) denotes that the Station Interface is enabled for that station.

ENABLE Station Interface

This check box enables the station interface for this sub-tab. Checking it will make the following configuration settings active.

EAS Station ID

Type up to 8 characters in this text field to identify the Station ID for this sub-tab. This code is included in all originated alerts, both manually forwarded and automatically forwarded alerts.

EAS Alert Text Timezone

The MultiStation mode allows stations in differing time zones to be configured in the same EAS unit. The default setting is 'Server' which maintains the same time zone that was configured in the **Setup > Time** screen. To change to a different time zone, click the pull-down menu and click the desired selection.

Primary Station Language
This pull-down menu is to select the primary alert language for this sub-tab. Select from the list of available languages.

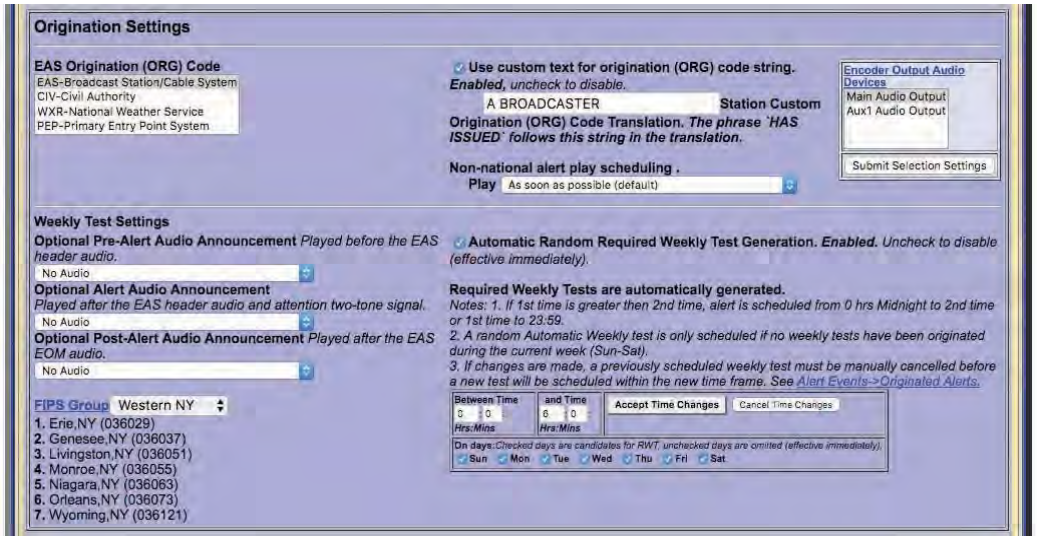
Extended Alert Languages
A list of available extended alert languages is displayed within this box. Select one language by clicking it. Multiple languages may be selected by using the CTRL key when making additional selections.

Omit serial/audio/video/stream play out for non-national alerts
Check to NOT play alert through serial/audio/video/stream outputs. Useful for only sending alert through non-streaming Net Alert interfaces. Applies to both Origination and Forwarding.

Run alert audio on Multiplayer
Due to the limited number of audio outputs in relation to the number of stations controlled by the EAS device in MultiStation mode, Digital Alert Systems Electronics provides an optional MultiPlayer. The MultiPlayer is a separate 1RU chassis that provides up to 5 completely independent EAS audio channels playable at any time. To enable the play out of EAS audio from a MultiPlayer, check this box.

Video Output upon alert Orig/Fwrd playout
For EAS units with internal Video Out; when checked, this setting will utilize the internal video output to generate a full screen alert page for this station.

Station Actions
This section represents a series of serial, GPIO, EAS Net, NET CG's, and SCTE-18 client configuration settings for this station. Select the appropriate settings and click the **Submit Selection Setting** button. Multiple selections can be made by using the CTRL key when making selections.



Station Sub-Tab Origination Settings Section

Note
A MultiPlayer will require proper setup prior to being configured in this screen. Follow the Quick Start Guide included with the MultiPlayer before checking this box.

Origination Settings

The Origination Settings are exactly the same with the exception of the **Encoder Output Audio Devices** settings.

Encoder Output Audio Devices

A list of available encoder output audio devices is presented. Select the desired output and click the **Submit Selection Settings**. Multiple selections can be made by using the CTRL key when making selections.

It is important to note that automatic random **Required Weekly Tests** may be generated for each enabled station. This interface gives users the ability to generate those random RWT's on differing time and day schedules.

Station Sub-Tab Forwarding Settings Section

Forwarding Settings

The Forwarding Settings are exactly the same with the exception of the **Forwarding Output Audio Devices** settings.

Forwarding Output Audio Devices

A list of available forwarding output audio devices is presented. Select the desired output and click the **Submit Selection Settings**. Multiple selections can be made by using the CTRL key when making selections.

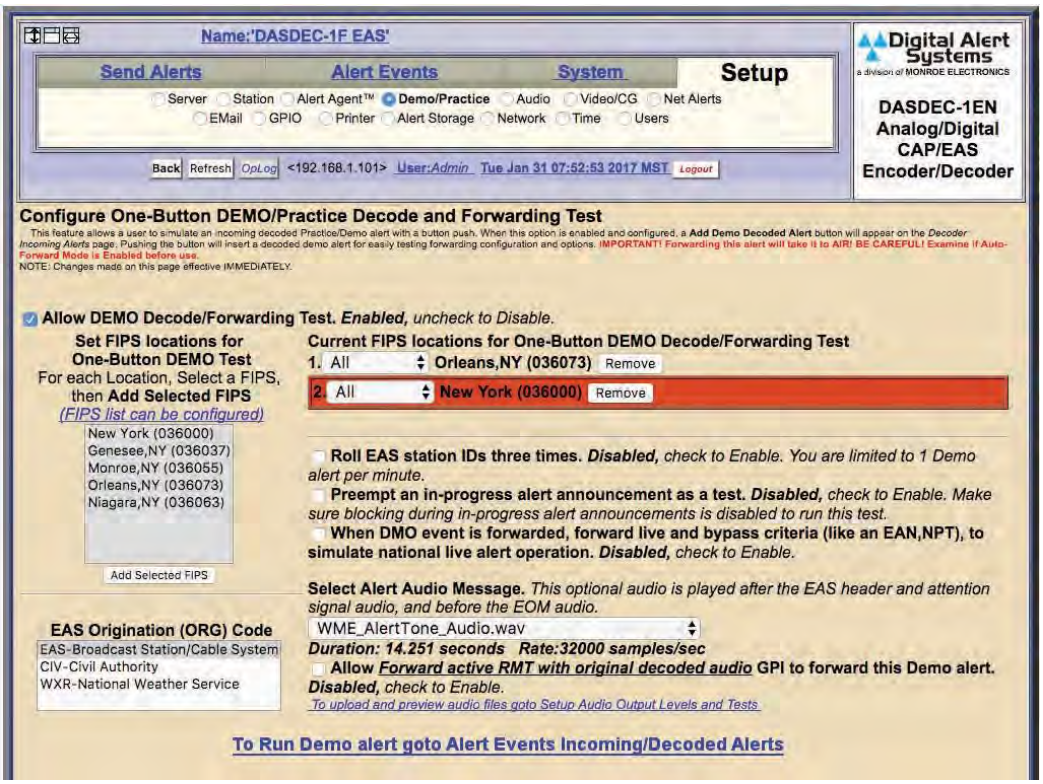
Station Auto-Forwarding Configuration

Auto-Forward mode timers may be configured for each station to accommodate differing program schedules. These control settings are described in detail in the **Setup > Station > Main** screen.

DEMO/PRACTICE SETUP

This page allows you to enable the Practice/Demo operation mode. You can configure alert parameters for a practice and test run of decoding and forwarding. By generating a trial decoded DMO (Demo/Practice Warning) alert, rather than having to wait until an actual alert is received, you can simulate the behavior of any incoming decoded alert on the EAS DEVICE. The actual alert is generated within the **Alert Events > Incoming/ Decoded Alerts** screen. (See Chapter 6 - Incoming/Decoded Alerts for more details). Once generated, all the forwarding buttons and edit/review options for the active alert are available for operation. This feature is especially useful for testing MultiStation operation.

Options on this page configure availability of the Run DEMO button, and FIPS codes and audio for the DMO alert.



Demo/Practice Screen

Configure One-Button DEMO/Practice and Forwarding Test

Allow DEMO Decode/Forwarding Test

When enabled, the **Add Demo Decoded Alert** button is available on the **Alert Events > Incoming/Decoded Alerts** screen.

Set FIPS locations for One-Button DEMO Test

This list is used to select the FIPS codes for the DEMO alert. The list is generated from the **Configure Available FIPS for Encoder Alert Origination** section of the **Setup > Alert Agent™ > FIPS Groups** screen. If a FIPS code is not available from the list, follow the **FIPS list can be configured** hyperlink to add the FIPS code to the available FIPS list.

Warning
BE CAREFUL! Forwarding any Demo/Practice Warning (DMO) will take it to AIR. Examine if Auto-Forward Mode is enabled before use. Make sure your EAS broadcast system is off line during practice.

Select a FIPS code from the list and click the **Add Selected FIPS** button to add to the **Current FIPS locations for One-Button DEMO Decode/Forwarding Test**. Multiple selections can be made using the CTRL key when making selections or they can be added one at a time.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but likely not very common.

Current FIPS locations for One-Button DEMO Decode/Forwarding Test
Contains a list of FIPS codes intended for use with the Demo/Practice Warning test. Each FIPS code has a pull-down menu for subdividing the FIPS location. The default value is 'All'. To delete a FIPS code from this list, click the corresponding **Remove** button.

Roll EAS station IDs three times
When checked, will roll EAS station ID three times. Left unchecked, EAS station ID will roll once.

Preempt an in-progress alert announcement as a test
Check to enable. Make sure blocking during in-progress alert announcements is disabled to run this test. This setting requires Administration-level permission to enable. All other users will see grayed text.

When DMO event is forwarded, forward live and bypass criteria (like EAN, NPT)
Will simulate a national live alert. This setting requires Administration-level permission to enable. All other users will see grayed text.

Select Alert Audio Message
This selector allows an audio message file to be selected for the audio message portion of the DMO alert.

Under the Select Alert Audio Message pull-down menu, a hyperlink labeled **To upload audio files goto Setup Audio Output Levels and Tests** is provided to go to the **Setup > Audio Output Levels/Tests** screen where users can upload and listen to the available audio files (See the Audio Setup section of this chapter).

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

Allow *Forward active RMT with original decoded audio* GPI to forward this Demo alert
This option allows an unforwarded DMO (Practice/Demo Warning) alert to be forwarded by the ***Forward active RMT with Original decoded audio*** GPI.

EAS Origination (ORG) Codes
Displays a list of available EAS Origination (ORG) Codes. Select one of the codes by clicking on it. This code will be used with the Demo/Practice EAS message.

NET ALERTS SETUP

There are up to six sub-tabs within the **Setup > Net Alerts** page. Valid license keys will display the appropriate sub-tabs.

Sub-Tab	Description
DVS168	Configuration of a single DVS-168/EARS client for sending EAS alerts..
EAS NET	Provides a variety of methods to exchange data (including alert notifications) between EAS devices and other remote hosts. Includes support for multiple DVS-168 network clients. This sub-tab replaces the DVS168 sub-tab (above) when enabled. **Requires valid EAS NET and Encoder license keys**.
CAP Decode	Enables communication with Common Alerting Protocol (CAP) servers such as FEMA's IPAWS. **Requires a valid CAP Plus license key**.
DVS644 (SCTE18)	Offers communication with edge decoders and some of the latest digital set-top-boxes to send alert messages. This, in conjunction with Stream MPEG, provides a complete digital solution in one box for cable EAS requirements. **Requires a valid DVS644 (SCTE18) license key**.
Stream MPEG	An EAS device can uni-cast or multicast an MPEG2 video/ audio details page. **Requires a valid Stream MPEG 1/2 license key.**
Net CG	Communication with network-based character generators is configured via this interface.
Net Switch	Network-based control of external switching devices.
Net GPIO	External GPIO devices are configured and controlled through this interface.

Most of the Net Alert interfaces can be separately enabled / disabled per feature and per client interface. The standard Networked GPIO supports FIPS programmable LAN based relay triggering during alerts and alert states.

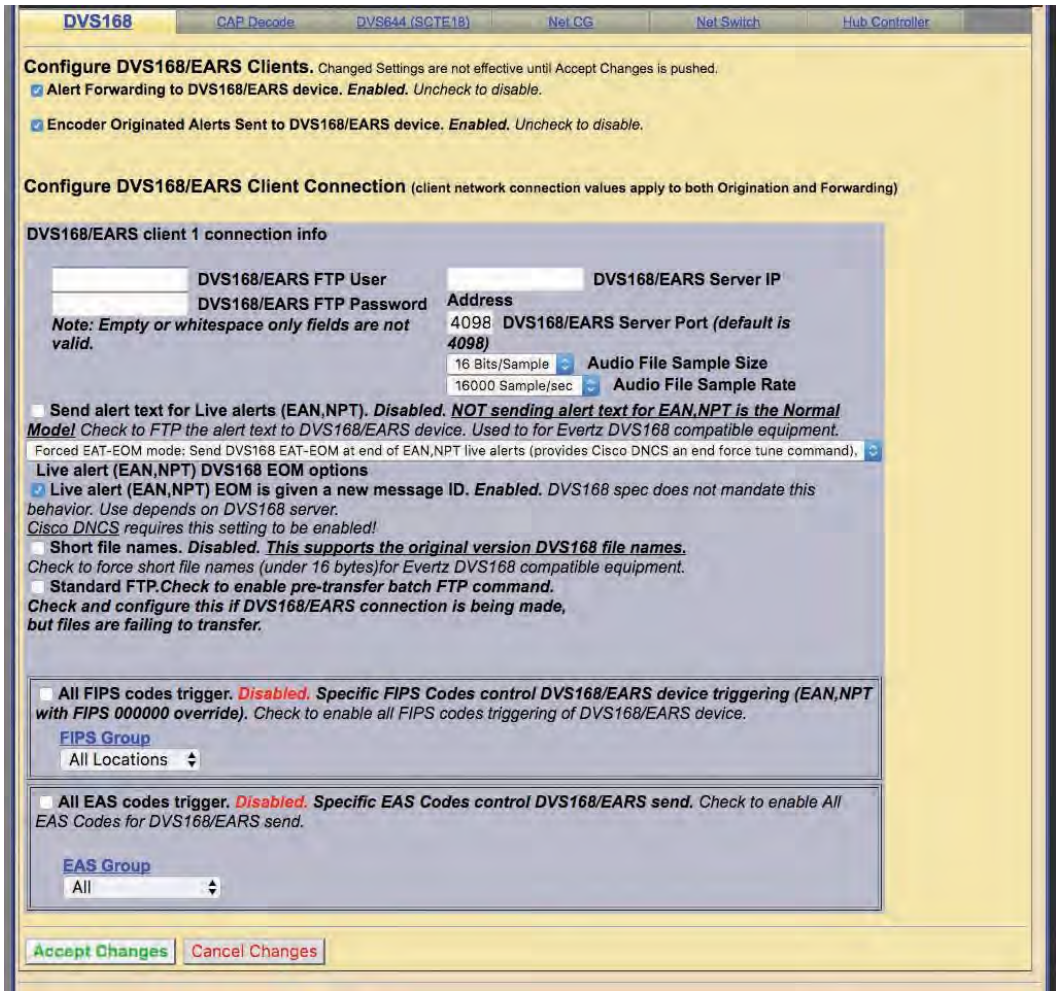
If a required network interface is not available, it can be enabled using the License Key Manager interface under **Setup > Server > Main/License**. (See the Server Setup - Main/License section of this chapter) License keys may be purchased from Digital Alert Systems.

All of the **Setup > Net Alerts** options require the use of the **Accept Changes** button for submitting changes.

MultiStation mode: When MultiStation mode is enabled, the Net Alert client interfaces used per station are selectable. A station can choose to NOT use an enabled Net Alert interface. The station assignment options do not allow reprogramming of a Net Alert interface – just its inclusion. Also, the specific included Net Alert interface MUST be enabled for the station to be able to trigger its action. This allows specific Net Alert interfaces to be assigned to different stations and thereby trigger a Net Alert action only when a specific station is active. Configure individual station Net Alert assignments within the desired station sub-tab screen under **Setup > Station**.

DVS 168

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



DVS168 Sub-tab

Alert Forwarding to DVS168/EARS device.
Placing a check in this box will allow received EAS alerts to be forwarded through the EAS device and sent out using the DVS-168 protocol. A gray **DVS168/EARS client 1 connection info** interface will be displayed when this options is checked.

Encoder Alert Send to DVS168/EARS device.
Placing a check in this box will allow originated alerts to be sent out using the DVS-168 protocol. If not already displayed, a gray **DVS168/EARS client 1 connection info** interface will be displayed when this option is checked.

Alert Forwarding and sending to DVS168/EARS Client
Once forwarding and/or sending have been enabled, four information fields must be configured to identify the DVS-168/EARS host. See above screenshot. Enter the IP address, the IP port, the FTP user and password, select Audio File Sample Size, and the Audio File Sample Rate (Default is 16000 Sample/sec). Alerts with all FIPS codes can be forwarded by placing a check mark in the box to enable all FIPS to trigger DVS168/EARS device. Alerts for specific FIPS areas can also be filtered/ passed through the protocol. Remove the check mark from the box that says

Note
For configurations requiring more than a single DVS-168 interface, an EAS NET license key is needed.

All FIPS codes trigger the DVS168/EARS device to enable FIPS forwarding control. When configured, select a FIPS codes group that will be used to check against the incoming forwarded alert. If any of these FIPS are included in the incoming forwarded alert, the alert will be sent to the DVS-168 client.

Remove the check mark from the box that says **All EAS codes trigger** the DVS168/ EARS device to enable EAS forwarding control. When configured, select an EAS code group that will be used to check against the incoming forwarded alert. If any of the EAS codes are included in the incoming forwarded alert, the alert will be sent to the DVS-168 client.

When an alert is forwarded to a DVS-168 client, a WAV file of the EAS audio and a text file of the alert details are constructed. These are FTP'd to the DVS-168 client. A socket is temporarily opened from the EAS device to the DVS-168 client, and a control message is sent that describes the alert. The Operation Log will log each of these actions and their success/ failure.

EAS NET

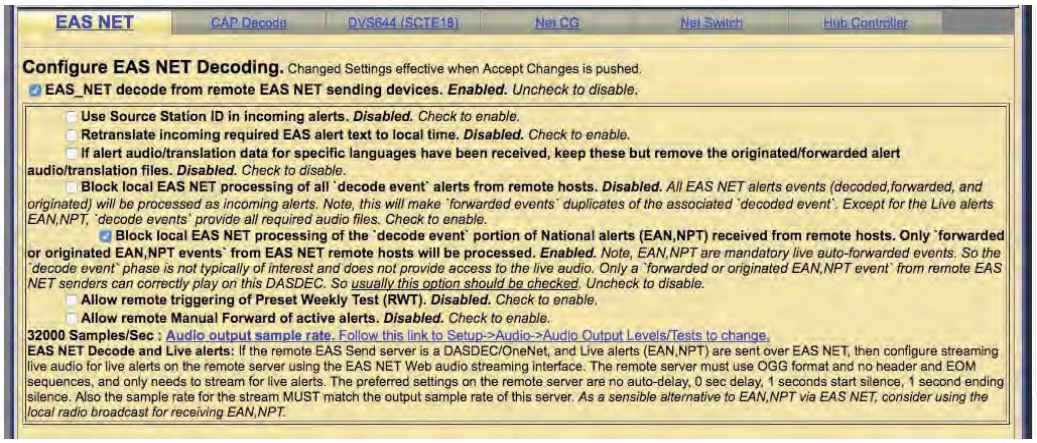
There are three sections on the EAS NET sub-tab: EAS NET Decoding, Web audio streaming, and EAS NET Clients.

Configure EAS NET Decoding

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

Basic Operation

EAS NET operates by sending optional audio, optional text translations, and an EAS event notification file from an EAS device to a remote device over LAN or WAN. There are some differences depending on the chosen EAS NET protocol. SSH STDIN Only does not offer sending of digital audio WAV files or text translations. DVS-168, a legacy protocol, does not send the same type of event notification data as the other protocols. For everything but DVS-168, the remote host/server device is sent as an event text file or ASCII data sequence that contains a set of key value style data lines describing the EAS alert. For every protocol but SSH STDIN Only and DVS-168, the text event file by default is copied into the remote host file EAS_ NET_ALERT under the remote user home directory. This filename and path can be overridden when configuring the client schema file. A standard set of information fields is sent in the text file, but the actual names of the keys can be custom edited per client according to a programmable schema. Each client can be set to use the Default or a custom edited schema. The EAS device EAS NET client interface provides a schema editor to create specialized schemas.

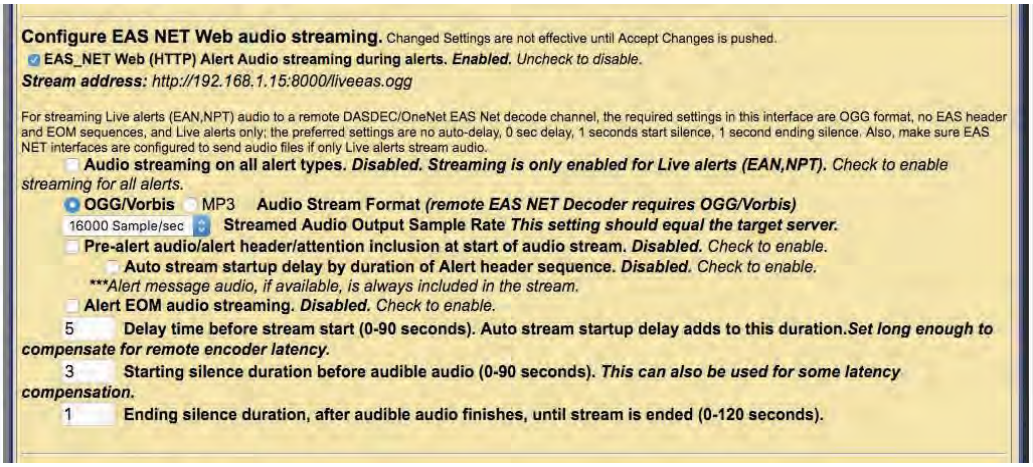


EAS NET Decoding Section

There is only one check box button to enable EAS NET decode. Check the check box labeled **EAS_NET decode from remote EAS NET sending devices**. The EAS device will then be able to receive alerts sent via EAS NET send from a properly configured remote EAS device. EAS NET decoded alerts are clearly labeled in the **Alert Events > Incoming/Decoded Alerts** screen as being received from input channel EAS NET. The alert event files are stored in a separate disk storage area from audio decoded alerts. Other than those differences, EAS NET decoded alerts are handled the same as alerts decoded from the audio inputs. Click the **Accept Changes** button to save changes.

Configure EAS NET Web audio streaming

EAS Net Client Web audio streaming is included with the EAS NET license. This provides a convenient way to stream live alert audio over a network. This is used primarily to provide live EAN/NPT audio from EAS NET sent to an EAS NET client device (including another EAS device). The stream is not an MPEG transport stream. It is an http audio stream. Remote clients must actively load the URL for the stream in order to play it. This can be done via most modern media players. An EAS device with EAS NET decode will automatically use this audio stream as a live input for EAS audio as needed. Refer to the screen shot below.



EAS NET Web Audio Streaming Section

EAS_NET Web (HTTP) Alert Audio streaming during alerts

Enable this check box to generate live web streamed audio during alerts. The default values of the options are designed to work for EAN/NPT.

Audio Streaming on all alert types

This check box controls audio streaming for National Alerts (EAN/NPT) or all alert types. For testing purposes, the check box **Audio streaming on all alert type** can be enabled to allow all alert types to have audio streaming. Make sure to use this button to test live audio for any remote EAS device EAS NET decoder.

Audio Stream Format

You can select either OGG/Vorbis or MPEG Layer 3 (MP3) audio. For audio to a remote EAS device EAS NET decoder, use OGG.

Audio Output Sample Rate
The correct value for this depends on the destination. For audio to a remote EAS device EAS NET decoder, use the output sample rate selected on the remote EAS device. Choices are 16000, 32000, 44100, and 48000 samples/sec.

Pre-Alert audio/alert header/attention inclusion at start of audio stream

Alert EOM Audio Streaming
These three check box options are included for control of the total content of the alert audio that is streamed. For purposes of this interface, alert audio consists of three parts:

- Pre-Alert audio/EAS Alert FSK header/Alert Attention signal
- Alert audio voice message
- Alert FSK EOM audio

No matter the choices, the second part, alert audio voice message, if it exists, is always streamed. Any combination of these options will work when streaming to a remote EAS device EAS NET decoder. The default is to not stream the header or EOM sequence, just the audio voice message. Use the options as required by the specific application on a remote server.

To review, the options allow the inclusion/exclusion of:

- Pre-Alert audio/EAS Alert FSK header/Alert Attention signal
- EAS alert FSK EOM

Delay time before stream start, Starting silence duration, Ending silence duration
These options allow streaming to be delayed by the duration of the alert header. Three numeric text fields allow entry of three additional audio delay components. Each delay is in seconds and applies to a specific location during the audio stream. Use as needed for the specific application.

Note
At least one of these check boxes must be enabled to allow editing of EAS_NET clients.

Configure EAS NET Clients

Two check boxes are displayed for enabling EAS_NET during alert forwarding and origination.

Forwarded Alerts can be sent to EAS_NET devices
This check box enables EAS_NET send processing during alert forwarding. It can be enabled / disabled at any time.

Encoder Originated Alerts can be sent to EAS_NET devices
This check box enables EAS_NET send processing during alert origination. It can be enabled / disabled at any time.

Decoded Alerts Can be sent to EAS_NET devices
This check box enables EAS_NET send processing during alert decoding. Decoded alerts can be sent to another EAS_NET device without forwarding and putting it on the air.

Configure EAS NET Client Connection Section

Configure EAS_NET Client Connection

Once enabled, you can create configurations for up to 8 EAS_NET clients. Each client can be independently enabled and disabled, allowing an easy way to stop or restart a client for a specific region.

If no client configurations exist, or if you want a new one and less than 8 clients exist, click the **Add EAS_NET Client Interface** button to create a new interface configuration.

To edit an existing client interface, select the named client from the **Select EAS_NET client** pull-down menu and edit the fields provided in the table underneath.

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

To duplicate an existing client interface *(a different name will be automatically generated; less than 8 clients must exist)*, select the **Duplicate EAS_NET Client Interface** button. This is the best way to create new client interfaces that are mostly the same as an existing one except for the IP address.

During alert processing, the Operation Log will log the success or failure of the EAS_NET forwarding/origination action per client.

EAS NET uses a flexible set of LAN communication protocols to send EAS data to a remote device. Generally, the remote device needs to have running software that understands EAS NET files and data formats in order for anything useful to be triggered by an EAS NET event. All EAS NET protocols will send an alert event data notification file or ASCII data string from the EAS device to the EAS NET remote server host. Most protocols allow for sending separate data files (like audio WAV files).

Caution
EAS_NET client configuration addition, duplication, and deletion is immediate and cannot be canceled.

Various information fields must be configured to identify and correctly communicate to the EAS NET remote client. Common to all are:

Client Interface Name
This text box allows the user to give the client interface a descriptive name. These names appear in the selection list.

Client Enable/Disable
This check box enables and disables the EAS NET client.

Event Data Protocol
Enables the user to configure the desired protocol for the EAS NET client. The available options are:

- **EAS NET** – Digital Alert Systems' exclusive communications protocol software enabling EAS data and audio transmissionover a TCP/IP network for up to eight (8) EAS-NET compatible platforms.
- **Common Alert Protocol (CAP)** – standard CAP v1.2 FEMA/IPAWS profile 1.0 text
- **PureCAP™ - Source CAP File** – forwards the original CAP message without modification for separate processing.
- **PureCAP™ Plus - Embedded Source CAP File** – this file wrapper contains only those languages appearing in the original CAP source. If the output languages are not present then EAS NET will not send.
- **Advanced Emergency Alerting Table (AEAT) Container** – protocol used in support of the Advanced Emergency Alerting (AEA) part of ATSC 3.0 - generating a proprietary XML file and sending it to various downstream devices.

New Feature
Support for PureCAP Plus is new in version 4.0.

New Feature
Support for Advanced Emergency Alerting (AEA) is new in version 4.0.

Remote Host Address
Displays the IP address of the remote EAS NET host where the EAS NET event info is sent.

EAS NET Event Transfer Protocol
Displays the event transfer protocol (the LAN communication method used to send the alert event data). Depending on the event transfer protocol, other configuration fields may be necessary or optional. Some protocols require passwords, others use encryption keys. Most provide for optional data file connections. The event transfer protocol options are:

- **Secure Copy (SCP)** – Uses the Secure Shell (SSH) network protocol for both the data file transfers and event file transfer. No passwords are needed for any of the Secure Shell protocols (**1.3**). Instead, the EAS device public ssh key id (under /root/.ssh/id_dsa.pub and also displayed at the bottom of the **System > Status > Network** screen) must be added into the remote host's authorized ssh keys list. The keys provide for encrypted data transfer and for secure authentication without a password.
- **Secure Shell STDIN Only (SSH)** – Uses the Secure Shell (SSH) network protocol for the event file transfer. No data files can be sent. This protocol requires that the receiving device read the EAS NET event file from standard input from within the shell script. In such a configuration, SCP and SSH login to the EAS NET user will not present to the remote platform shell.
- **Secure Shell STDIN & Copy (SSH with SCP)** – This is a variation on protocol #2 above. The event file is sent as in #2, but the Web interface will display a field to enter a second user account for sending data files to the remote host. The Secure Shell (SSH) network protocol is used for both transfers.

Note
The **EAS_NET Event Transfer Protocol** pull-down menu selection will dictate the available configuration settings within this screen. The following configuration setting descriptions represent the most commonly used. Not all settings will be available for the selected EAS_NET Event Transfer Protocol. See **Other possible EAS NET Client Configurations Options** (below).

- **FTP Copy** – Uses the File Transfer Protocol (FTP) network protocol for both the data file transfers and event file transfer. A password is required. FTP does not encrypt or secure passwords during transmission. The password is sent in clear text to the remote host FTP daemon. If security is an issue, do not use or design an FTP based EAS NET scheme. Some FTP daemons refuse passive port connections. Use the provided check box to enable a non-passive connection if needed.
- **TCP Event Notification** – Uses a TCP socket from the EAS device to the remote host to send the alert event file. For sending the optional data files, one of FTP or SSH SCP network protocols can be selected. A valid user account on the remote host must be entered. The information described above for passwords and keys apply, depending upon the chosen data protocol.
- **DVS168/EARS** – This is a special case of EAS NET. A TCP socket is used to communicate an event notification, while FTP is used to send data files.
- **Legacy Mediaroom** – This is a special protocol bundled under EAS NET when the Microsoft© Mediaroom™ option is licensed.
- **Mediaroom2** – This is a special protocol bundled under EAS NET when the Microsoft© Mediaroom™ option is licensed. This is in accordance with the Mediaroom 2.0 software.
- **MINERVA** – This is a special protocol bundled under EAS NET when the Minerva option is licensed. A TCP socket is used to communicate an EAS event notification as per the Minerva protocol.
- **WideOrbit** – This is a special protocol bundled under EAS NET when the EAS NET Automation option is licensed.
- **RCS Nexgen** – This is a special protocol bundled under EAS NET when the EAS NET Automation option is licensed.

Event Data IP control options (or Event/Ancillary Data IP control options)

Remote EAS NET Host IP Address
Enter the host name or IP address of the remote host computer

EAS_NET Event Transfer Protocol

- Secure Copy
- Secure Shell STDIN Only
- Secure Shell STDIN & Copy
- FTP Copy
- TCP Event Notification
- DVS168/EARS
- Legacy Mediaroom
- Mediaroom2
- MINERVA
- WideOrbit
- RCS Nexgen

Remote EAS NET Host Port
The field displays the port on the remote EAS NET host where the EAS NET event info is sent.

FTP Ancillary Data File control options

EAS NET User
Displays the user account name on the remote device. Files sent to the remote host will by default be copied relative to this account home directory.

Current Schema

The schema determines key names of the information fields sent to the EAS NET client's remote host. It also determines file names and paths for any files sent to the remote host. The schema can be edited by clicking on the **Edit/Review Schema** button.

Note
The schema does not set the values of the client interface fields.

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.

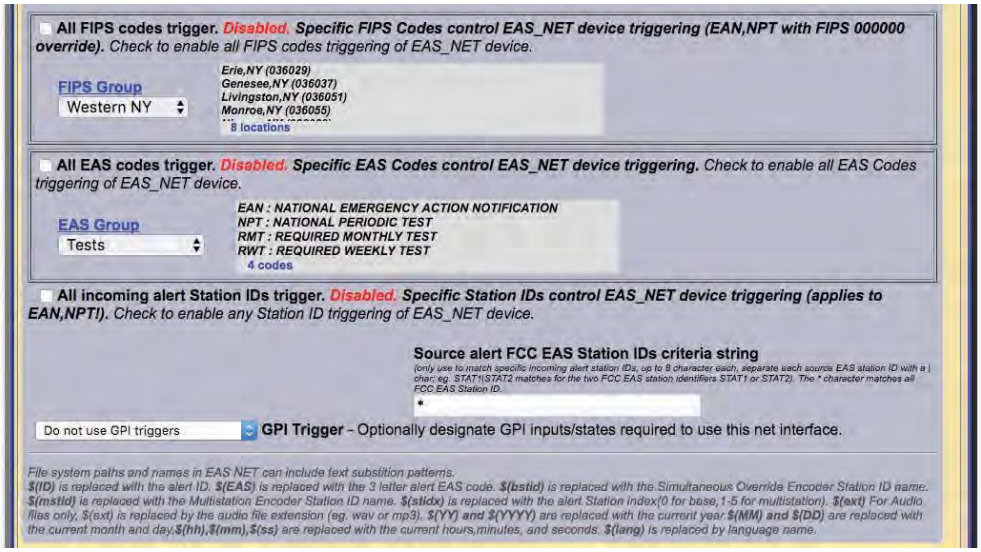
EAS Audio File send
When enabled (checked) the individual audio sections of the EAS alert will be sent as separate files to the EAS NET client's remote host. File names/path on the remote host are determined by the schema.

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 / EAS Codes Trigger Section

All FIPS codes trigger

If enabled, all alert FIPS codes will trigger the EAS NET client interface. In the above screen shot this option is disabled. Set the check box to enable/disable FIPS code filtered trigger control. If disabled, the alert FIPS codes are filtered for at least one specific match as a way to control whether or not EAS NET is triggered. Alerts for specific FIPS areas can be filtered as a way to control whether or not EAS NET is triggered. If All FIPS is disabled, select a FIPS codes group from the **FIPS Group** pull-down menu. That group of FIPS codes are included in the incoming active forwarded/originated alert and the alert will be sent using the EAS NET client. With careful use of this feature, and with multiple clients, one EAS device can serve many different regions at the same time.

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

DVS168/EARS devices

DVS168/EARS can be selected as an option on the EAS NET Event Transfer Protocol selector. See the screen shot below. Like the other EAS NET protocols, the EAS NET remote host IP address and port must be entered. This would be the address and port of the DVS168/EARS server. Standard DVS168 uses FTP to send data files, so an EAS NET FTP user and password value must also be entered for a standard client configuration. However, there is an option to disable the FTP send. This is for servers that do not support handling digital file data but can be alerted by the DVS168 event protocol. If this option is checked the FTP user and password values are not displayed or needed since the audio and video files will not be sent.

Note
Since EAS NET is used in conjunction with third-party management software (on the remote host), configuration details will depend upon the exact third-party solution. Often instructions will be provided by this party. Configure the EAS NET client interface as required.

Configure EAS NET DVS168/EARS Client Section

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

1. To send just the EAS alert audio message, instead of the EAS FSK header and EOM audio and attention audio, use the provided check box. Before using this option, it is important to make sure your local EAS plan allows the FSK audio to be discarded.
2. Alert duration data format: typically in minutes, some DVS-168 interpreters have coded this differently. The selector provides two other interpretations.

The DVS168 protocol does not provide a programmable schema. For DVS168, the data schema is predefined and the schema selection is not displayed. As with the other EAS NET protocols, the Video Start Delay time, the Duration Extension time, and FIPS based net alert triggering are all configurable.

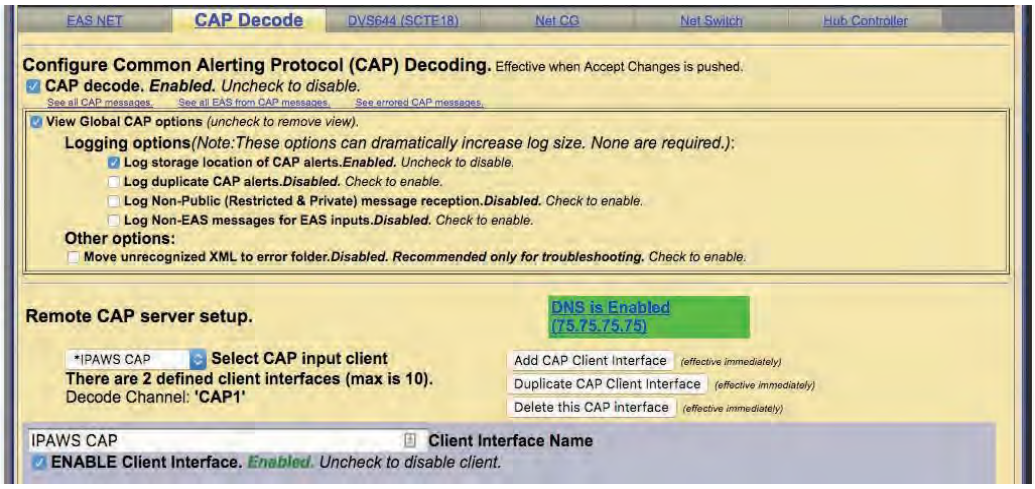
When you finish making changes, click **Accept Changes** to save the configuration.

DVS168/EARS Operation

When a forwarded/originated EAS alert is to be sent using a DVS-168 EAS NET client, a TCP socket is temporarily opened from the EAS device to the DVS-168 remote host. If this succeeds, and the alert is a non-national alert (and FTP is enabled), a WAV file of the EAS audio and a text file of the alert details are FTP'd to the DVS-168 remote server host. Then a control message is sent over the TCP socket that describes the alert and provides names for the data files. For non-national alerts, this is the only notification by TCP needed. For EAN and NPT national alerts, the audio is not generated or sent, since EAN/NPT alert audio is live and of undetermined duration. When the alert ends, a second control message is sent over the TCP socket to signal the end of the national alert. After this, the socket connection is "torn-down." The Operation Log will log each of these actions and their success or failure.

CAP Decode

There are two sections to configure in the CAP Decode sub-page: **Configure Common Alerting Protocol (CAP) Decoding** and **Remote CAP Server Setup**.



CAP Decode Sub-Tab

Configure Common Alerting Protocol (CAP) Decoding

CAP Decode

This check box enables or disables CAP decoding for the EAS device. Set it to enable to see all of the available options for CAP Decoding.

View Global CAP Options

This section of the web interface deals with logging and XML file handling.

Log storage location of CAP alerts

Will log the storage location of incoming CAP alerts.

Log duplicate CAP alerts

Duplicate CAP alerts will be logged separately.

Log Non-Public (Restricted & Private) message reception

Enables the logging of non-public CAP alerts

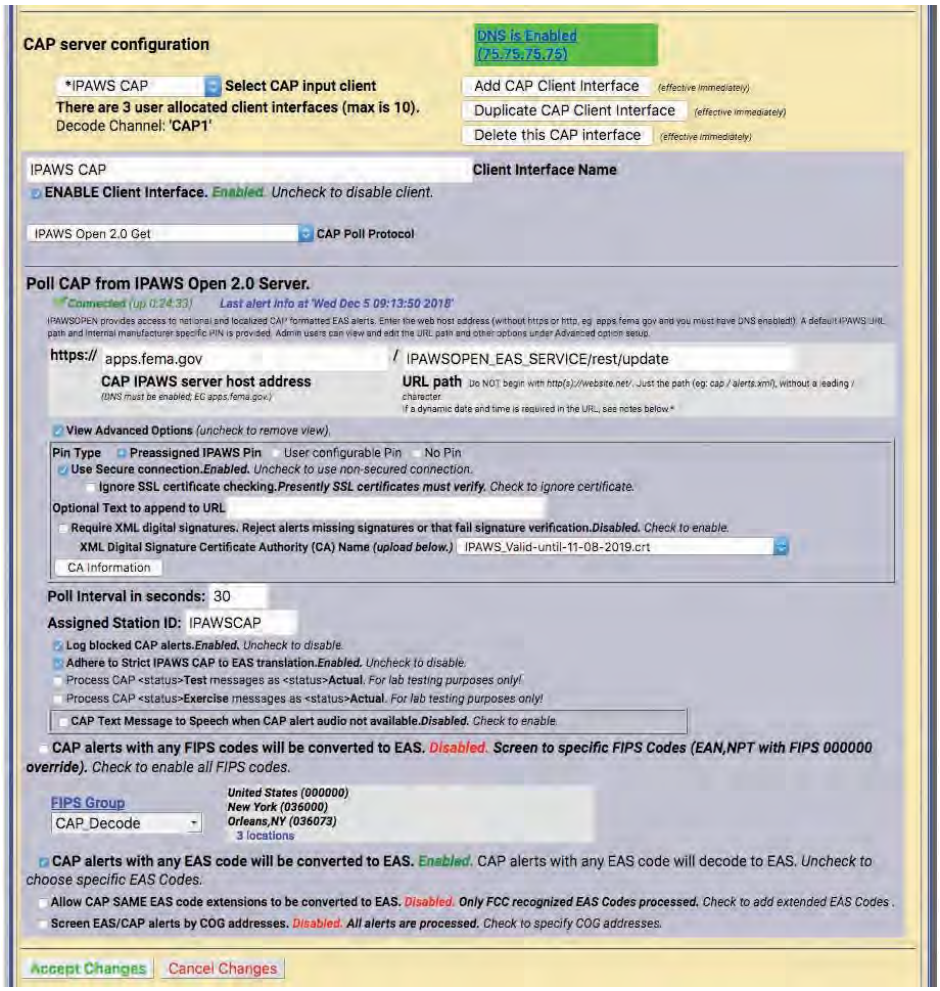
Log Non-EAS messages for EAS inputs

Non EAS messages will be logged

Move unrecognized XML to error folder

When an unrecognized XML file is detected, it is placed in the error folder. This option is recommended for trouble shooting purposes.

Note
To quick connect to the FEMA CAP Server and the Canadian NAAD system, see instructions located at the end of this section.



Remote CAP Server Setup Section

Remote CAP Server Setup

Select CAP Input Client

This pull-down menu allows you to choose which CAP client you are configuring. The default clients are: CAP PUSH INPUT and HTTP Get Client1.

The CAP PUSH INPUT is available if you want to Receive CAP Alerts from a remote push server. Note: this option is not used often as FEMA would have to know all of the specific IP addresses that it was pushing CAP Alerts to. Because FEMA does not know your EAS devices' IP Address location, it is not going to push an alert to you this way. **It is recommended that this client interface is disabled.**

For the HTTP Get Client1 default option, you can choose between a few CAP Polling Protocols. Choose between HTTP, HTTPS, SSH and the IPAWS Open 2.0 option.

Add, Duplicate and Delete this CAP Interface

These buttons add a new CAP Client Interface - duplicate the one that is currently being edited, or delete the one that is currently being edited.

Client Interface Name

Choose a name for the specific Client Interface that you will configure.

ENABLE Client Interface

Check this box in order to enable the configured or new client to become active to EAS NET CAP Alerts.

CAP Poll Protocol

Choose between HTTP, HTTPS, SSH and the IPAWS Open 2.0 option.

- **WWW HTTP Get (Web URL) -** Use this option to poll from a WWW Server (CAP XML, EDXL-DE, NOAA Atom, RSS pages).
- **WWW Secure HTTPS Get -** Use this option to poll a WWW HTTPS Secured Server (CAP XML, EDXL-DE, Atom, RSS)
- **Secure Shell Get -** Use this option to poll a SSH Server (CAP XML, EDXL-DE, Atom, RSS)
- **IPAWS Open 2.0 Get -** IPAWSOPEN provides access to national and localized CAP formatted EAS alerts. Enter the web host address (without https or http; e.g. apps.fema.gov and you must have DNS enabled to connect). A default IPAWS URL path and internal manufacturer specific PIN is provided. Admin users can view and edit the URL path and other options under the advanced option setup.

Under each of those polling options are very similar credentials that need to be filled out in order to connect to the servers. The following list will show most of those options.

CAP Server Connection Status
The green and red text just below the **Poll CAP from IPAWS Open 2.0 Server** text displays the current status of the CAP server connection (Connected or Not Connected) along with the amount of up or down time. While in the Connected state, the interface will display the time and date of the last received alert.

CAP Server Host Address
This is the address of the server that you want to receive CAP Alerts from. In order to use a URL, a DNS connection must be enabled. Go to Server Network Configuration section at **Setup > Network** to change your DNS options or use the hyperlink.

URL path portion and/or remote path and file name
Put the URL path of the server that you want to receive CAP Alerts from.

Poll Interval in Seconds
This is the number of seconds the EAS device will take before it checks for another CAP Alert.

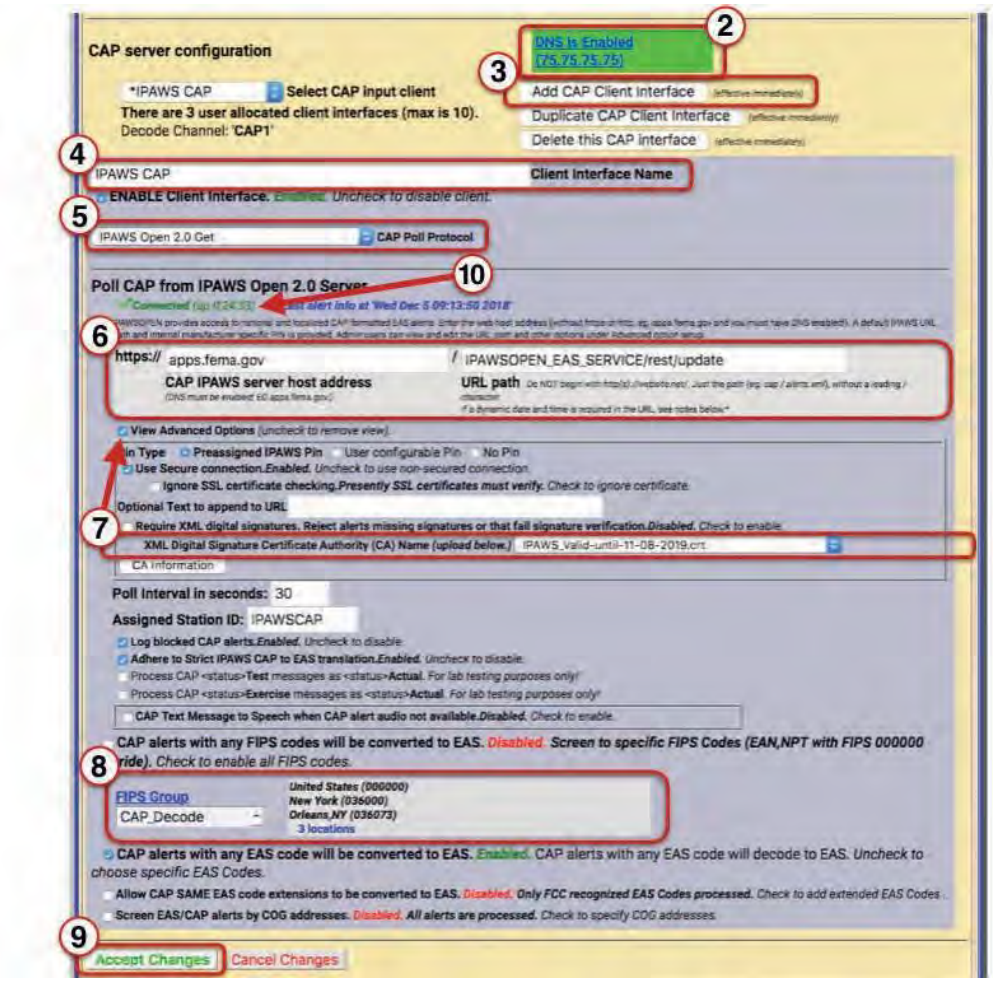
Assigned Station ID
Use this value to give the server that you are receiving CAP Alerts from an ID that will appear on the log of Decoded alerts.

CAP alerts with any FIPS codes will be converted to EAS
This option, when enabled, will convert CAP Alerts that are sent to any FIPS location to EAS on the EAS device. It is recommended this option be **DISABLED** as you won't need to know all of the cap alerts that are going on around the country. When this option is disabled, enter the desired FIPS Group. The FCC requires reception of CAP Alerts for your county, and your entire state - not every specific county in the state, but the option that gives you the entire state FIPS code.

Quick Connect to IPAWS CAP Server

To quick connect to the FEMA CAP Server, create a new client and follow the options in the screen shot below.

1. Navigate to the **Setup > Net Alerts > CAP Decode** screen
2. Ensure DNS is enabled (**Setup > Network**)
3. Click the **Add CAP Client Interface** button (just below the *DNS is Enabled* text)
4. Enter a descriptive name in the **Client Interface Name** field (i.e. IPAWS)
5. Select **IPAWS Open 2.0 Get** from the **CAP Poll Protocol** pull-down menu
6. Within the **Poll CAP from IPAWS Open 2.0 Server** section:
   a. Enter **apps.fema.gov** in the **CAP IPAWS server host address** text field
   b. Enter **IPAWSOPEN_EAS_SERVICE/rest/update** in the URL path text field
7. Click the **View Advanced Options** check box
   a. Select **IPAWS_Valid-unitl-11-08-2019.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu
8. Select the desired FIPS Group
   (This FIPS Group should include the United States code [000000], your state's code, and any county codes for your service area.)
9. Click the **Accept Changes** button
10. Check to see the EAS device is connected. Green text under the **Poll CAP from IPAWS Open 2.0 Server** section header should read **√ Connected**.



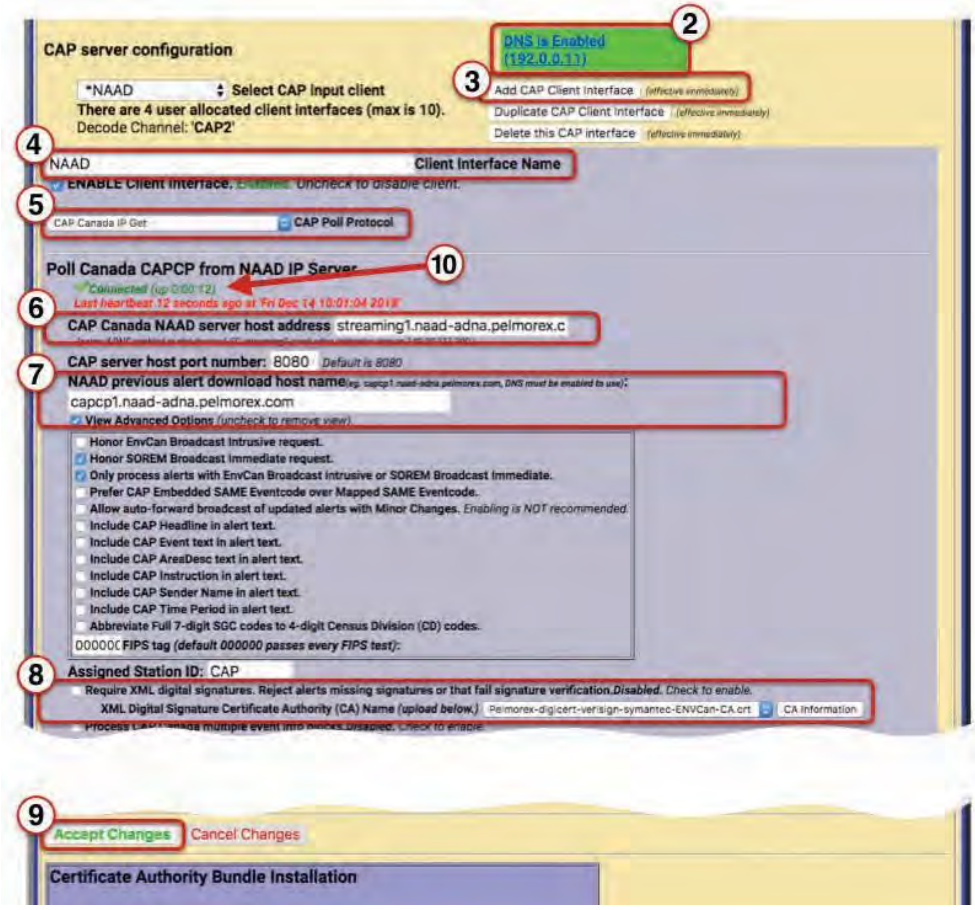
IPAWS CAP Server Interface Screen

New Feature
FEMA has updated their XML Digital Signature Certicate Authority (CA) Name. The new CA has been added to version 4.0.

Quick Connect to NAAD CAP Server (CAP Canada)

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

1. Navigate to the **Setup > Net Alerts > CAP Decode** screen
2. Ensure DNS is enabled (**Setup > Network**)
3. Click the **Add CAP Client Interface** button (just below the *DNS is Enabled* text)
4. Enter a descriptive name in the **Client Interface Name** field (i.e. NAAD)
5. Select **CAP Canada IP Get** from the **CAP Poll Protocol** pull-down menu
6. Enter **streaming1.naad-adna.pelmorex.com** in the **CAP Canada NAAD server host address** text field
7. Enter **capcp1.naad-adna.pelmorex.com** in the **NAAD previous alert download host name** text field
8. Select **Pelmorex-digicert-verisign-symantic-ENVCan-CA.crt** option within the **XML Digital Signature Certificate Authority (CA) Name** pull-down menu
9. Click the **Accept Changes** button
10. Check to see the EAS device is connected. Green text under the **Poll Canada CAPCP from NAAD IP Server** section header should read **√ Connected**.



CAP Canada / NAAD Server Interface Screen

New Feature
Canadian authorities have updated their XML Digital Signature Certicate Authority (CA) Name. The new CA has been added to version 4.0.

Attention
Enabling the **Honor EnvCan Broadcast Intrusive requests** setting should only be exercised in coordination with Environment Canada. Do not check/enable this feature prior to consulting with EnvCan.

Attention
The **Honor SOREM Broadcast Immediate requests** setting should be checked/enabled in compliance with Canadian CLF guidance.

Attention
Check/enable the **Only process alerts with EnvCan Broadcast Intrusive or SOREM Broadcast Immediate** if it is intended to ONLY transmit messages designated as Broadcast Immediate by alerting authorities.

DVS644 (SCTE18)

Configure DVS644 (SCTE-18) Clients

DVS644/SCTE18 is a SCTE standard for encapsulating EAS alert data into an MPEG transport stream format (as an MPEG system table) for delivery to MPEG client devices (such as set-top boxes and cable ready TVs). The EAS device has a sophisticated and powerful implementation of this standard.

This feature requires the DVS644/SCTE18 license. WhenDVS644/SCTE18 support is available on the EAS device, the sub-tab for this feature appears under **Setup > Net Alerts**. Two check boxes are displayed for enabling DVS644/SCTE18 during alert forwarding and origination.

Alert Forwarding to DVS644/SCTE18/CEAM devices
Enabling this check box allows SCTE18 send processing during alert forwarding.

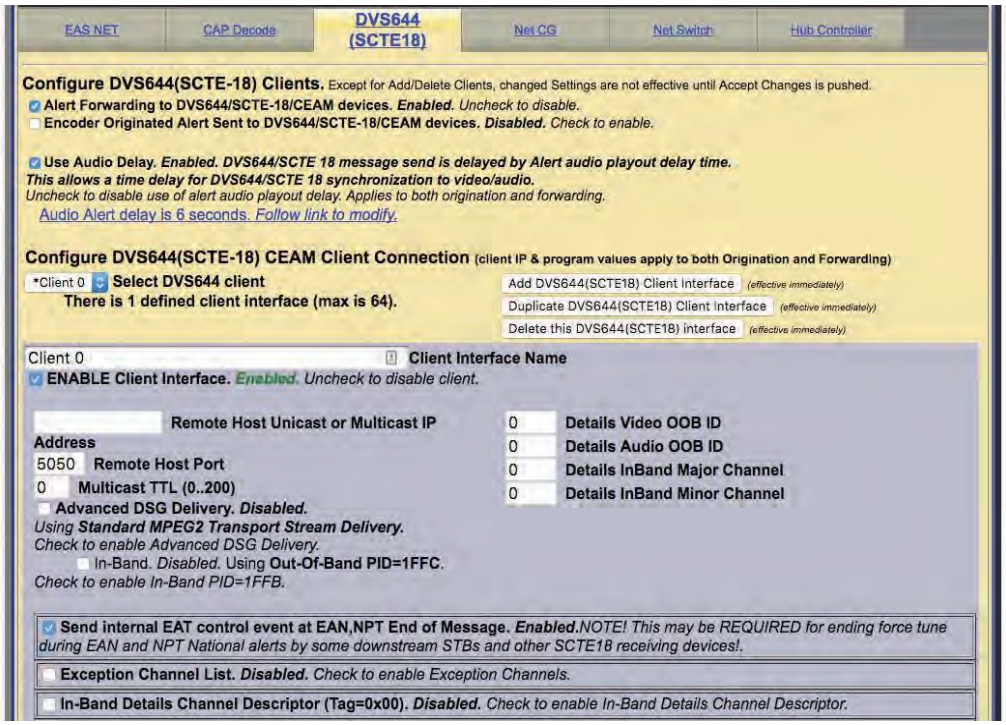
Encoder Originated Alerts Sent to DVS644/SCTE18/CEAM devices
Enabling this check box allows SCTE18 send processing during alert origination.

At least one of these check boxes must be enabled to allow editing of DVS-644/SCTE18 clients. In the screen shot below, the Alert Forwarding is enabled.

If either of the first two check boxes are enabled, the **Configure DVS644(SCTE-18) CEAM Client Connection** interface appears allowing the user to add and configure a DVS644(SCTE18) client.

Add DVS644(SCTE-18) CEAM Client Connection
Clicking this button will enable the user to create, configure, and manage a single of multiple DVS644(SCTE18) client(s).

Use Audio Delay
This check box will also appear allowing the audio to be delayed so as to synchronize the audio and video content. The Audio Delay setting is found in **Setup > Audio > Decoder Audio** at the bottom of the screen – Alert audio delay.



DVS644/SCTE18 Sub-Tab

Configure DVS644 (SCTE-18) CEAM Client Connection

Up to 64 DVS644/SCTE18 client interfaces may be defined. Each one can have a unique configuration and can send the SCTE-18 EAS protocol data to different IP addresses. During alert play-out processing, the Operation Log will log the success or failure of the DVS644/SCTE18 forwarding/origination action per client. Individual client interfaces may also be enabled and disabled. Every enabled client configuration is triggered for whichever action of alert forwarding and alert origination is currently enabled.

Select DVS644 client
This pull-down menu contains the names of the existing client interfaces. It also prints the current number of defined client interfaces. The maximum number of client interfaces is 64. Choose the named existing client interface to edit.

Add / Duplicate / Delete DVS644 (SCTE18) Client Interface Buttons
Users can create configurations for up to 64 DVS644 (SCTE-18) CEAM (Cable Emergency Alert Message) clients.

If no client configurations exist or a new configuration is needed, click the **Add DVS644(SCTE18) Client Interface** button to create a new interface configuration.

To delete a client configuration, select the desired client from the Select DVS644 client pull-down menu and click **Delete this DVS644(SCTE18) interface button**.

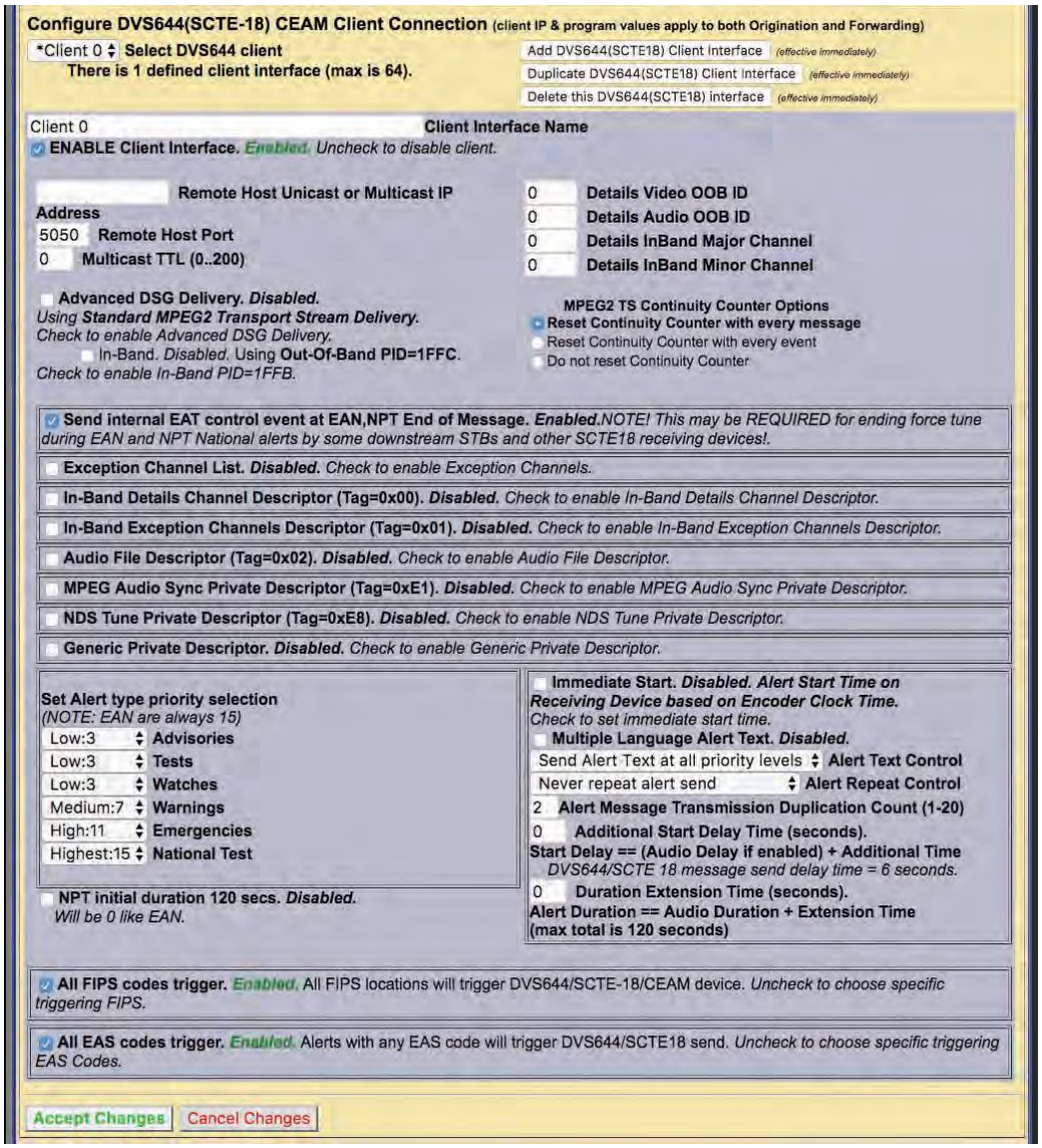
To duplicate an existing client interface, select the **Duplicate DVS644(SCTE18 Client Interface** button. A different name will be automatically generated. This is the ideal way to create many client interfaces that are mostly the same except for the IP address.

Caution
DVS644/SCTE18 client configuration addition, duplication, and deletion are immediate and cannot be canceled.

Client Interface Configuration Table

Client Interface Name
Use the **Client Interface Name** text entry field to name each client.

ENABLE Client Interface
Use this check box to enable/disable a client interface at any time. Each client can be independently enabled and disabled allowing an easy way to stop/ restart using a client for a specific region.



DVS-644/SCTE18 Client Configuration Interface Section

Various information fields must be configured to identify and correctly communicate to the DVS-644/SCTE18 client. The basic fields are the **Remote Host Unicast or Multicast** and **Remote Host Port.** Enter these addresses according to the specific DVS-644/SCTE-18 target server. Often this is an MPEG-2 multiplexor, such as a Stream Encryptor Modulator, serving a defined set of digital cable channels.

Multicast TTL

This value determines the number of router hops that are allowed during multicast of the DVS644/SCTE18 Cable Alert Message before the UDP message is blocked. Enter a sufficiently large value (from 0 to 200) if you are multicasting. Multicasting requires the proper configuration of a network outside the EAS device.

Advanced DSG Delivery

Defaults to Disabled. The default method for delivering the DVS644/SCTE18 Cable Alert Message MPEG2 system table uses a standard MPEG2 Transport Stream. Check to switch to Advanced DSG delivery. Use DSG delivery for communicating with DOCSIS Standard Gateway equipment.

If **Advanced DSG delivery** is used then the text field option for setting the **Network MTU** (Max transmission unit) is available. The default is 1500 but can be set lower if needed based on a specific network.

If **standard MPEG2 transport stream delivery** is used, then the following option is available:

In-Band
Check to Enable. If not checked (disabled) then **Out-of-Band (OOB)** communication of the DVS-644/SCTE18 message is made.

The DVS-644/SCTE18 Cable Alert Message is an MPEG2 system table structure, typically placed into the MPEG2 Transport stream and routed to the downstream cable set top boxes (STB) or SCTE-18 enabled TV's. The ultimate target for the DVS-644/SCTE18 alert message is a set-top box (STB) or a cable ready TV. The actual EAS alert handling is performed by the STB or TV, and although standard practices exist for these actions, differences do exist. The processing of the Cable Alert Message on the STB determines the actual response to the alert seen by a viewer. For alerts below a certain priority (by default, this would be the highest priority, 15), a crawl message is typically run on the video display for every channel.For alerts at or above this priority, the video channel is forced to a details channel. Based upon whether this channel is available at the STB as In-Band or Out-of-Band, set the **Details Major/Minor number** or the **Details Video/Audio OOB** channel numbers. This details channel is where the highest priority force tune alerts are switched. EAN/NPT will always cause a force tune to this channel.

Details Video OOB ID/ Details Audio OOB ID
When the alert details channel is an Out-of-Band channel, set the provided video/ audio channel field. An audio channel designation is not required when there is another means to provide the alert audio. A value of 0 means not used.

Details In-Band Major / Minor Channel
These two fields are for programming the digital in-band Major/Minor channel number of the in-band force tune details channel. A value of 0 means not used.

MPEG2 TS Continuity
Each MPEG-2 Transport Stream packet contains an incriminating Continuity Counter (CC) number (ranging from 0-15). This value is used to determine if any packets are lost, repeated, or out of sequence. Manufacturers of downstream MPEG devices may deal with the CC value in dissimilar ways. For this reason there are three separate settings.

Reset Continuity Counter with every message (default setting)
When you send an MPEG-2 / SCTE-18 alert event, the CC will start with a value of zero (0) and increment appropriately. If the alert is repeated (via the **Alert Repeat Control**), the CC will be forced to a value of zero (0) at the beginning of each message.

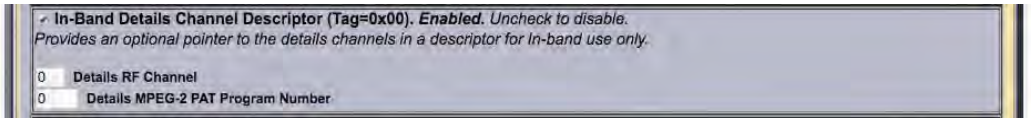
Reset Continuity Counter with every event
Each MPEG-2 / SCTE-18 alert event will begin with the CC set to zero (0) and will increment appropriately. The CC will not be forced to zero (0) until a new alert event is generated.

Do no reset Continuity Counter
The CC will always increment appropriately and will not be forced to a value of zero (0).

Exception Channel List Section

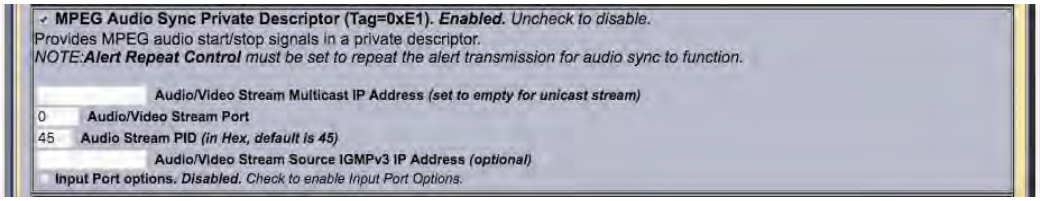
Send internal EAT control event at EAN,NPT End of Message
Enabling this check box will send and Emergency Action Termination (EAT) at the end of both an EAN or NPT to indicate the emergency action is over.

Exception Channel List
This interface allows specific In-Band and Out-of-Band channels to be excluded from the alert response of the STB. These channels have their own EAS. When enabled, the interface allows the creation of any number of exception channels.



In-Band Details Channel Descriptor 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 Section

MPEG Audio Sync Private Descriptor
Check to enable the MPEG Audio Sync Private Descriptor - a special private descriptor for synching a EAS device MPEG2 A/V stream to the DVS644/SCTE18 message processor. Use of this method requires custom support by the DVS644/ SCTE18 message processor.

NDS Tune Private Descriptor
Check to enable the NDS Tune Private Descriptor method - a special private descriptor for synching a EAS device to an NDS system. Use of this method requires custom support by the DVS644/SCTE18 message processor.

Generic Private Descriptor
Check to enable an interface to create one static DVS644/SCTE18 Private Descriptor. Use of this method requires custom support by the DVS644/SCTE18 message processor.

Set Alert Type Priority / FIPS & EAS Code Triggers Section

Alert Type Priority Selection
Use this interface to configure the associated priority number for EAS alert codes. The scheme is based upon five EAS groups: Advisories, Tests, Watches, Warnings, and Emergencies. The exact alerts that fall into each category are defined on the EAS device at **System > Help > EAS Codes**.

DVS644/SCTE18 provides for 16 priority values (0-15). However, reserved uses for most values means that in practice, priority values are 0, 3, 7, 11 and 15, with 15 being the highest priority alerts. The priority of 0 has a special meaning. An alert sent with 0 priority will establish a new set-top box or TV sequence number. The sequence number is incriminated (modulo 32) whenever an alert is sent with updated information. The EAS device supports this reset mode by allowing an alert to be set to 0 priority. This setting should only be used for one alert and then changed to 1-15. There is also a field to extend the alert duration past the default EAS device audio duration. Keep in mind that the maximum allowed time for a DVS644/SCTE18 message is 120 seconds.

NPT initial duration 120 secs
When unchecked, the NPT initial duration is 0 – which means this live alert is open-ended. Once the EOM is reached a second message with a 5 second duration is sent which ends the NPT alert. By selecting this check box, a fixed duration of 2 minutes is forwarded within the NPT.

Immediate Start (Alert Start Time)
This check box sets the EAS Alert message start time on the receiving device. When enabled, the start time of the alert on the receiving device is immediate upon reception. When disabled (unchecked), the Alert Start Time is set to use a clock-based start time. The actual time used is the EAS alert UTC.

Caution
If a clock time is used, it is CRITICAL that the EAS device and the receiving device be time synchronized.

Multiple Language Alert Text
Allows SCTE-18 to send multiple language translations to the SCTE-18 connected device.

Alert Text Control
This pull-down menu programs when the alert text section of the DVS-644/SCTE18 message is sent, based on alert priority. It allows text to not be sent if the priority becomes higher than a specified value and allows the STB to omit alert text crawls when a force tune to a details channel is made based upon alert priority.

Alert Repeat Control and Alert Message Repeat Period
The EAS device can be configured to periodically resend the alert message, with the DVS644/SCTE18 Cable Alert message field **alert_time_remaining** field decremented automatically. This is controlled using the **Alert Repeat Control** selections. The options are based on alert priority, allowing repetition to be invoked for alerts above a given priority. When repetition is selected, the **Alert Message Repeat Period** field for entering the time period (in seconds from 6 to 60) is also displayed.

Alert Message Transmission Duplication Count (1-20)
When a forwarded/originated alert is sent to a DVS-644 client at a specific IP address, the DVS-644/SCTE-18 MPEG-2 system table is generated and sent to the MPEG multiplexor client. Programming this interface controls the number of times the table is sent as a duplicate, from 1 - 20 times, to insure downstream reception.

Additional Start Delay Time (seconds)
This check box allows time to be added before the DVS644/SCTE18 Cable Alert Message is first sent over the network. The formula for the delay time is: Start Delay == (Audio Delay if enabled) + Additional Time.

Duration Extension Time (seconds)
This field allows extra time to be added to the alert duration programmed into the Cable Alert Message **alert_time_remaining** field. The maximum time allowed for this field is 120 seconds. This can be used to guarantee a minimum amount of time for short Weekly Test alerts. The formula for the Alert Duration is: *Alert Duration == Audio Duration + Extension Time (max total is 120 seconds)*.

All FIPS codes trigger
If enabled, all alert FIPS codes will trigger the DVS644/SCTE18 client interface. In the above screen shot this option is disabled. Set the check box to enable/disable FIPS code filtered trigger control. If disabled, the alert FIPS codes are filtered for at least one specific match as a way to control whether or not DVS644/SCTE18 is triggered. Alerts for specific FIPS areas can be filtered as a way to control whether or not DVS644/SCTE18 is triggered. If All FIPS is disabled, select FIPS Groups from the pull-down menu. If any of these FIPS codes are included in the incoming active forwarded/originated alert, the alert will be sent using the DVS-644/SCTE18 client. With careful use of this feature, and with multiple clients, one EAS device can serve many different cable regions at the same time.

All EAS codes trigger
If enabled, all EAS codes will trigger the DVS644/SCTE18 client interface. In the above screen shot this option is disabled. Set the check box to enable/disable EAS code filtered trigger control. If disabled, then the alert EAS code is filtered for a specific match as a way to control whether or not DVS644/SCTE18 is triggered. If All EAS is disabled, select EAS Group from the pull-down menu. If the EAS codes of an active forwarded/originated alert matches any included in the EAS Group, the alert will be sent using the DVS-644/SCTE18 client. With careful use of this feature, and

with multiple clients, one EAS device can serve many different cable regions at the same time.

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

Stream MPEG

If Streaming MPEG hardware/software is available on the EAS device, a sub-tab will display under **Setup > Net Alerts** that allows configuration of up to two client targets. As in the other Net Alert pages, use the Alert Forwarding and/or the Encoder Alert stream check boxes to enable/disable the use of streaming MPEG clients when alerts are forwarded and/or originated.

Stream MPEG Sub-Tab

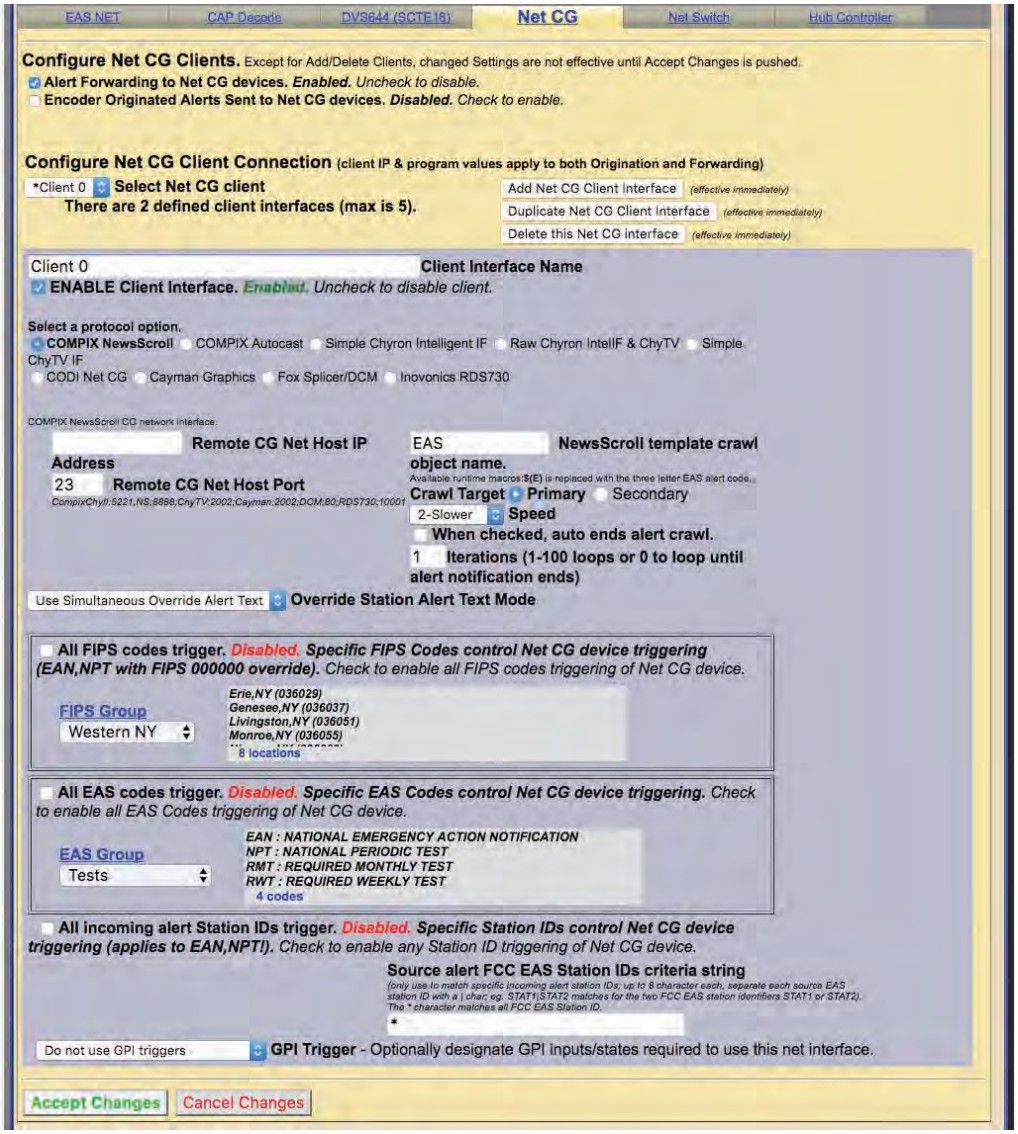
Addition/deletion, configuration, and enable/disable for each client interface is handled like other Net Alert interfaces described above. Unlike those interfaces, there are a few global settings that affect all streaming clients. These control the video/audio format and encoding bitrate of the stream (from the hardware). The user can also program Audio/Video, Audio only, or Video only being encoded. To account for the latency of starting up stream encoding and actually streaming, a delay of a few seconds is needed before audio is played for a net forwarded/originated alert. Audio delay status and a link to the configuration field for audio delay is provided.

Streaming MPEG requires very few configuration fields. A unicast or multicast IP address must be set, along with a port. The Multicast TTL value must be set high

enough to insure the multicast data is sent past all the LAN routers between the EAS device and the destinations. Also, as with the EAS NET and DVS-644 interfaces, FIPS and EAS code-based triggering is supported per client.

Net CG

This page allows configuration of up to five client targets for running alert crawls. The Net CG units must support Ethernet and be connected to the same LAN as the EAS device. As in the other Net Alert pages, use the Alert Forwarding and/or the Encoder Originated Alert check boxes to enable/disable the use of Net CG clients when alerts are forwarded and/or originated.



Net CG Sub-Tab

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

The first option: **Client Interface Name** allows the user to name the CG to reduce confusion between multiple devices.

ENABLE Client Interface

Check this box in order to enable the specific client you have created or selected to edit.

Select a Protocol Option
Select the CG that pertains to your situation. The list of compatible Network CGs are, COMPIX NewsScroll, COMPIX Autocast, Simple Chyron Intelligent IF, Raw Chyron IntelIF & ChyTV, Simple ChyTV IF, CODI Net CG, Cayman Graphics, Fox Splicer/DCM, Inovonics RDS730.

Remote CG Net Host IP and Port
In this field, type the IP address and the port of the CG that is on the same network connection that your DASDEC is on.

All FIPS codes trigger
Check to enable all alerts, regardless of FIPS codes, to trigger a crawl on the target Net CG clients. Uncheck to only allow alerts for specific FIPS areas to trigger the crawl. When unchecked, you can select from the FIPS Group pull-down menu. Alerts to any FIPS code within the group will be sent to the remote Net CG clients.

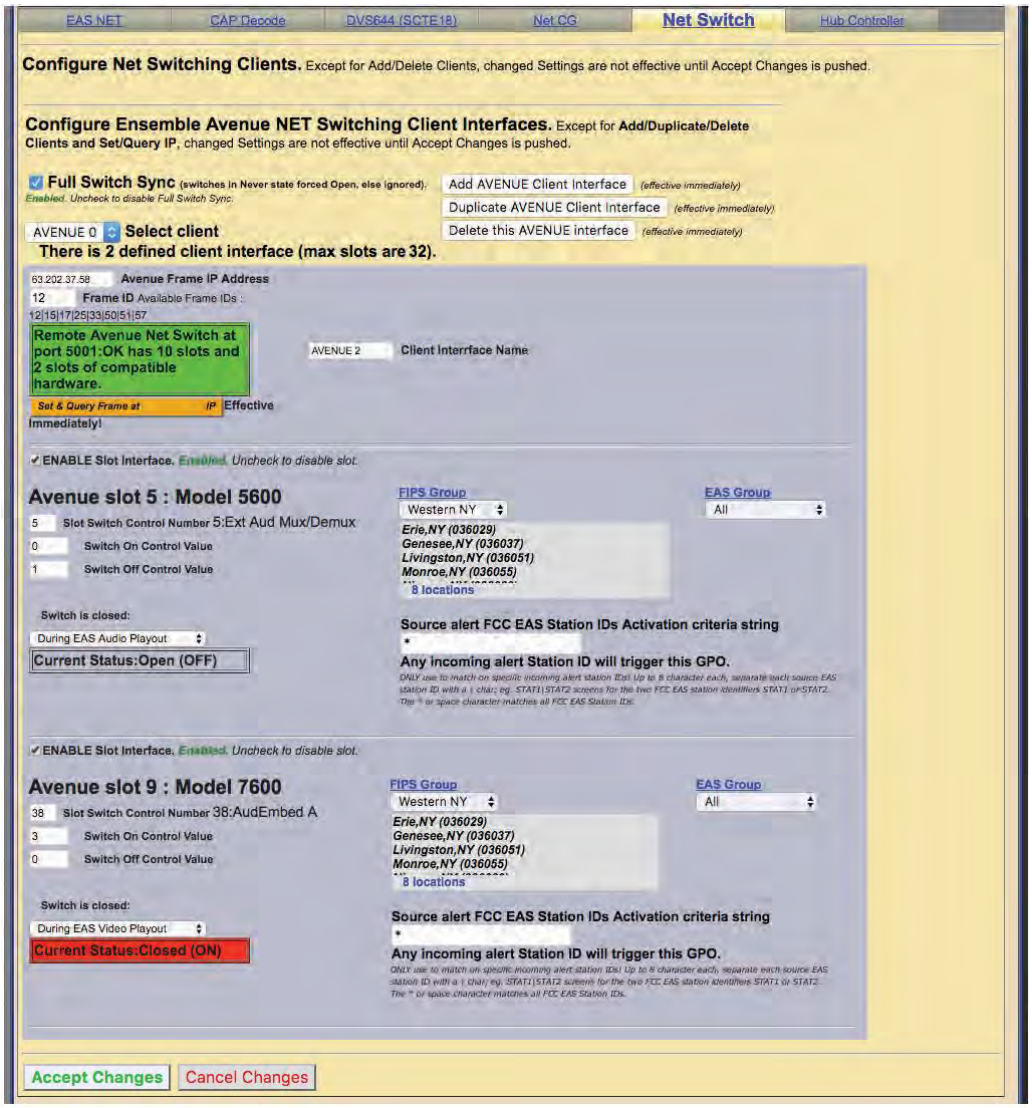
All EAS codes trigger
If enabled, all EAS codes will trigger the Net CG client interface. Set the check box to enable/disable EAS code filtered trigger control. If disabled, the alert EAS code is filtered for a specific match as a way to control whether or not the target Net CG client is triggered. If All EAS is disabled, select an EAS Group from the pull-down menu. If the EAS code of an active forwarded/originated alert matches any of the EAS codes within that group, the alert will be sent using the Net CG client. With careful use of this feature, and with multiple clients, one EAS device can serve many different regions at the same time.

All incoming alert Station IDs trigger
This is additional filter criteria for activation of this Net CG client. Enter the desired Station ID or Station ID's (separated by a '|') into this text field – up to 8 characters for each ID. This Net CG client will not activate without matching this station ID(s). The default value is the wildcard character (*). All station ID's will activate this Net CG client when using that character.

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

Net Switch

The **Net Switch** sub-tab enables control of an Ensemble Designs Avenue™ 7600 HD/SD Embedder/Disembedder for EAS alert audio switching. Utilizing the onboard audio channel swap and shuffle capabilities of the Avenue 7600 module, users can switch between EAS alert audio (assigned to AES 7/8) and 5.1 program audio (AES 1/2, 3/4, 5/6). The Net Switch sub-tab is displayed with a valid Plus Package license key.



Net Switch Sub-Tab

Configure Net Switching Clients

Click the **Add AVENUE Client Interface** button to add a new Net Switching Client. This action will create a new client interface named AVENUE 0. This descriptive name can be changed by typing new text in the **Client Interface Name** text field.

Avenue Frame IP Address
Enter the IP address of the Avenue frame.

Frame ID
Enter the Frame ID from the list of Available Frame IDs below this text box.

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

Slot Switch Control Number
Enter the slot number of the desired card/module.

Switch On Control Value
Enter the switch on control value.

Switch Off Control Value
Enter the switch off control value.

Switch is closed:
This pull-down menu provides a choice of actions within the EAS device that will trigger the Avenue module.

The actions can be tied to alert FIPS Groups, EAS Groups, and specific EAS Station IDs. To add FIPS code filtering, click the desired selection from the **FIPS Group** pull-down menu. Active alerts containing any of the FIPS codes contained in the selected FIPS Group will trigger that relay (close the contact) while the associated condition is true. Repeat the same process selecting an EAS code group from the **EAS Group** pull-down menu. When selecting "All" from either the FIPS Group or EAS Group pull-down menus, no filtering will take place.

The default value in the **Source alert FCC EAS Station IDs Activation criteria string** is an asterisk (*). This is a wildcard that will not filter for specific Station IDs. Only enter text in this field to match on specific incoming alert Station IDs. Up to 8 character each, separate each source EAS station ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2).

Attention
An Ensembles Designs Avenue 5035 (1RU Frame) or 5030 (3RU Frame) System Control module is required for switching audio from an EAS device.

Note
This interface supports both the Avenue 5600 Embedder/Disembedder and 7600 HD/SD Embedder/Disembedder. As of the writing of this manual, the Avenue 5600 has been discontinued and is no longer available.

Hub Controller / Net GPIO

This sub-tab under **Setup > Net Alerts** is a standard feature on a EAS device to allow remote, LAN connected GPIO relays and inputs to be associated to active alerts. **Hub Controller** is used in a One-Net and **Net GPIO** is used in a DASDEC. Both have the exact same controls and are grouped together in this manual for that reason. The EAS device supports the following equipment:

- Digital Alert Systems – R190A Hub Controller (four relays)
- Digital Alert Systems – R197 Audio Switch
- Digital Alert Systems – R198 AES Audio Switch
- Titus - W300
- Control by Web – WebRelay-Quad (four relays)
- Control by Web – WebRelay-Dual (two relays)
- Dataprobe – iPIO-8 (eight relays)

This interface page provides for the creating, duplicating, deleting and configuring client connections for up to eight LAN positioned relays. This type of hardware provides an inexpensive and convenient way to expand the contact closures relays of the EAS device. Since these relays can be placed on a LAN, and controlled by the EAS device remotely, they can be used to trigger actions during alerts without extra wiring. Configuration is much like other Net Alert pages. Up to 8 clients can be configured and active at a time.

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

Attention
Because a Net GPIO unit must be continually queried via HTTP for an input contact closure, this option is slow compared to GPIO input hardware that is directly a part of the EAS device. Thus this option requires the contact closure to last for at least one second in order to be detected.

Configure Net GPIO Connection

Below is a description of the client interface controls.

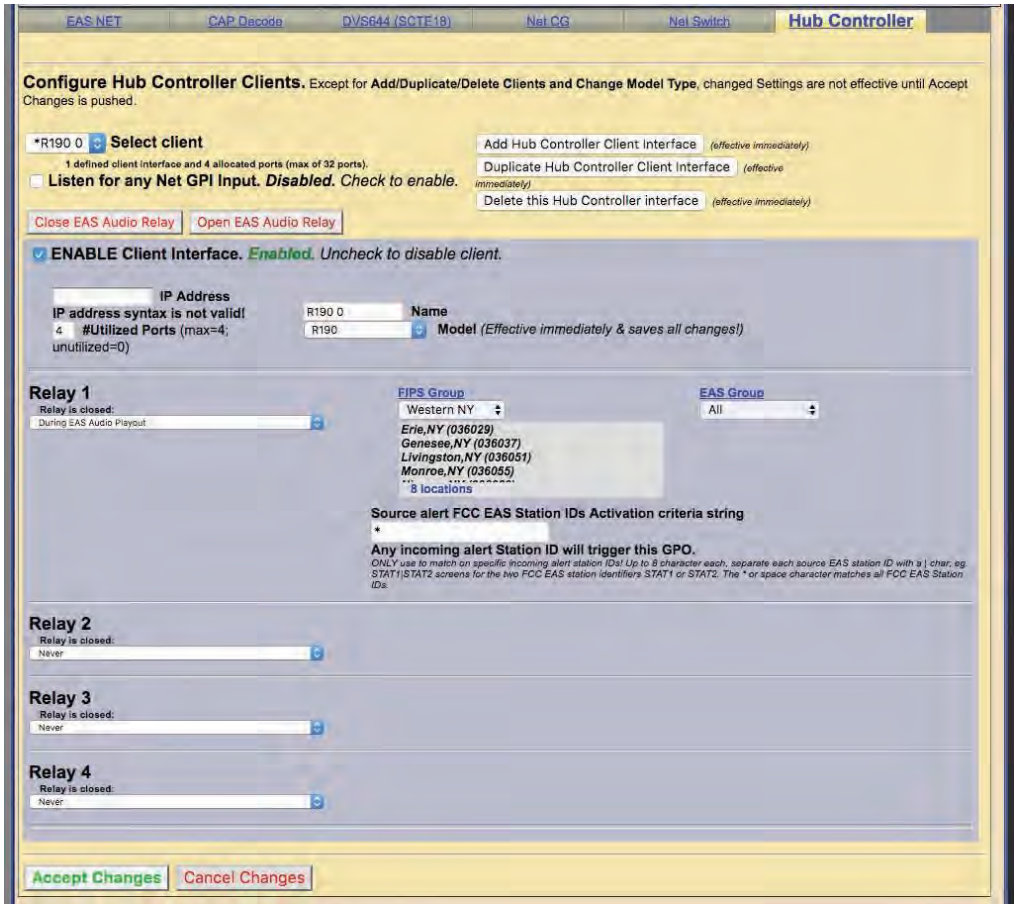
Select client
Use the pull-down menu to select the client interface to examine or configure.

Listen for Net GPIO Input
When enabled this check box causes the EAS device to listen for input contact closures from the Net GPIO units. This option only works if at least one of the connected Online Net GPIO units supports inputs. As of EAS device version 8.0, only the Web Relay Dual unit supports inputs. **Only enable this option when an input from a Net GPIO unit is required.**

Add / Duplicate / Delete NetGPIO Client Interface
You can create configurations for up to 8 Net GPIO clients.

- If no client configurations exist, or if you want a new one, click the **Add NETGPIO Interface** button to create a new interface configuration.
- To delete a client configuration, select the client and click on **Delete this GPIO interface**.
- To duplicate an existing client interface (a different name will be automatically generated), select the **Duplicate NETGPIO Client Interface** button. This is the best way to create many client interfaces that are mostly the same except for the IP address.

Close EAS Audio Relay, Open EAS Audio Relay
Manual overrides intended for test purposes. Pressing either button will either close or open any audio relays programmed for audio playout. This will control both the internal relays and the Net Controller / Net GPIO relays programmed for audio playout.



Hub Controller / Net GPIO Sub-Tab

Caution
Net GPIO client configuration addition, duplication, and deletion is immediate and cannot be canceled.

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 Playout
- Momentarily at start of EAS Audio Playout
- Momentarily at end of EAS Audio Playout
- Momentarily at start and end of EAS Audio Playout
- During EAN Audio Playout (During Live EAN/NPT Audio Playout)
- During EAS Video Playout
- During Main Serial EAS Playout
- 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 Playout
- During Audible parts of segmented live EAS Audio
- During audio preview
- During Global Auto-Forward mode enabled
- During Station Auto-Forward mode enabled

NET GPIO Input Action

The Web Relay Dual client provides 2 inputs. A variety of actions can be triggered on the EAS device when a contact closure is made on these inputs. The following list shows the various actions. These selectors are only available when **Listen for Net GPIO Input** is enabled and only for Hub Controller / Net GPIO units that support input.

- None
- Issue Weekly Test (RWT) upon closure
- Start segmented live EAS on closure; more closures skip to EOM
- Acknowledge unforwarded active alert and play decoded audio
- Acknowledge unforwarded active alert and/or play decoded audio
- Forward active decoded EAS upon closure
- Forward active RMT wit original decoded audio
- Preview RMT substitute alert audio
- Preview active decoded alert audio
- Re-enable forwarded EAS alert
- Originate cued alert
- Hold or Release Non-National EAS alerts
- Allow or Block net/serial interface operation
- Light Front Panel Alert LED while closed
- Toggle Global Auto Forward mode upon closure
- Toggle Station Auto-Forward mode closure

The actions can be tied to alert FIPS Groups, EAS Groups, and specific EAS Station IDs. To add FIPS code filtering, click the desired selection from the **FIPS Group** pull-down menu. Active alerts containing any of the FIPS codes contained in the selected FIPS Group will trigger that relay (close the contact) while the associated condition is true. Repeat the same process selecting an EAS code group from the **EAS Group** pull-down menu. When selecting “All” from either the FIPS Group or EAS Group pull-down menus no filtering will take place.

The default value in the **Source alert FCC EAS Station IDs Activation criteria string** is an asterisk (*). This is a wildcard that will not filter for specific Station IDs. Only enter text in this field to match a specific incoming alert Station IDs. Up to 8 characters each, separate each source EAS station ID with a vertical bar (|) character (e.g. STAT1|STAT2 screens for the two FCC EAS station identifiers STAT1 or STAT2).

Note
The option “During Audible parts of segmented live EAS Audio” requires a valid Plus Package license key.

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

GPIO SETUP

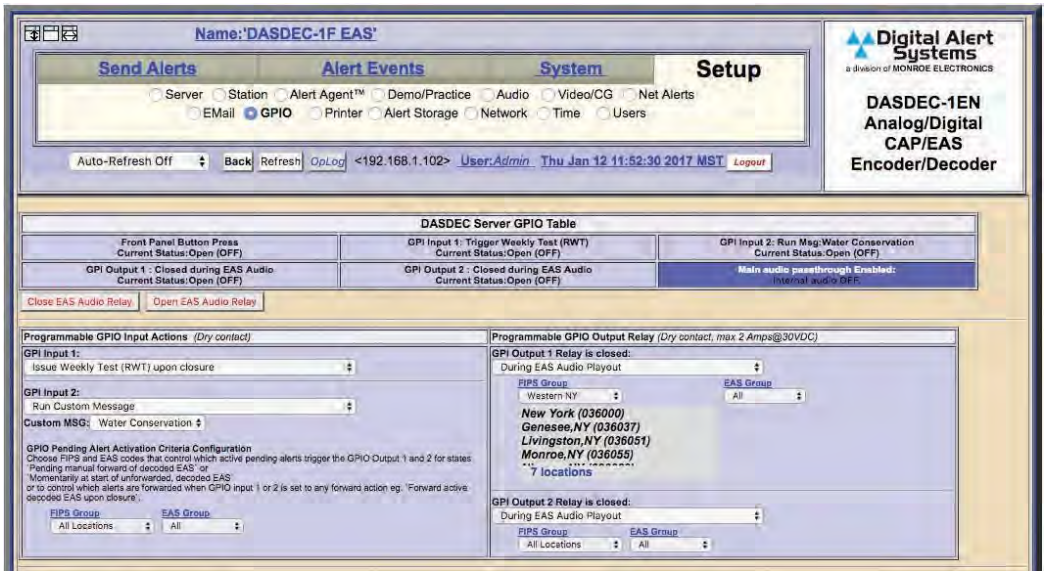
The Setup GPIO page allows the user to program and display the state of the General Purpose Inputs and Outputs (GPIO) settings. GPIO wiring is provided by connectors on the back panel of the EAS device or through networked attached units.. The state of the Front Panel button and the Internal Balanced Audio output is included in the GPIO table display.

Auto-Refresh Timer

With a valid Plus Package license key the web interface displays an **Auto-Refresh Timer** pull-down menu in the left corner of the screen header. This allows the page to refresh every 15, 30, or 60 seconds. This feature can be used to automatically view updates to the GPIO status.

The GPIO web interface contains the following sections:

- **Server GPIO Table**
- **Programmable GPIO**
- **Expansion GPIO Input / Output Tables** *(when configured with an Expansion GPIO option)*
- **Network GPIO Table** *(if a network-attached GPIO unit is configured)*



GPIO Setup Screen

Server GPIO Table

The top section of this page displays the current status of the built-in GPIO hardware. The top row displays the status of the inputs. The first input is the state of the Front Panel button. This is not available as a GPIO input but uses the internal GPIO circuitry. The next two columns show the programmed actions and current closure state for GPIO inputs 1 and 2. The second row displays the status of the relay outputs and of the internal audio/pass-through relay. The first two columns show the programmed triggers and current closure state for GPIO outputs 1 and 2.

Two buttons are placed under the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio. The companion button, **Open EAS Audio Relay**, sends the command to open all relays programmed to EAS audio playout.

Note
Changes made to the GPIO actions/ relay associations are immediate and the screen updates instantly.

Caution
The **Close/Open EAS Audio Relay** buttons apply to ALL relays assigned to EAS audio playout – both internal and external (Net Controller / Net GPIO) relays. Make sure the use of these buttons does not negatively impact regular EAS operations.

Programmable GPIO Input / Output Actions

Programmable options are GPIO Input 1, GPIO Input 2, GPIO Output 1 Relay, and GPIO Output 2 Relay. The available pull-down menu selections will vary depending on the enabled license keys. Pay close attention to the following descriptions to view the appropriate pull-down menu options.

GPIO Input 1

A pull-down menu allows GPIO Input 1 to be programmed to do one of the following:

- None
- Issue Weekly Test (RWT) upon closure
- Start segmented live EAS on closure; more closures skip to EOM (△)
- Acknowledge unforwarded active alert and play decoded audio
- Acknowledge unforwarded active alert and/or play decoded audio (△)
- Forward active RMT with original decoded audio (△)
- Preview RMT substitute alert audio (△)
- Preview active decoded alert audio (△)
- Forward active decoded EAS upon closure
- Re-enable forwarded EAS alert
- Forward active decoded EAS once to all upon closure (§)
- Re-enable EAS alert forwarded once to all (§)
- Originate cued alert (△)
- Hold or Release Non-National EAS alerts
- Allow or Block net/serial interface operation
- Light Front Panel Alert LED while closed
- Toggle Global Auto Forward mode upon closure
- Run Custom Message (▼)

A valid Plus Package license key is required to view/select any of the above items with a (△) symbol. MultiStation is required to view/select the above items with a (§) symbol. Custom Message Pro is required to view/select the above item with a (▼) symbol.

GPI Input 2

A pull-down menu allows GPIO Input 2 to be programmed to do one of the options below. The same pull-down menu options from GPI Input 1 are available for GPI Input 2.

GPIO Output 1 Relay

This selection box allows for programming the GPI Output 1 closure. Set according to the condition that needs to be monitored. The following is a list of the available pull-down menu selections:

- Never
- During EAS Audio Playout
- Momentarily at start of EAS Audio Playout
- Momentarily at end of EAS Audio Playout
- Momentarily at start and end of EAS Audio Playout
- During EAN Audio Playout (During Live EAN/NPT Audio Playout) (**X**)
- During EAS Video Playout
- During Main Serial EAS Playout

- Momentarily at start of decoded EAS
- Momentarily at start of unforwarded, decoded EAS (**X**)
- Pending manual forward of decoded EAS (**X**)
- Pending acknowledgement of unforwarded, active decoded EAS (**X**)
- During EAS alert cued (confirm general origination)
- During hold of EAS until GPI closure
- During hold of EAS during GPI closure
- During Audible parts of segmented live EAS Audio
- During audio preview (**X**)
- During Global Auto-Forward mode enabled (**X**)
- During Station Auto-Forward mode enabled (**X**)

GPIO Output 1 Activation Filter Configuration
Choose the FIPS Group and/or EAS Group that will control which alerts trigger the applicable programmed GPIO output 1 relay. Items in the above GPI Output Relay pull-down menu list that contain an (**X**) do not offer FIPS Group and/or EAS Group filtering.

GPI Output 2 Relay
This pull-down menu allows for programming the GPI Output 2 Relay. Operation of this relay is the same as GPI Output 1 Relay above.

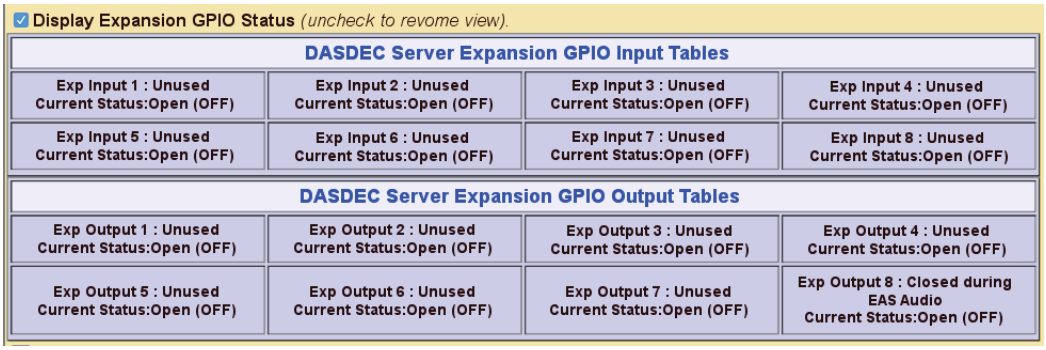
GPIO Output 2 Activation Filter Configurations
Choose the FIPS Group and/or EAS Group that will control which alerts trigger the applicable programmed GPIO output 1 relay. Items in the above GPI Output Relay pull-down menu list that contain an (**X**) do not offer FIPS and/or EAS Group filtering.

GPIO Pending Alert Activation Filter Configuration
Choose FIPS Group and EAS Group to control which active pending alerts trigger the GPIO Output 1 or 2 Relay for states **Pending manual forward of decoded EAS** or **Momentarily at start of unforwarded, decoded EAS** or to control which alerts are forwarded when GPIO Input 1 or 2 is set to **Forward active decoded EAS upon closure**.

This interface is only present when the GPI Input 1 or 2 is programmed to **Forward active decoded EAS upon closure**, or when the GPIO Output 1 or 2 Relay is set to close **Pending manual forward of decoded EAS**. This interface allows the selection of FIPS Groups and EAS Groups filtering criteria to be applied to the programmed GPI input action or to be applied to an alert that would trigger either GPIO 1 Relay or GPIO 2 Relay closure. Use this interface to narrow down active alerts that will be forwarded upon GPI input contact closure or to narrow which active unforwarded alerts trigger a relay closure. To use the interface, select the desired group from the **FIPS Group** and/or **EAS Group** pull-down menu. All selections are immediately active once the desired group is selected.

The remainder of the GPIO screen provides status displays for:

- Expansion GPIO
- Multiplayer GPIO
- Hub Controller / Net GPIO



Expansion GPIO Status Table

Display Expansion GPIO Status

If the EAS device is configured with an internal expanded GPIO card, the **Display Expanded GPIO Status** check box will appear on this screen and there will be a sub-tab labeled **Expansion GPIO** within the **Setup > GPIO** menu. Click this check box to view the Expansion GPIO Table where the status of each GPIO input and output is shown. Configuration of the Expansion GPIO is performed within the **Setup > GPIO > Expansion GPIO** sub-tab.

Display Multiplayer GPIO Status

The **Display Multiplayer GPIO Status** check box will appear if the EAS device is configured with an external MultiPlayer (for MultiStation support). Click this check box to view the Multiplayer GPIO Table where the status of each GPIO input and output is shown. Programming of these GPIOs is performed within the Multiplayer sub-tab within **Setup > GPIO**. To setup a new Multiplayer, go to **Setup > Audio > Multiplayer**. Configuration of the MultiPlayer is performed on the **Setup > GPIO > Multiplayer GPIO** screen. (See below for more details)

Display Net GPIO Status

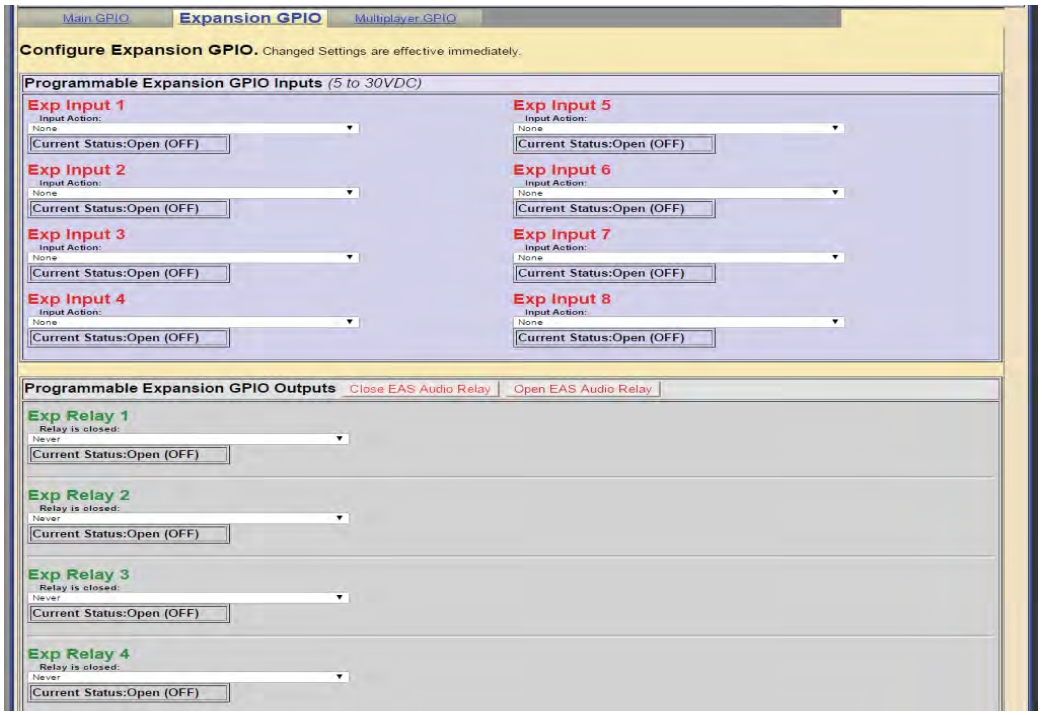
If the EAS device is configured with an external Hub Controller / Net GPIO unit, the **Display NET GPIO Status** check box will appear. Click this check box to view the Hub Controller / Net GPIO Table where the status of each GPIO is shown. To add, delete and configure a Hub Controller / Net GPIO unit go to **Setup > Net Alerts > Hub Controller / Net GPIO** screen.

MultiStation Mode

When MultiStation mode is enabled, the configured GPIO outputs are selectable for each station. A station can choose to NOT use a GPIO output. The station assignment options do not allow reprogramming of a relay, just its inclusion. This allows specific GPIO outputs to be assigned to different stations and thereby recognized as triggering an action because a specific station is active. Configure per station used GPIO output relays on the proper station interface configuration page under **Setup > Station** and use the appropriate station sub-tab(s).

Expansion GPIO

When an Expansion GPIO board is installed, the **Expansion GPIO** sub-tab is available within the **Setup > GPIO** menu. This factory installed option adds 8 more GPIO inputs and 8 more GPIO outputs. The configuration of these inputs and outputs is performed in this sub-tab.



Expansion GPIO Sub-Tab

This configuration screen works the same way as other GPIO settings. The screen is divided into two sections: **Programmable Expansion GPIO Inputs** and **Programmable Expansion GPIO Outputs**.

Programmable Expansion GPIO Inputs

The GPIO inputs are labeled **Exp Input 1 – 8**. Each input has an **Input Action** pull-down menu where users select the desired action based on triggering that input. The pull-down menu options are the same as the GPIO Input 1 selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Input Action** pull-down menus.

Programmable Expansion GPIO Outputs

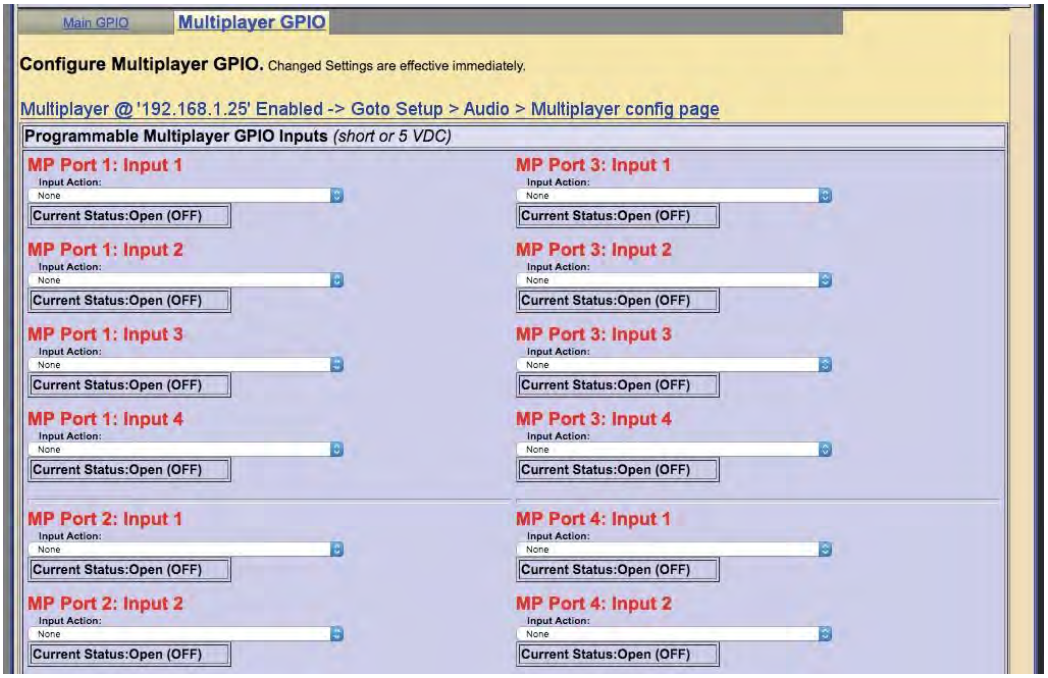
The GPIO outputs are labeled **Exp Relay 1 – 8**. Each output has a **Relay is closed** pull-down menu where users select the desired action to close the associated relay. The pull-down menu options are the same as the GPIO Output 1 Relay selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Relay is closed** pull-down menu.

After selecting an option from the **Relay is closed** pull-down menu, **FIPS Group**, **EAS Group** and **Station ID** filtering is available for most options.

Two buttons are located at the top of the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio playout. The companion button, **Open EAS Audio Relay**, sends the command to open all relays that are programmed to EAS audio playout.

Multiplayer GPIO

In situations that require an additional EAS audio playout channel (i.e. MultiStation mode), an external MultiPlayer can be added. Along with the four audio channels, the MultiPlayer includes four GPIO inputs and two GPIO outputs per audio channel. When configured, a MultiPlayer sub-tab will appear within the **Setup > GPIO** menu. MultiStation and MultiPlayer options require a valid Plus Package license key.



MultiPlayer Sub-Tab

This configuration screen works in the same way as the other GPIO settings. The screen is divided into two sections: **Programmable MultiPlayer GPIO Inputs** and **Programmable MultiPlayer GPIO Outputs**.

Programmable MultiPlayer GPIO Inputs

Each MultiPlayer audio channel (or MP Port) is numbered (1 - 4). The web interface label 'MP Port 1: Input 3' represents GPIO input 3 on MultiPlayer port 1. There is an **Input Action** pull-down menu where users select the desired action based on triggering that input. The pull-down menu options are the same as the GPIO Input 1 selections listed above.

Programmable MultiPlayer GPIO Outputs

The GPIO outputs are labeled by MP Port (1 - 4) and relay number (1 - 2). The web interface label 'MP Port 2: Relay 1' represents GPIO output relay 1 on MultiPlayer port 2. Each output has a **Relay is closed** pull-down menu where users select the desired action to close the associated relay. The pull-down menu options are the same as the GPIO Output 1 Relay selections listed above. The **Current Status** [Open (OFF) or Closed (ON)] is displayed just below each **Relay is closed** pull-down menu.

After selecting an option from the **Relay is closed** pull-down menu, **FIPS Group**, **EAS Group** and **Station ID** filtering is available for most options.

Two buttons are located at the top of the table for testing GPIO output relays. The first button, **Close EAS Audio Relay** sends out a command to close all relays programmed to EAS audio playout. The companion button, **Open EAS Audio Relay**, sends the command to open all relays programmed to EAS audio playout.

The **Current Status** [Open (OFF) or Closed (ON)] is displayed below each Input Action pull-down menu.

For more information regarding the installation and configuration of a MultiPlayer, see the Quick Start Guide included with the MultiPlayer or download it from the Digital Alert Systems website.

PRINTER SETUP

A basic task associated with EAS is printing logs of alert activity. The EAS device allows multiple means to retrieve alert event information for printing logs:

- Logs can be printed from a host computer using the web browser interface
- Logs/reports can be e-mailed from the EAS device and printed on a local/ network printer (see **Setup > EMail**)
- Individual alerts can be printed directly from the EAS device

The first two options require some manual intervention. The third option and the topic of this section, will enable the automatic printout of EAS alerts as they occur. Using this approach means that each alert will print on an individual page.

Connecting to a Network Computer or Via USB

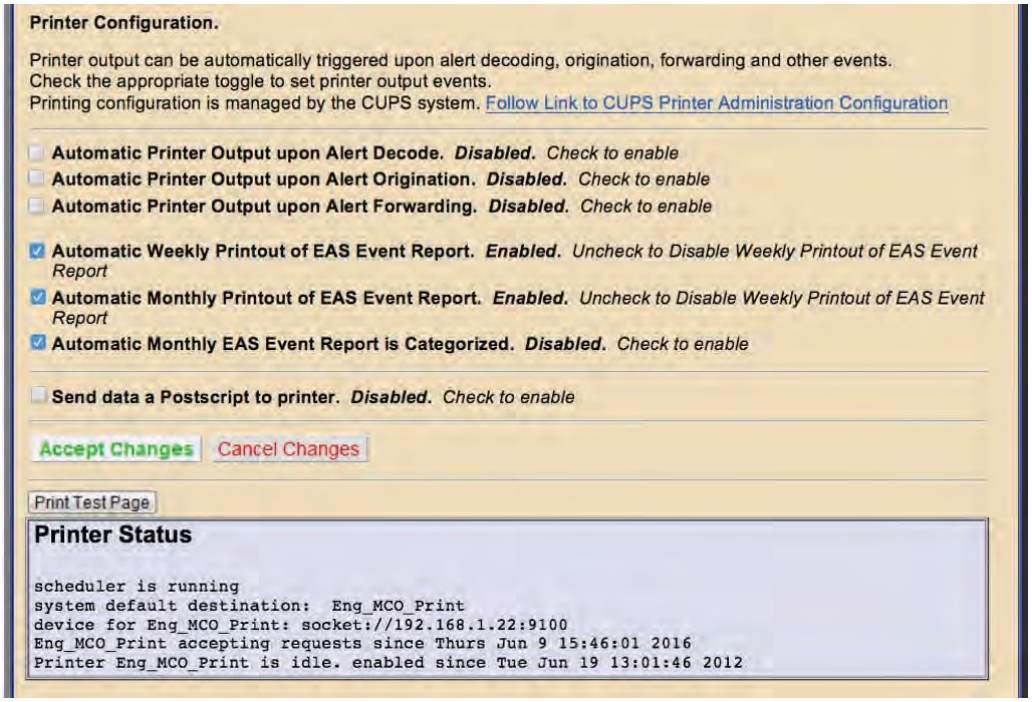
- To connect to a printer via USB, plug the printer into a USB port located on the back of the EAS device. Then click the **Follow Link to CUPS Printer Administration/Configuration** hyperlink. Click on the **Printers** tab at the top of the page. If the printer you have pugged in shows up on the page you must click **SET THE PRINTER AS THE DEFAULT PRINTER**. Then print a test page to make sure it works.
- To connect to a Network computer, go to **Setup > Printer** from a web browser interface. Click the **Follow Link to CUPS Printer Administration/ Configuration** hyperlink On the CUPS homepage, click **Add Printer**. Fill out all the information. You will need to know the IP address of the computer on the network, as well as information about the brand and model.

It is important to set your printer up as the default printer. Even if you have only one printer, at the end of your setup, you need to set that printer as default. This option is the way that CUPS communicates with the EAS device. If you do not set the printer to default, it will not work.

Attention
When filling out the Add New Printer text fields, make sure NOT to use the following characters: "/", "#", or space.

There is a thorough App-note on the website about connecting your printer via the Network. Go to http://www.digitalalertsystems.com/resources_application_notes.htm and find the App-note that pertains to connecting a printer to the EAS device.

Configuration



Printer Configuration Screen

There are seven check box options available, check to enable. They are:

Automatic Printer Output upon Alert Decode
When enabled, a report will be printed whenever an EAS alert is decoded.

Automatic Printer Output upon Alert Origination
When enabled, a report will be printed whenever an EAS alert is originated.

Automatic Printer Output upon Alert Forwarding
When enabled, a report will be printed whenever an active decoded EAS alert is forwarded.

Automatic Weekly Printout of EAS Event Report
When enabled, a report will be printed at midnight on Sunday morning of the previous weeks' worth of EAS activity.

Automatic Monthly Printout of EAS Event Report
When enabled, a report will be printed at midnight on the morning of the first day of the month of the previous months' worth of EAS activity.

Weekly and Monthly EAS Event Report is Categorized
When enabled, this option puts all of the prints in groups by type, and then puts them in order by date and time. The order is originated alerts, forwarded alerts, and then decoded alerts.

Send data as Postscript to printer
When enabled, Postscript data will be sent to the default printer.

Use the **Accept Change** button to save changes to this page.

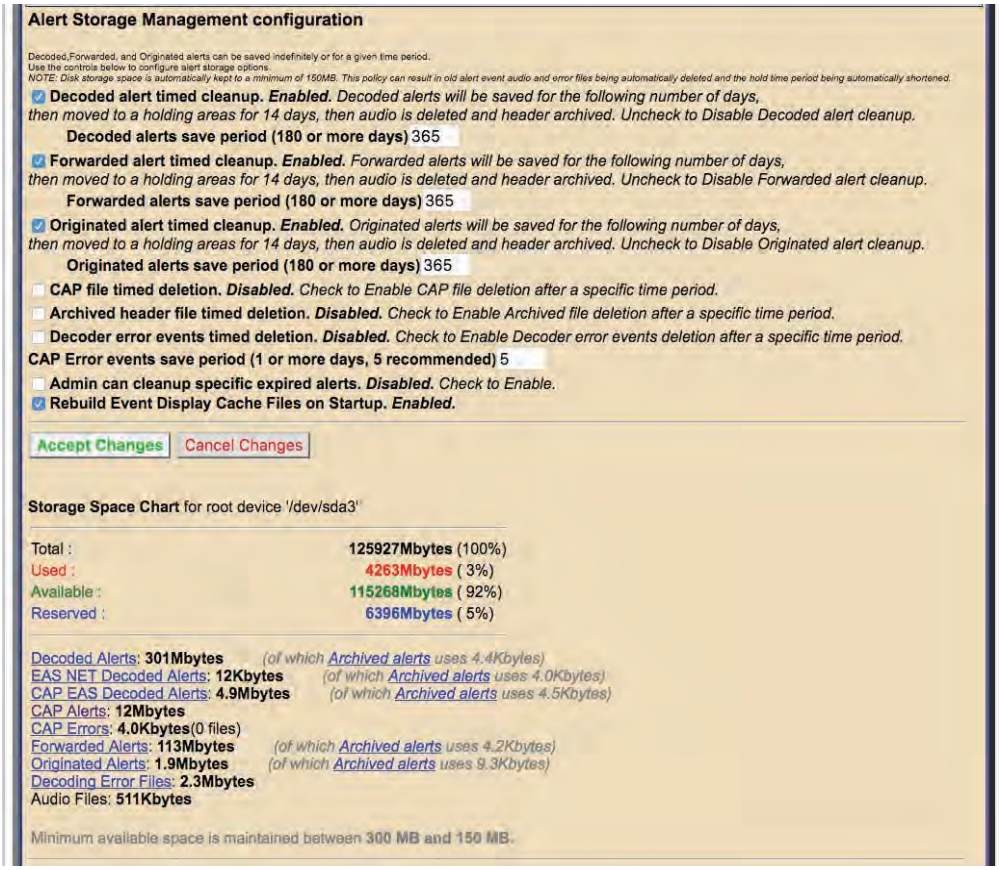
Below the printer options is a system status report about the configured line printer.

When a printer is configured, the expired alert status reports displayed on the **Alert Events > Incoming, Incoming/Decoded, Forwarded Alerts, Originated/Forwarded Alerts, Originated, and All Alerts** screens provide a **Print** button. You can use the Print button to test printing as well as to print reports of retrieved events.

ALERT STORAGE SETUP

The Alert Storage Management configuration screen has storage options that enable custom event storage management by timed deletion of the following event types:

- Decoded alerts
- Forwarded alerts
- Originated alerts
- CAP alerts



Alert Storage Setup Screen

By default, all event type data is configured to stay available on the EAS device for 365 days (unless the storage space drops below the minimum size of 100MB). Each event type is given a separate deletion control check box with a separately configurable deletion period. When enabled, event data (sound and text files) are deleted after the user-entered number of days. Timed deletion can also be completely disabled for any of the event types.

Deletion of an event consists of removing audio and text data. Event header text files are moved to the archive and always kept. Deletion does not purge the EAS device of its record of a past EAS event.

Storage Space Chart

Towards the bottom of the screen is a chart of the current storage space use. The chart shows the total capacity, the used space, available space, and reserved space in Megabytes. The storage space is further analyzed by specific alert event types. Hyperlinks are provided for each alert event type to guide the user to a directory of files for that specific alert event type.

Minimum space is maintained between 300 MB and 100 MB. If the EAS device available storage space drops below 100 Megabytes, the oldest events will be chosen for automatic deletion. This process is initiated after every alert event and at midnight every night. If a minimum space condition is detected, event data is deleted until at least 300 MB of space becomes available. The deletion time periods are also automatically adjusted downward if needed to reflect the dates of the deleted events.

Chapter 6: Alert Events Tab

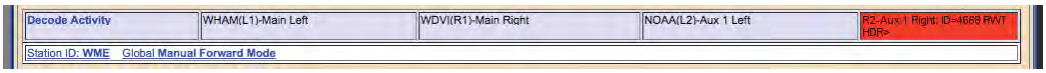
The **Alert Event** menu has six radio button options:

Radio Button	Description
Incoming Alerts	Displays the following: • Status of Incoming and Active Decoded alerts Unacknowledged alerts can be forwarded and Demo Decoded alerts can be added from this screen.
Incoming/Decoded Alerts	Displays the following: • Status of Incoming and Active Decoded alerts • Expired Decoded Alerts Unacknowledged alerts can be forwarded and Demo Decoded alerts can be added from this screen. EAS alert logs can be printed and/or saved.
Forwarded Alerts	Displays the following: • Status of Active Forwarded alerts • Expired Forwarded Alerts. EAS alert logs can be printed and/or saved.
Originated/ Forwarded Alerts	Displays the following: • A list of Scheduled Originated Alerts • Current Active Originated/Forwarded Alerts • Expired Originated/Forwarded Alerts EAS alert logs can be printed and/or saved.
Originated Alerts	Displays the following: • A list of Scheduled Originated Alerts • Current Active Originated Alerts • Expired Originated Alerts EAS alert logs can be printed and/or saved.
All Alerts	Displays the following: • A list of Scheduled Originated Alerts • Current Active Alerts • Expired Alerts EAS alert logs can be printed and/or saved.

Each radio button brings up status display screens of current and expired alerts. These screens show the active alerts and those that have expired or have been decoded, forwarded, and originated. These screens allow a precise audit of current and past EAS activity.

Auto-Refresh Timer

With a Plus Package license key, the web interface displays an **Auto-Refresh Timer** (just below and to the left of the page title in the header section) allowing the page to be re-displayed every 15, 30, or 60 seconds. Use this option to stay informed of the EAS device's decoding activity and decoded events status.



Decode Activity Table

Decode Activity Table

The Incoming Alerts, Incoming/Decoded Alerts, and Forwarded Alerts screens include the Decoder Activity Table which displays the input decoders for reference purposes. Each decoder channel has its own box in the table. When there is no incoming alert the channel is light blue. When there is an incoming decoding alert, the channel display box is red and displays the current state of the incoming decoding alert. In the screen shot below, event 4668, a Required Weekly test (RWT), is in process of being decoded, and the full header has been received (HDR>). The **Decode Activity** hyperlink takes users to the **Setup > Audio > Decoder Audio** screen.

Station ID and Global Forwarding Mode

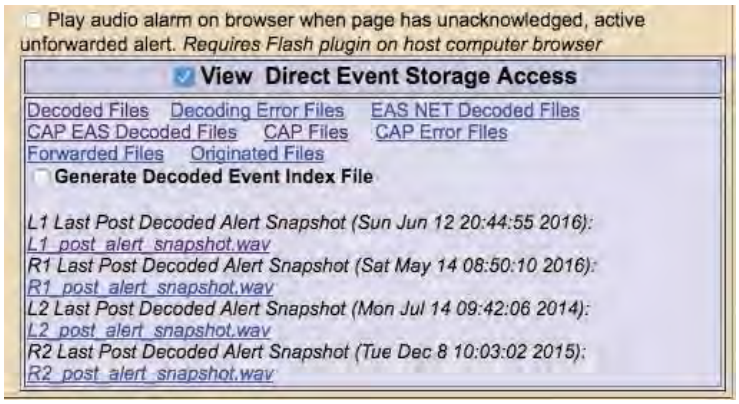
Just below the **Decode Activity** table are hyperlinks for **Station ID** and **Global Forwarding Mode** (either Manual Forward Mode or Auto-Forward Mode). Both hyperlinks take users to the **Setup > Station > Global Options** screen.

- In Auto-Forward mode, alerts that match the auto-forwarding criteria are automatically forwarded (played).
- In Manual mode, no decoded alerts are forwarded. Active alerts have a button allowing manual forward.
    - With the Plus Package license key unlocked, if GPI input is properly programmed, an unforwarded active alert can be forwarded via GPI contact closure. The Plus Package license also allows Manual Forwarding to be blocked for specific alerts that do not match the Auto-Forwarding filter criteria.

Alert Forwarding Action Table

Alert Forwarding Action Table *(Incoming Alerts & Incoming/Decoded Alerts)*

Below Active Decoded Alerts is the optional Alert Forwarding Action Table. It displays current settings for actions associated with forwarding the alert. The serial protocol, the Net Alert protocols, and the Analog Audio/Video states are displayed to make it easy to know what peripheral devices is triggered by alert forwarding. Labels inside this table are hyperlinks directing the web interface to the correct Setup page for changing the configuration of the associated action.

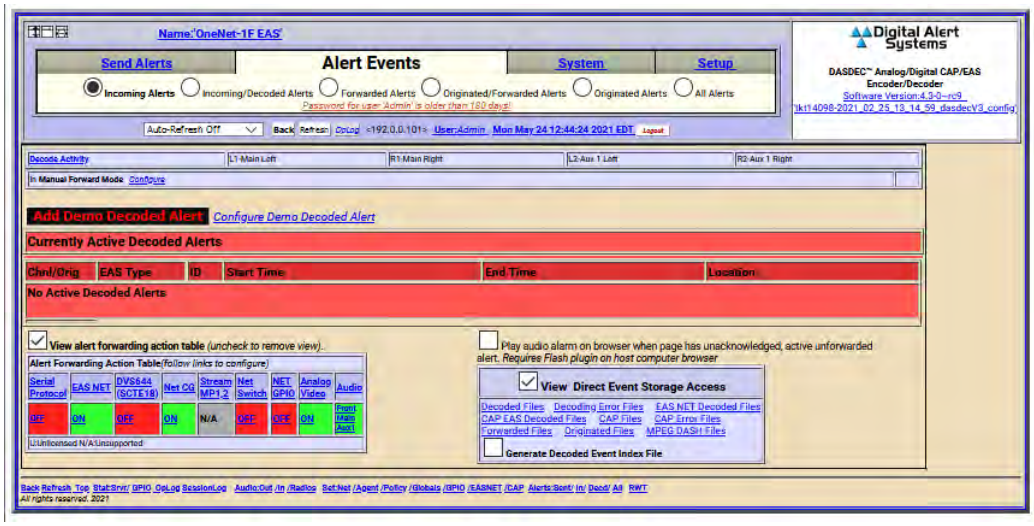


Direct Event Storage Access Table

Direct Event Storage Access table *(applies to Incoming Alerts & Incoming/Decoded Alerts only)*

To the right of the Alert Forwarding Action Table is the Direct Event Storage Access Table with hyperlinks to Decoded Files, Decoding Error Files, EAS NET Decoded Files, CAP EAS Decoded Files, CAP Files and CAP Error Files. These hyperlinks navigate the web interface into the disk file storage area for decoded alerts; EAS NET decoded alerts, and errored alerts. Navigating one of the hyperlinks will place the web interface into a file view where all alert event files can be directly examined and downloaded. This is useful if an alert could not be decoded. The WAV file saved during the decode error can be downloaded and examined or sent to Digital Alert Systems for analysis.

The Generate Decoded Event Index File can be toggled to generate a monthly index file of alerts received. Use it to automate queries of alert activity. Index files are stored in the Decoded Files storage area and are named “events_YYYY_M(M)”.



Incoming Alerts Screen

Note
All options within the Alert Events tab are immediate and do not require the Accept Changes button to become active.

INCOMING ALERTS

This screen shows the status of Incoming and Currently Active Decoded Alerts. The **Incoming Alerts** screen monitors new and incoming EAS alert activity. Broadcasters who manually forward alerts should stay logged into the EAS device to view the **Incoming Alerts** screen with the auto-refresh option enabled.

The **Incoming Alerts** screen displays the status of all incoming alerts "received" by the EAS device. This screen contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Event Storage Access Table (described above)

Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Add Demo Decoded Alert
- Acknowledge Pending Alerts
- Forward Alerts
- Edit/Review Forwarding Text/Audio

This screen does not provide the interface for accessing expired alerts – this is found in the section: Incoming/Decoded Alerts.

All other interfaces on this web page are described in the Incoming/Decoded Alerts below.

Note
Under normal operation, disable the display of both of these tables to speed up the page load and refresh.

INCOMING/DECODED ALERTS

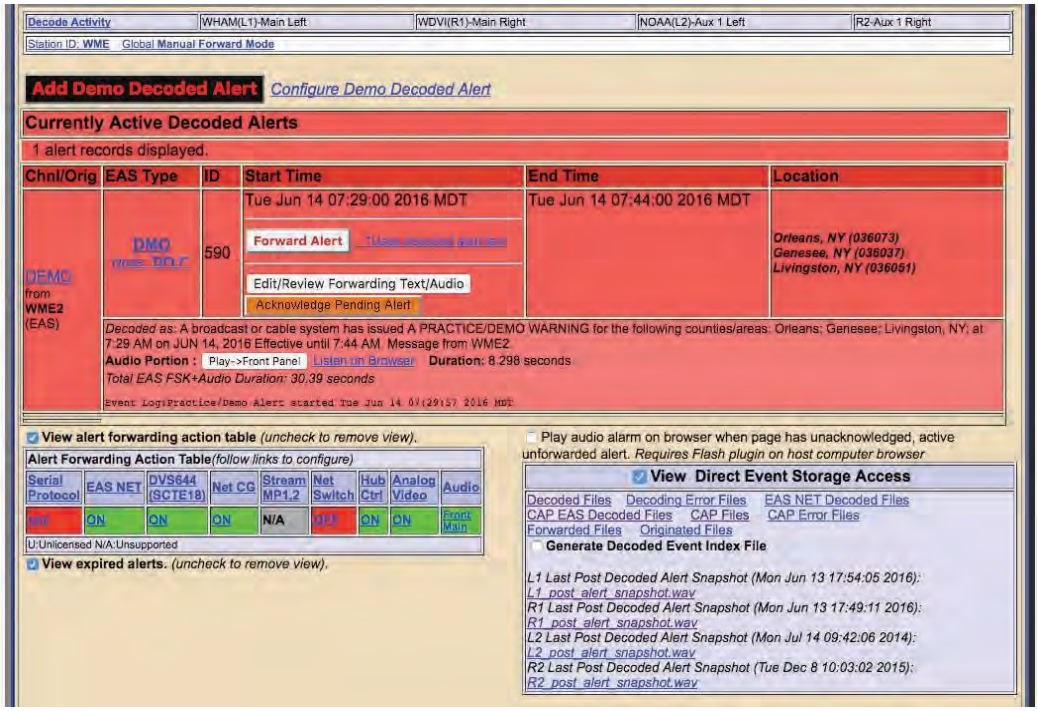
Incoming/Decoded Alerts indicates the status of Incoming, Active and Expired Decoded Alerts. It is the primary interface for viewing current and past decoding activity. It displays the current forwarding mode (auto-forward or manual), current decoding activity (active alerts), the alert forwarding action table, event storage access table, active decoded EAS alerts, and expired decoded EAS alerts.

The **Incoming/Decoded Alerts** screen displays status of all incoming and decoded alerts "received" by the EAS device. This screen contains the following sections:

- Currently Active Decoded Alerts
- Alert Forwarding Action Table (described above)
- Event Storage Access Table (described above)
- Expired Decoded Alerts

Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Add Demo Decoded Alert
- Acknowledge Pending Alerts
- Forward Alerts
- Edit/Review Forwarding Text/Audio
- Review expired Incoming/Decoded EAS alerts
- Display, save, and print EAS message logs



Incoming/Decoded Alerts Screen with Active Alert

Add Demo Decoded Alert

If the Demo Decode Alert mode is not enabled, go to **Setup > Demo/Practice** to enable it. This will make the **Add Demo Decoded Alert** button appear on the screen.

When Demo mode is enabled, simulate a newly decoded alert using the **Add Demo Decoded Alert** button shown below the Decode Activity Table. Pressing the button will generate an EAS DMO alert (Demo/Practice alert) and place it in the active decoded alert queue. This is a quick, convenient way to test the forwarding options. The Demo Alert is a real EAS alert and will have the same Manual Forwarding and Edit/Review button options as any other decoded alert. This is especially useful for practice and training of the Manual Forwarding options. Demo Alerts are set to a fixed duration of 15 minutes.

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.

Configure Demo Decoded Alert hyperlink

This text to the right of the **Add Demo Decoded Alert** button is a hyperlink to the **Setup > Demo/Practice** screen. From this screen the user can enable the Add Demo Decoded Alert button/feature and configure the parameters of the DMO alert message (see Chapter 5 - Demo/Practice).

Currently Active Decoded Alerts

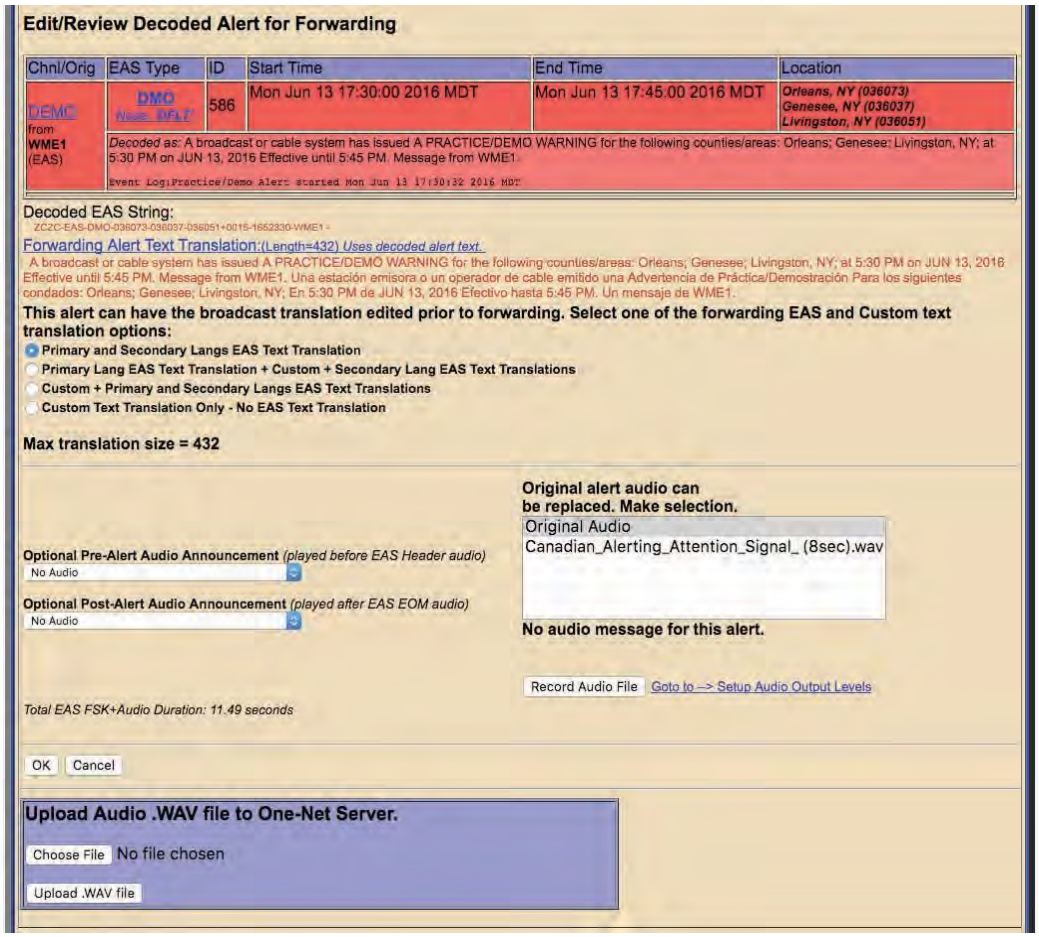
These alerts are below the Decode Activity Table and displays all decoded EAS alerts currently in progress between the start and end time for the alert. An active event remains on the active list until it reaches its expiration time, or until it is updated or canceled by another event of the same type and for the same area, which redefines the event times. Decoded alerts appear in the Currently Active Decoded Alerts list as long as they are current. Active events move to the expired alert list as each one reaches its end time.

Forwarded active events display the forwarding time as an active link label on the **Alert Events > Forwarded Alerts** status page.

Active events that are not automatically forwarded present buttons to allow review and editing, acknowledgment, and manual forwarding / re-enable manual forwarding. These buttons are described below.

Acknowledge Pending Alert

The screen shot above shows an active, unacknowledged, unforwarded alert for the active Demo alert. Decoded alerts that have not been forwarded or acknowledged will be in an *unacknowledged* state. This state is indicated on the EAS device's front panel status LED with a blinking slowly/regularly red light and within the web interface active alert status display by a flashing button labeled **Acknowledge Pending Alert**. To end the unacknowledged state and stop the front panel red status LED from flashing, click the flashing **Acknowledge Pending Alert** button. You can also acknowledge an alert by pressing the front panel button once or a by a programmed GPIO closure. Any alert that remains unacknowledged or unforwarded will remain in this state until it expires.



Edit/Review Decoded Alert for Forwarding Screen

Edit/Review Forwarding Text/Audio

To review and edit the alert audio before forwarding, click the **Edit/Review Forwarding Text/Audio** button. This button displays the **Edit/Review Decoded Alert for Forwarding** screen. It allows you to:

- Play the original audio, select a new audio message from the local audio file list, upload or record new audio, add audio announcements to be played prior to or after alert play-out.
- If the Plus Package license key is unlocked, you can add text that will be displayed on the local CG during forwarding.

Note
If a decoded alert expires during edit/review, it cannot be forwarded after exiting the Edit/ Review Decoded Alert for Forwarding screen.

The active decoded event is displayed as well as the translations that will be used when the alert is manually forwarded. Make changes as needed, and choose either the OK or Cancel buttons to return to previous alert status page.

Forward Alert button

The Forward Alert button will manually forward the alert. Once the alert is forwarded this button disappears from the active alert event display and is replaced by an **Enable Reforward** button, While an alert is actively being forwarded, a flashing indicator will display near the top of the page. A link labeled Forwarded followed by the time of forwarding, will also be displayed. Follow the link to the **Alert Events > Forwarded Alerts** page.

Blocked Alert Example

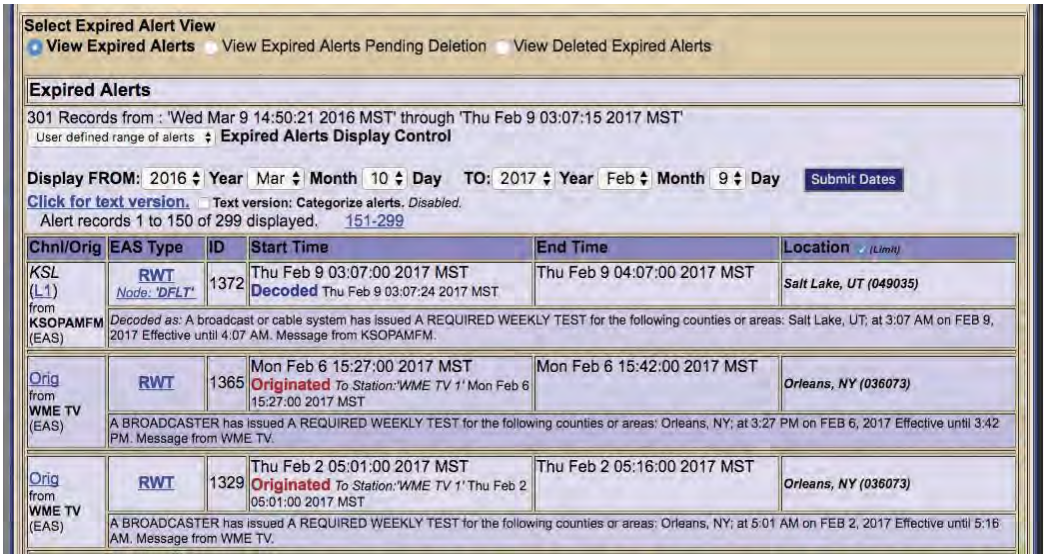
Blocked Forwarding

Any alert to be blocked will be displayed in the **Currently Active Decoded Alerts** list. A hyperlink will appear in the Start Time column titled **Forwarding blocked for this event**. Clicking this hyperlink will take the user to the **Setup > Alert Agent™ > Manage Alert Nodes** screen where the Alert Node was configured to block the alert.

Enable Reforward

Use the **Enable Reforward** button to allow a previously forwarded alert to be manually forwarded again. After this button is pressed, the **Forward Alert** button will again be displayed.

Note
With a valid Plus Package, the **Setup > GPIO** screen allows the **Enable Reforward** button to be triggered from a GPIO input contact closure by selecting **Re-enable forwarded EAS alert**.



Expired Alerts Section

View Expired Alerts

These check boxes enable the display of the following expired alerts:

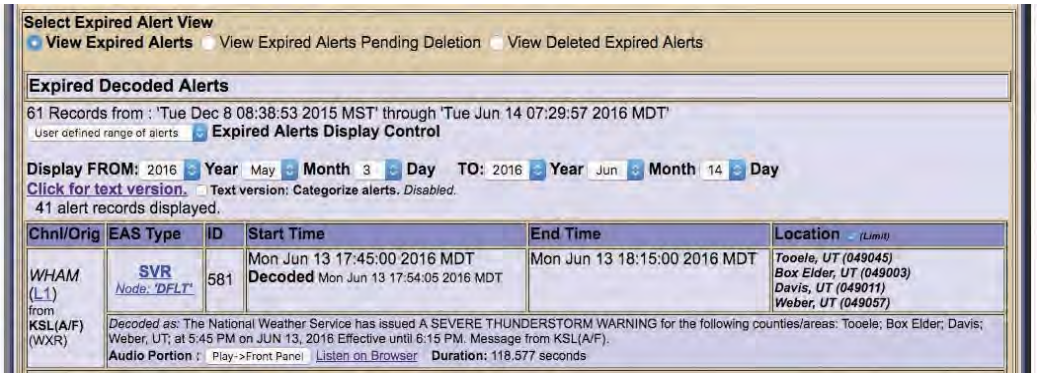
- Expired Alerts (complete audio, text and aux data is stored on disk)
- Expired Alerts Pending Deletion (pending audio file deletion)
- Deleted Expired Alerts (expired alerts that have had audio data deleted)

Use these radio buttons to select the types of expired alerts to be viewed. Each of the listed alerts contain hyperlinks and a button that can be used to review the specific expired alert.

The deleted alerts viewer will only show events if Alert Storage management is enabled. Select **Setup > Alert Storage**, and choose a date range for alert records. The screen shot below shows the most commonly used option **View Expired Alerts**. The other two options present the same interface.

Expired Decoded Alerts list

The Expired event list shows past decoded alerts for any range of dates. Use the pull-down menu titled **Expired Alerts Display Control** to view a multitude of date range options. A user defined date range is available enabling custom start and end dates (year, month, day). The screen shot shows an example of the expired alerts list for a selected range of dates.



Expired Alerts Section – Custom Date Range

Set the Date Range
Whatever Expired Alert View is selected, the number of expired alert records and the earliest to latest dates for these expired alerts is displayed. Control the expired alerts display date range by entering a from/to date. All expired alerts between and including these dates will be displayed in order.

To select a date range, select **User defined range of alerts** from the **Expired Alerts Display Control** pull-down menu. Next, choose a Year, Month, and Day for the FROM and TO dates. Make sure to click the **Submit Dates** button when finished entering the date range. All data for each expired alert decoded within the selected time period will display. Decoded headers are stored on the EAS device. This information is an accurate reflection of what was received. The EAS device can archive an enormous number of expired events and will automatically remove the oldest event descriptions as needed to reserve enough space for new alerts, however storage capacity is in the thousands so do not worry about losing important archived information.

A text version is available. Select the option **Click for text version**. This will display a text file copy of the current range of expired alerts in the browser. To categorize this text version by EAS codes, use the **Text version: Categorize alerts** check box. Otherwise the text version will be organized by date of alert.

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 **Click for text version**. This will print the text version of the displayed alerts. You may print the event status page to compile FCC paper documents for EAS test accounting.

Expired Alerts Display
Details about the alert is displayed in a table:

- The time the alert was decoded
- The time the alert was forwarded, and if it was forwarded

Forwarded alerts are displayed on the **Forwarded Alerts** or **Originated/Forwarded Alerts** screen.

Audio Portion
An alert with an audio message, can be played through the EAS device front panel internal speaker by clicking **Play->Front Panel** button inside the online alert entry area. You can also play the audio file on your host computer by clicking on **Listen on Browser** hyperlink. To listen to the audio, the host computer must have a WAV file player. Alerts without an audio message will not display either the **Play->Front Panel** button or **Listen on Browser** hyperlink.

TDX portion
If the alert has TDX details data, information is appended to the text translation for the alert. Also, links to any TDX-provided URL information is displayed. These links can be followed to go to web pages with more detailed information relevant to the alert. TDX details must originate from the alert source.

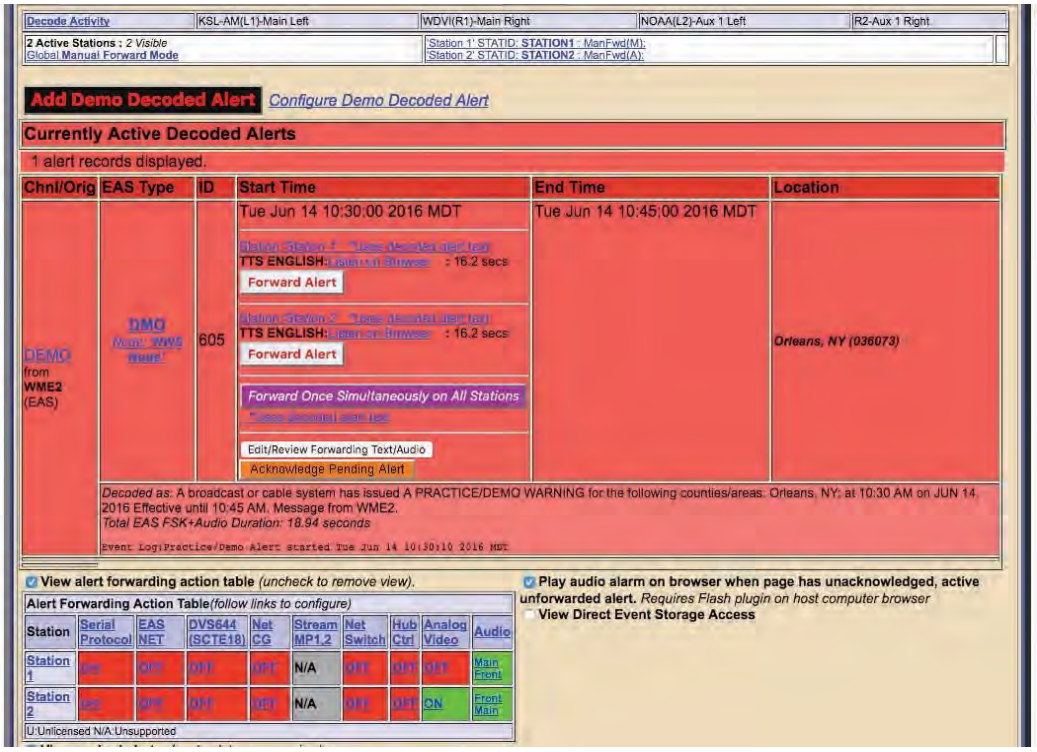
Play audio alarm on browser
On the right side of the page, under the Active Decoded alert table, is the **Play audio alarm on browser when page has unacknowledged, active unforwarded alert** check box to control an audible browser announcement for active, decoded alerts that have not yet been acknowledged or forwarded. Enabling this option on a speaker-equipped computer, along with an auto-refresh, can audibly notify control room staff that an alert has been decoded. Every time the browser page

refreshes while a decoded alert remains unacknowledged and unforwarded, an audio recording of the three burst EAS end-of-message "noise" will play over the host computer's speakers. The audio notification will stop once the alert is forwarded or acknowledged. An alert can be acknowledged using the **Acknowledge Pending Alert** button on the active alert status display, by pressing the EAS device's Front Panel button, or a programmed GPIO input closure.

Note
Adobe Flash Player must be installed for the audio notification to work.

Incoming & Incoming/Decoded Alerts: Multistation Mode

The active decoded alerts display supports MultiStation mode. You can view the active (enabled) stations on the right side of the page above the active decoded alerts table. Within the active decoded alert status, a target station ID and a **Forward Alert** button is displayed for each enabled station. Alerts can be forwarded to any station by pressing the appropriate **Forward Alert** button. The screen shot below shows one active, unacknowledged decoded alert, with two available enabled station targets and thus, two **Forward Alert** buttons, one per station. A single **Acknowledge Pending Alert** and **Edit/Review Forwarding Text/Audio** button is provided to cover MultiStation mode.



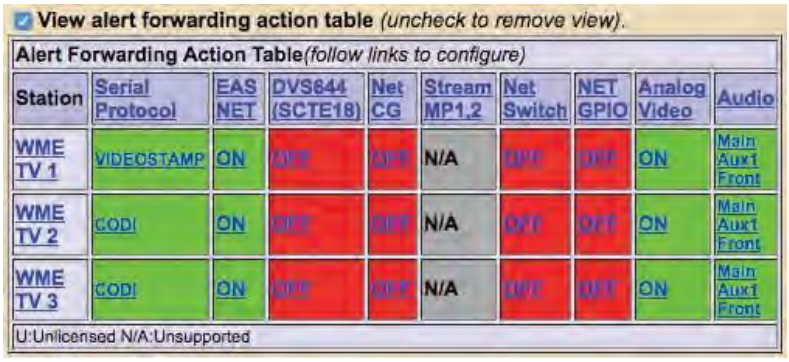
Active Decoded Alerts – MultiStation Mode

Note
In MultiStation mode, to customize the alert audio/text translation, you must run the Edit/Review process separately before station forwarding.

A severe EAS alert may need to be forwarded faster than to each enabled station in sequence. In that case, a separate button, labeled **Forward Alert Once for All Stations**, is available and can be pressed to forward the alert to the Main station configuration. If this button is used, all stations will forward immediately.

Alert Forwarding Action Table

Below the active alerts, the Alert Forwarding Action Table supports multiple station status by displaying the enabled and disabled actions per station. They may be changed at any time prior to forwarding in order to affect the outcome of actions when an alert is forwarded to a specific station. Follow the station name links to the **Setup > Station** (and appropriate station sub-tab) to change the desired settings for station alert forwarding.



View alert forwarding action table *(uncheck to remove view).*

Alert Forwarding Action Table *(follow links to configure)*

Station	Serial Protocol	EAS NET	DVS644 (SCTE18)	Net CG	Stream MP1,2	Net Switch	NET GPIO	Analog Video	Audio
WME TV 1	VIDEOSTAMP	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front
WME TV 2	CODI	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front
WME TV 3	CODI	ON	OFF	OFF	N/A	OFF	OFF	ON	Main Aux1 Front

U:Unlicensed N/A:Unsupported

Alert Forwarding Action Tale

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 shows the display for an active decoded alert after forwarding to the second station.

Currently Active Decoded Alerts

1 alert records displayed.

Chnl/Orig	Code	ID	Start Time	End Time	Location
DEMO from WKDQ/FM (EAS)	DMO	9	Tue Jun 19 13:42:00 2012 EDT Station:'Station 1' *Retranslates alert text Forward Alert Forwarded to Station 'Station 2' Tue Jun 19 13:44:49 2012 EDT Enable Reforward Station:'Station 2' *Uses decoded alert text Forward Alert Forward Alert Once for All Stations *Uses decoded alert text Edit/Review Forwarding Text/Audio	Tue Jun 19 13:57:00 2012 EDT	*Orleans, NY (036073)* *Genesee, NY (036037)* *Monroe, NY (036055)* *Niagara, NY (036063)* *New York (036000)*

Decoded as: THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A PRACTICE/DEMO WARNING FOR THE FOLLOWING COUNTIES/AREAS: Orleans; Genesee; Monroe; Niagara, NY; New York; AT 1:42 PM ON JUN 19, 2012 EFFECTIVE UNTIL 1:57 PM. MESSAGE FROM WKDQ/FM.

Audio Portion : Play->Front Panel Listen on Browser **Duration:** 11.699 seconds

Total EAS FSK~Audio Duration: 34.43 seconds

Event Log: Practice/Demo Alert started Tue Jun 19 13:42:14 2012 EDT

Active Decoded Alerts – MultiStation Mode w/ Enable Reforward button

Below is an example of the changes to the alert display after using the other **Forward Alert** buttons. The screen shot shows the active decoded alert status after forwarding to the first, second, and third enabled station, and after forwarding to all stations once (using the **Forward Alert Once to All Stations** button for forwarding to all stations simultaneously). This screen also shows the **Enable Reforward** buttons which can be pressed to once again enable the Forward Alert button per station (or for all stations).

FORWARDED ALERTS

Forwarded Alerts contain the same detailed alert information about Forwarded Alerts as previously discussed in the Alert Events section. They are organized alike, without the options for the Forwarding Action table, Play audio alarm, and the Event Storage Access Table.

The **Forwarded Alerts** screen displays the status of all forwarded alerts and contains the following sections:

- Currently Active Forwarded Alerts
- Expired Forwarded Alerts

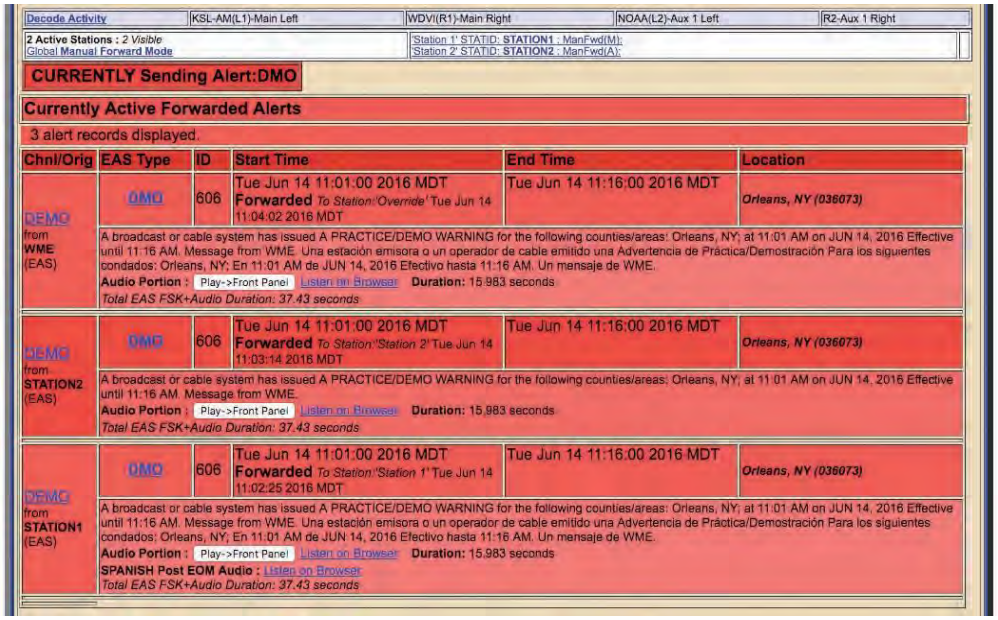
Users may perform the following actions from this screen:

- View Decode Activity Table
- View Forwarding Mode Table
- Review expired Forwarded EAS alerts
- Display, save, and print EAS message logs

Forwarded Alerts: MultiStation Mode

The **Forwarded Alerts** screen indicates which alerts have been forwarded to MultiStation mode enabled stations. They display the station ID in the Event Status Table for each forwarded alert. The bottom two DMO alerts below show that one Demo alert has been forwarded sequentially to two different enabled stations.

This screen shot also shows the active Forwarded Alerts display after the same decoded alert was forwarded to all stations using the **Forward Alert Once to All Stations** button (top DMO alert). It replaces the two active alerts forwarded earlier to the individual stations. The active alerts for the two stations are updated by this new forwarded alert and thus have expired.



ORIGINATED/FORWARDED ALERTS

The **Originated/Forwarded Alerts** screen displays the status of all alerts "sent" from the EAS device. Three sections display the following:

- Scheduled Originated Alerts
- Currently Active Originated/Forwarded Alerts
- Expired Originated/Forwarded Alerts.

Users may perform the following actions from this screen:

- Review expired Originated and Forwarded EAS alerts
- Display, save, and print EAS message logs

Scheduled Originated Alerts

This section lists scheduled alerts. Typically, it is populated with the next Required Weekly Test when Automatic Random Required Weekly Test Generation is turned on (see Chapter 5 - Station > Main).

Currently Active Originated/Forwarded Alerts

This section lists originated and forwarded currently active alerts.

Expired Alert View

As with the other event status views, you may choose View Expired Alerts, View Expired Alerts Pending Deletion, or View Deleted Expired Alerts. (See the **Incoming/ Decoded Alerts section** for more information about the options in this section.)

Expired Originated/Forwarded Alerts

This section displays the total number of expired and currently active originated and forwarded alerts, and offers the same expired alert event viewer as the other event viewers.

The **Date Range** field sets a date range to display alerts.

ORIGINATED ALERTS

The **Originated Alerts** screen displays the status of all originated alerts "sent" from the EAS device. Three sections display the following:

- Scheduled Originated Alerts
- Currently Active Originated Alerts
- Expired Originated Alerts

Users may perform the following actions from this screen:

- Review expired Originated EAS alerts
- Display, save, and print EAS message logs

This screen operates in the same way as other **Alert Events** screens but only displays Originated Alerts.

ALL ALERTS

The **All Alerts** screen is typically used to view or print all activity for a selected date range. This screen displays the following sections:

- Scheduled Alerts
- Currently Active Alerts
- Expired Alerts

Users may perform the following actions from this screen:

- Review all expired EAS alerts
- Display, save, and print EAS message logs

This screen functions in the same way as other Alert Events screens.

Scheduled Alerts

This section lists scheduled alerts.

Currently Active Alerts

This section lists all currently active alerts.

Expired Alert View

As with the other event status views, you may choose to view Expired Alerts, Expired Alerts Pending Deletion, or Deleted Expired Alerts.

Expired Alerts

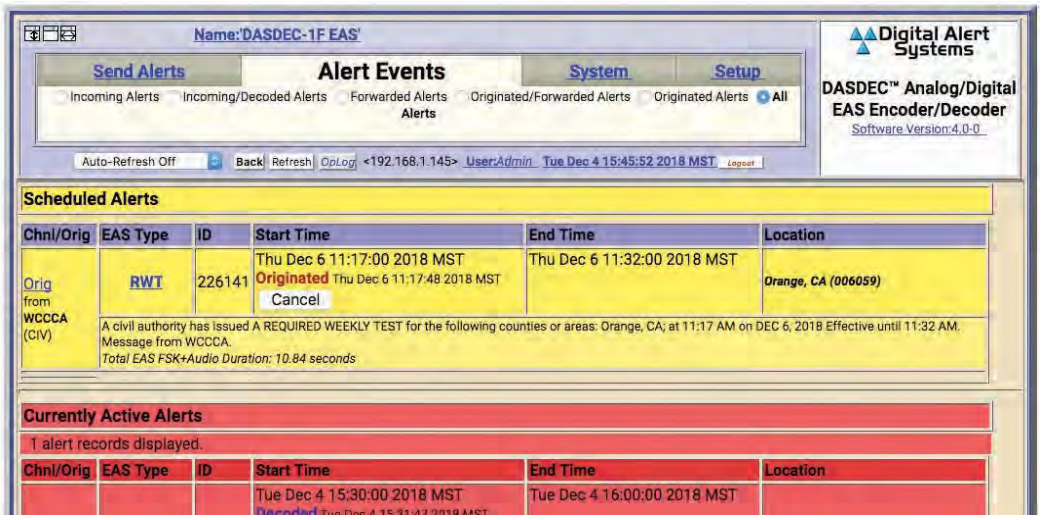
This section lists all EAS device expired alerts. Decoded, Forwarded and Originated (labeled Encoded) alerts are clearly labeled in order to distinguish between them.

Use the **Date Range** field to set a date range to display alerts.

BACKING UP EAS EVENT LOGS

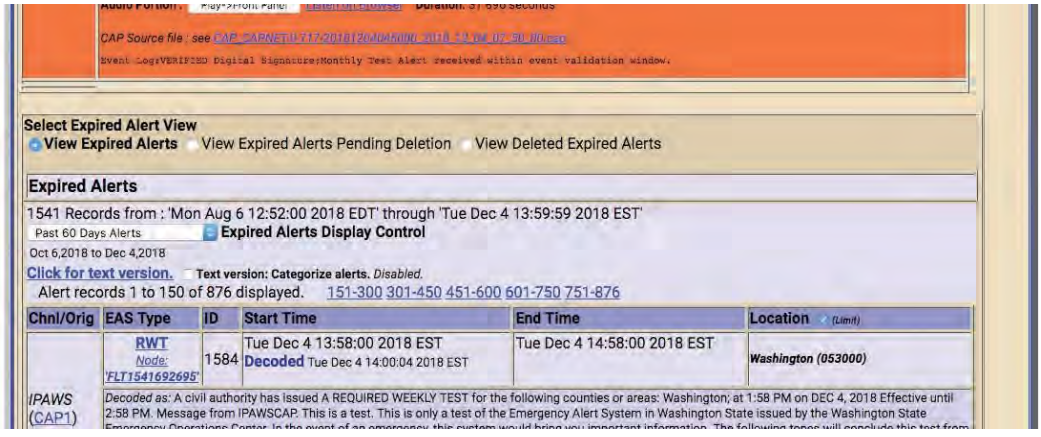
The following provides step-by-step instructions on how to back-up EAS event logs. On those occasions when manually backing-up EAS events is desirable, these steps will assist in exporting the selected logs to a local computer.

1. Log into the DASDEC/One-Net.
2. Go to **Alert Events**



Alert Events Screen

3. Depending the types of logs desired use the radio button to select one of the following:
   - Incoming / Decoded Alerts
   - Forwarded Alerts
   - Originated / Forwarded Alerts *(This is the typical selection for FCC logging purposes)*
   - Originated Alerts
   - All Alerts
4. Scroll down and find **Select Expired Alert View** and make sure the radio button **View Expired Alerts** is selected



Select Expired Alert View Section of Alert Events Screen

5. The blue area reflects the EAS logs that have been processed within the above selections.

Note
Establishing an EAS Event Report by EMail is the preferred method of exporting EAS event logs. The EMail method sends regular (weekly/monthly) and automated e-mail messages to the configured address(es). These e-mails may be used for FCC filings.

6. The total number of records is shown (above the '**Expired Alerts Display Control**' pull-down) along with the date range. These EAS records are sorted from earliest (at top of list) to latest dates.

Select Expired Alert View Section of Alert Events Screen

7. Use the **Expired Alerts Display Control** pull-down menu to further refine the records displayed.

8. Once the desired list is displayed, clicking the **Click for text version** hyperlink will produce a text-only web-page representation of the selected data.
    - Standard web-page print functions will allow these logs to be printed.

Text Version of EAS Event Logs

9. OPTIONAL: Many web browsers also include a 'Save Page As...' option in the File menu. Use this feature to download the selected EAS log data to your local computer.

Chapter 7: Send Alerts Tab

The **Send Alerts** tab is for originating different types of EAS alert messages. Only an EAS device configured with a valid Encoder license key will display the **Send Alerts** tab. Within this tab, there are up to three radio buttons.

Radio Button	Description
General Alerts	Originate (create and send) general EAS alert messages. Store and recall EAS message templates. **Requires a valid Encoder license key.**
One-Button Alert	Send Required Weekly Test. Provides hyperlinks to test setup screens. **Requires a valid Encoder license key**.
Custom Message	Originate custom EAS (CEM, ADR, and CAE) and non-EAS alert messages. **Requires a valid Encoder and Custom Messaging license keys.**

Use the **Send Alerts** screens to originate EAS alerts (when an EAS alert is first issued from an EAS encoder/decoder platform). EAS alert encoding is when the digital codes and alert audio tones and message defined by the EAS protocol are assembled and played over a broadcast medium for which EAS decoders might be listening. EAS alerts can be constructed and issued from these web interface screens. This differs from forwarding - when a decoded EAS alert is re-encoded and relayed.

Due to the need for immediate action during origination, Send EAS pages do NOT have any **Accept Changes** buttons. Changes to check boxes, pull-down menus, radio buttons, and action buttons are immediate.

Before originating any alert messages, make sure the Available FIPS and EAS codes have been configured within the **Setup > Alert Agent™ > FIPS Groups** and **EAS Code Groups** screens. The **Configured Available Encoder FIPS Locations** and **Configured Available Encoder EAS Codes** establish which codes are available for origination.

An EAS alert comprises a specific set of data values for encoding as Frequency Shift Keyed (FSK) digital audio data into an audio header - creating the characteristic EAS “squawk” sound that is repeated three times at the start of an EAS alert message. The data placed into an EAS message is:

- the origination code
- the EAS code type
- FIPS codes
- alert duration
- start time
- station ID

A decoded EAS header shows these values following a standard 4 letter sequence ZCZC.

Example: a 15-minute Required Monthly Test for Genesee and Orleans, NY starting on June 14 at 5:18PM from a station named WME would be encoded to or decoded as:

ZCZC-EAS-RMT-036037-036073+0015-1662318-WME.

This information can be interpreted by an EAS decoder into a human readable form, referred to as the "Standard Translation." The Standard Translation of the above alert string is:

> **A BROADCASTER has issued A REQUIRED MONTHLY TEST for the following counties or areas: Genesee; Orleans, NY; at 5:18 PM on JUN 14, 2016 Effective until 5:33 PM. Message from WME.**

The text translation is used for video and sign displays driven from the EAS device when an alert is originated or when a decoded alert is forwarded. The translation is also prominent in the EAS device event status displays and the operation log. All interfaces that originate and forward the alert display the translation.

A valid Plus Package license key provides options to customize the alert translation. Custom translation allows video displays driven by the EAS device to better describe an alert and provide more details than what is actually transmitted within the EAS protocol. The custom translation only affects the video displays. Unless TDX is used, these added text details are not sent out within the encoded EAS alert audio. A translation can be set to substitute a user-written string for the ORIG code and well as to prepend or append text to the standard translation or even fully substitute the translation for custom text.

Note
Some browsers will not accept the text field change until the mouse is clicked outside of the field entry box. Other browsers simply will accept the change when the Enter key is touched. Make sure to click outside the text field to insure text entry.

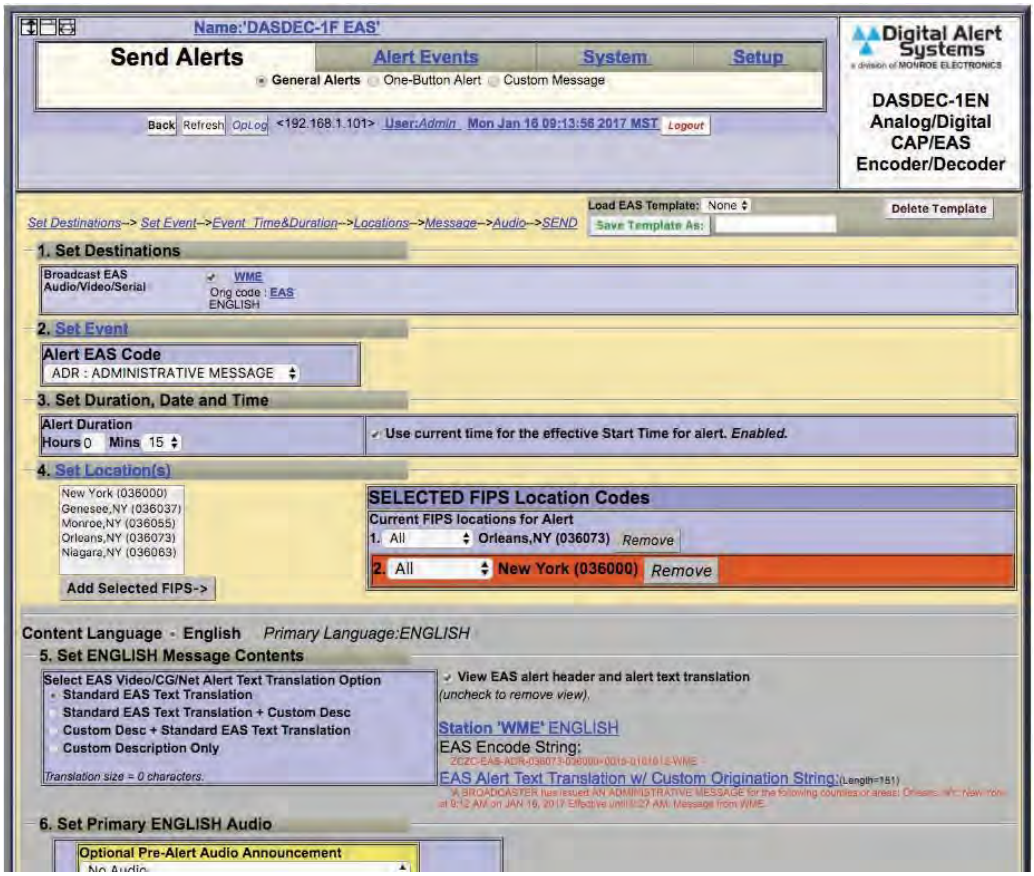
GENERAL ALERTS

The **General Alert** web interface screen provides an easy-to-use interface for setting the EAS data elements.

To make and send an EAS alert, review and set items on the **General Alert** page corresponding to the described EAS protocol and to the generation of local video displayed text information.

- Station ID
- EAS alert code
- Alert duration
- Starting time (effective time)
- FIPS Location Code(s)
- Message contents
- Pre-alert audio announcement (optional)
- Alert audio message (if any)
- Post-alert audio announcement (optional)
- Optional text translation modifications (required valid Plus Package license key)

The General Alerts screen is composed of seven numbered sections along with several useful hyperlinks, an EAS Template Management (save/load/delete section), and an alert action table. This screen has been updated to include the addition of EAS templates.



General Alerts Screen

Note
The screen captures within this chapter may look different based on the licensed options on your system.

Template Management

Message templates may be saved, recalled, and deleted using the following controls:

Load EAS Template

This pull-down menu enables users quick and easy access to pre-configured (or saved) EAS templates. A saved EAS Template will recall all configuration settings saved within the gray message composition area of this interface. Click this pull-down menu once to view the available options, then select/click the desired option.

Loaded EAS Templates can be modified prior to being sent. Recall the saved template, make the desired changes, and send the Alert.

NOTE
Selecting ***None*** from the **Load EAS Template** pull-down menu will clear all the text fields and reset all the controls to their default configuration settings.

Delete Template Button

The process of deleting EAS Templates is a three step process. First, load the desired template from the **Load Custom MSG Template** pull-down menu. Second, click the Delete Template button next to the pull-down menu. This will change the screen to a confirmation page where the user may perform the third and final step - choosing to continue to delete the template or cancel the delete process. To delete the template, click the **Yes, delete template** button and return to the General Alerts screen. Click the **No, cancel** button to abort the deletion process and return to the Custom Messaging Pro screen.

Save Template As:
EAS templates may be saved for later recall. Once the user has composed the desired message – including destinations, Alert EAS Code, duration, locations, language/message contents, and alert audio content – type a name for the EAS template into the text box adjacent to this button and click the **Save Template As:** button. The template will be saved and available in the **Load Custom MSG Template:** pull-down menu.

Set Destinations

These settings are only displayed on devices with a valid EAS-NET™ license key. The frame below the Set Destinations heading displays Station ID, Origination Code, Alert Language settings, and a check box that enables audio, video, and triggering serial communication for that station. The **Station ID** value is taken from the **Origination EAS Station ID** setting found within the Origination Settings of the **Setup > Station > Main** screen. The **Origination (ORG) Code** and **Alert Language** (Primary and Extended) settings are also found in the same screen. These settings will generally not need to be changed. If the Station ID, Origination Code, or Alert Language needs to be changed, the **Station ID** and **Orig Code** labels are hyperlinks to the above mentioned screen. Edit as needed and then use the Back button to return to the Send Alerts > General Alerts screen.

Note
Only specially configured EAS devices allow origination of National Alerts – Emergency Action Notification and National Periotic Test (EAN & NPT).

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.

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 under an hour to be set in 15 minute increments. Alerts of an hour or more are set in 30 minute increments. The EAS device interface enforces this FCC compliance.

Use current time for the effective Start Time for alert
When checked, the EAS alert message will contain the current date and time (month, day, and year followed by the current time). Users can manually set the effective (starting) date and time for the alert by unchecking this box and manually entering the desired information.

Set Location(s)

An EAS alert must be issued for specific locations. Until FIPS location codes are entered, the EAS device will not display a **Send Alert** button. Instead, a message box will show on the right side of the screen stating, ****Need to Add FIPS Codes****. Two additional red message boxes will appear (one in the Set [Content Language] Message Contents section and the other in the Send Alert section) stating **Alert NOT Ready to send::Specify FIPS Codes**.

General Alerts – Set Location(s) Section

To set the FIPS location(s) for the alert code, select from the list of **Available FIPS Code**. The codes shown are the ones that were added on the **Setup > Alert Agent™ > FIPS Groups** screen. *(To correct the list, click on **Set Location(s)** hyperlink. Add FIPS codes to the Configured Available Encoder FIPS Location list. Use the Back button to return to the Send Alerts > General Alerts screen to continue constructing the alert.)*

For each location, select one or more FIPS, and click **Add Selected FIPS->** button. Up to 31 FIPS location codes may be added using the FIPS selection table.

As you build the list of current FIPS locations for the alert, locations will display on the right in the **SELECTED FIPS Location Codes** frame. The sub-region of the FIPS location can be edited for every chosen location. If a different sub-region is desired, select one of the choices presented in the pull-down menu displayed to the left of the FIPS code.

If a FIPS location needs to be removed, click the corresponding **Remove** button.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but not very common.

After selecting the FIPS location(s), the “Alert NOT Ready...” message changes to a **Send Alert** button. The alert can be sent immediately if no audio message or language settings are needed. However, often the alert should have Pre-Alert Audio Announcement or an Alert Audio Message file.

Content Language

These radio buttons dictate the language-related settings for Message Contents and Audio within this gray’d section. When using both Primary and Extended languages, these radio buttons allow the user to select individual configuration settings for each language.

English and Spanish languages are standard within each EAS device. Users can choose a Primary Alert Language and one or more Extended Alert Language from the Setup > Station > Main screen (use the Station … hyperlink under the View EAS alert header and alert text translation check box for quick access). These settings will encode a primary and extended languages into the EAS alert message. By selecting the same language for both the Primary and Extended Alert Language setting, only one language will be enclosed in the EAS alert message. Selecting two different languages will enable both languages (Primary followed by the Extended Alert Language).

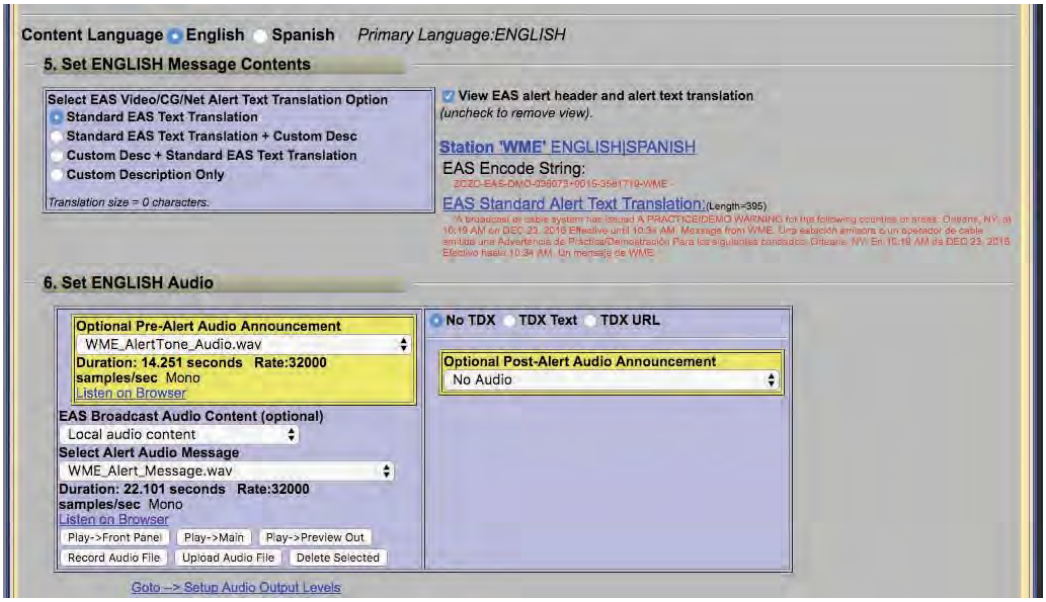
Note
Additional languages (beyond English and Spanish) are available with a valid OmniLingual™ license key.

Set [Content Language] Message Contents
A valid Plus Package and EAS NET™ license keys will display the **Select EAS Video/ CG/Net Alert Text Translation Option** frame. Use radio buttons to select one of four combinations of Standard Translation and Custom Translation. For selections with custom translations, a text entry field displays where the text can be entered is displayed.

The alert text translation is used for the local video details, serial and net-attached CGs, and EAS NET™ devices. This alert text can be augmented or replaced with the provided options. Options are provided to add a custom message in front of, after, or completely replace the standard translation. The default is the Standard Text Translation selection. Custom descriptions are outside the scope of EAS alert messages and will not be contained within the EAS alert message. They will be transmitted to local video output details page, serial and network-attached CG's, and EAS NET™ devices. The available radio button selections are:

- Standard Text Translation
- Standard Text Translation + Custom Description
- Custom Description + Standard Text Translation
- Custom Description Only

View EAS Alert header and alert text translation
Enable this check box to view the alert header EAS Encode String and the EAS Alert Test Translation for the currently constructed alert. When enabled, the actual EAS encode string (or EAS header) is displayed. Below this is the current translation. The label above the translation will state if the translation is the basic standard translation or one with a Custom Origination String (see Origination Settings within the **Setup > Station > Main** screen). Both these labels are hyperlinks to this setup screen allowing you to make changes as needed.



General Alerts – Language & Audio Selection Section

Set [Content Language] Audio

Use this frame to attach pre-recorded audio voice messages to the EAS alert. Each interface permits selection of no audio file or of an audio WAV file that has been recorded or uploaded onto the EAS device. Add audio files to these lists list in two ways.

- Upload WAV files using the **Upload Audio File** button
- Directly record audio files into the EAS device by using the **Record Audio File** button

Optional Pre-Alert Audio Announcement

Use the pull-down menu to select a pre-recorded audio file to precede the actual alert announcement.

When an audio file is selected, its duration appears along with its sample rate. A **Listen on Browser** hyperlink is available to listen to the audio file within the web interface.

If the audio file does not match the configured **Audio Output Sample Rate** found in the **Setup > Audio > Audio Output Levels/Tests** screen, the text "NOTE:Resample to output rate (*configured output sample rate*) to avoid play out slowdown!" and a **Resample File** button will appear. This process will maintain a constant sample rate for all audio output files and prevent slow-downs when playing differing audio files.

EAS Broadcast Audio Content (optional)

This setting enables users to select where audio content is sourced. This pull-down has the following three options:

- **Local audio content** – Allows users to select and play locally stored WAV files. When this option is selected, a **Select Alert Audio Message** pull-down menu will be present below. Users can choose **No Audio** to play during the alert or a pre-recorded audio message from the list in the drop-down menu.

The audio file duration (in seconds) and sample rate is displayed below the selection. There might also be a **Resample File** button – as described above.

Attention

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

If the TDX option is licensed and enabled (**Setup > Station > Global Options**), then to the right of the alert audio selection are three radio buttons: No TDX; TDX Text; TDX URL. These control the addition of TDX alert details.

Audio 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**)

Warning
Prior to clicking any of playout options, make sure the audio will not interrupt the stations on-air audio. These options are intended to allow users to preview the selected audio file.

Audio Management Options:

Included in this section are three buttons to assist with managing audio files within the EAS device:

- **Record Audio File** – clicking this button displays a new **Record Alert Audio File** screen. This screen enables users to record audio files with a microphone or from the line input. The active input source is noted at the end of the hyperlink in the middle of this screen. In the example below, the input source **Microphone** is noted. Click the hyperlink to be directed to the **Select audio device for alert audio file recording:** section of the **Setup > Audio > Encoder Audio** to change the input source.

  Enter a unique audio file name in the **Audio Filename** text field. (A unique file name is one not already used in the provided **Select Alert Audio Message** selection pull-down. If you use an existing name, the original file by that name will be overwritten.)

  The duration of this file must be under two minutes (119 seconds) as the EAS device automatically cuts off recording at 2 minutes. Click the **Start Record** button and speak. A new screen will appear with a running countdown (from 2:00) clock. Click the **Stop Recording** button when finished. The web interface will return to the General Alerts sub-tab.

- **Upload Audio File** – An **Upload Audio .WAV file** interface appears when you click this button. The user is presented with the following buttons:
  - **Choose File** – click this button to choose a file from the users' local workstation
  - **Upload .WAV file** – once a .WAV file has been chosen, click this button to upload the file
  - **Cancel** – click this button to cancel the upload process
- **Delete Selected** – available when an audio file is selected and will immediately delete the selected file.

Note
To change audio output levels, use the text link Goto --> **Setup Audio Output Levels** hyperlink to the **Setup > Audio > Audio Output Levels/ Tests** screen. Return using the **Back** button.

- **Remote URI audio content** – Uniform Resource Identifier defines a network accessible audio file/location to play content from. This option is utilized to access remote content from a centralized, internet location.

  Two pull-down menus and a text entry box will appear once this option is selected:

  - **Audio Type**:
    - › **IPAWS MP3 audio file** (audio/x-ipaws-audio-mp3)
    - › **IPAWS MP3 streaming audio file** (audio/x-ipaws-streaming-audio-mp3)
    - › **WAV audio** (audio/wav)
    - › **MP3 audio** (audio/mpeg3)
  - **URI Type**:
    - › **http://** - HyperText Transfer Protocol
    - › **https://** - HyperText Transfer Protocol Secure
  - **URI Address Text Entry Field** – enter the URI address for the desired audio file
  - **Auto-download upon send** check box – will download the desired audio file for logging purposes.
- **Text to Speech from text content** – utilizes the internal text-to-speech engine. If there are licensed Premium TTS voices they will be listed here. Select the desired voice. Otherwise the generic TTS voice will be used.

There are three available buttons and a hyperlink available:

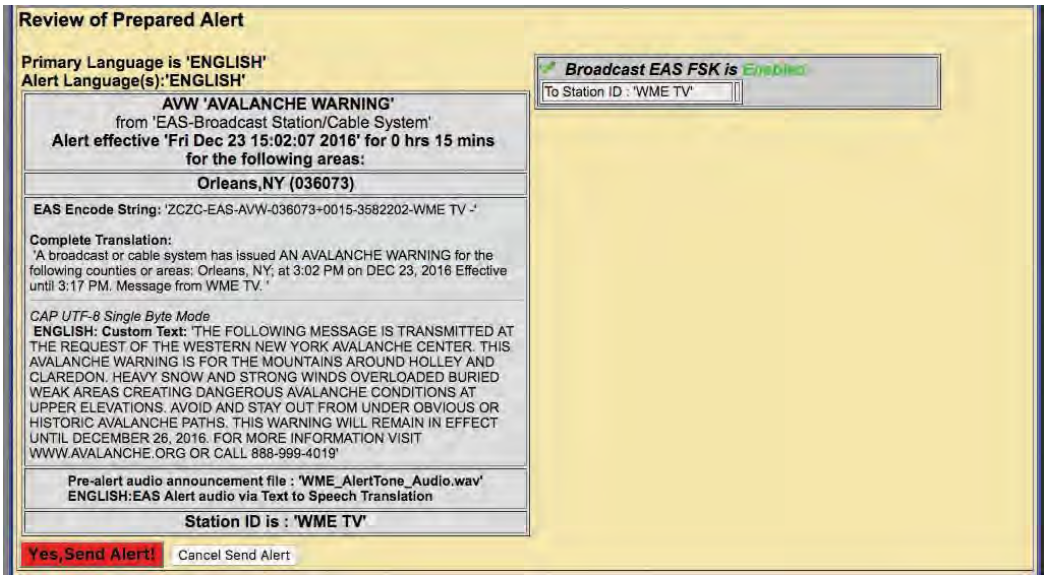
- **Make Draft TTS Audio File** – click this button to create an audio file based on the configured alert options. The audio file will be stored on the EAS device and can be previewed using the following playout options. A new TTS file will need to be created each time any of the alert settings are modified.
- **Play->Front Panel** – plays the audio file out the internal front panel speaker
- **Play->Preview Out** – plays the audio file out the configured Audio Preview Devices (see **Setup > Audio > Audio Output Levels/Tests / Direct Audio Output Levels and Tests**)
- **Play on browser** hyperlink– will play the selected audio file within the web-browser

Optional Post-Alert Audio Announcement
Similar to the pre-alert announcement. Allows an audio message to be played after the end of an EAS alert.

Within the **Set [Content Language] Audio** section of this interface are buttons to **Record Audio File** and **Upload Audio File**.

Send EAS Alert/Alert NOT Ready to Send

When the alert is ready, the **Send Alert** button will appear. Click this button to send the alert. The EAS device will show a **Review of Prepared Alert** screen (confirmation) with a consolidated view of the alert details. If the alert is correct, click the **Yes, Send Alert!** button. If incorrect, click the **Cancel Send Alert** button. If the alert send is canceled, the EAS device will go back to the General Alerts screen. Edit the alert information before sending the alert again.



Review of Prepared Alert Screen

When you've clicked the **Yes, Send Alert!** button, the alert will be played out of the selected EAS device's audio output ports. The originated alert audio ports are selected from the **Setup > Audio > Encoder Audio** screen.

During the origination time, the front panel red LED will be lit, and the alert's audio will play from the built-in internal speaker. For the duration of the issued alert, the unit will periodically crawl the alert text across the front panel LCD. The LCD text for the alert will be preceded by the letter "O", indicating an originated alert. You can view details of the alert on the screen **Alert Events > Originated/Forwarded Alert** or **Originated Alert** screens.

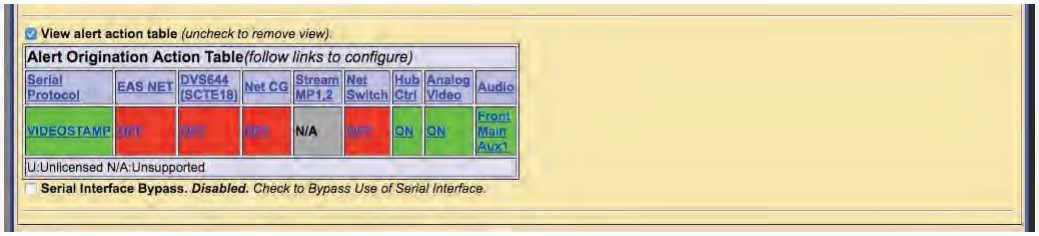
During active alert sending, a red notice displays in the Send Alert interface. After the alert is sent, click the **Return** or **Refresh** button to return to the main Send Alerts screen.

Reset

The entire alert setup process can be restarted by clicking the **Reset** button – to the right of the red **Send Alert** button.

View Alert Action Table

When the alert action table check box is checked, you can see the Alert Origination Action Table. It contains active hyperlinks displaying the current status of the various peripheral interfaces that can be activated by an alert. The table displays which peripheral interfaces are available and which are enabled. The active links point to the associated page under **Setup**. Click the interface name to follow the hyperlink and change any specific peripheral used during alert origination.



Send Alert and View Alert Action Table Sections

Serial Interface Bypass

If a serial protocol has been selected, a Serial Interface Bypass check box is displayed. When the Serial Interface Bypass check box is checked, the currently selected serial protocol will not be used during the alert origination. A message in the Origination Table above changes to say the Serial Protocol is bypassed.

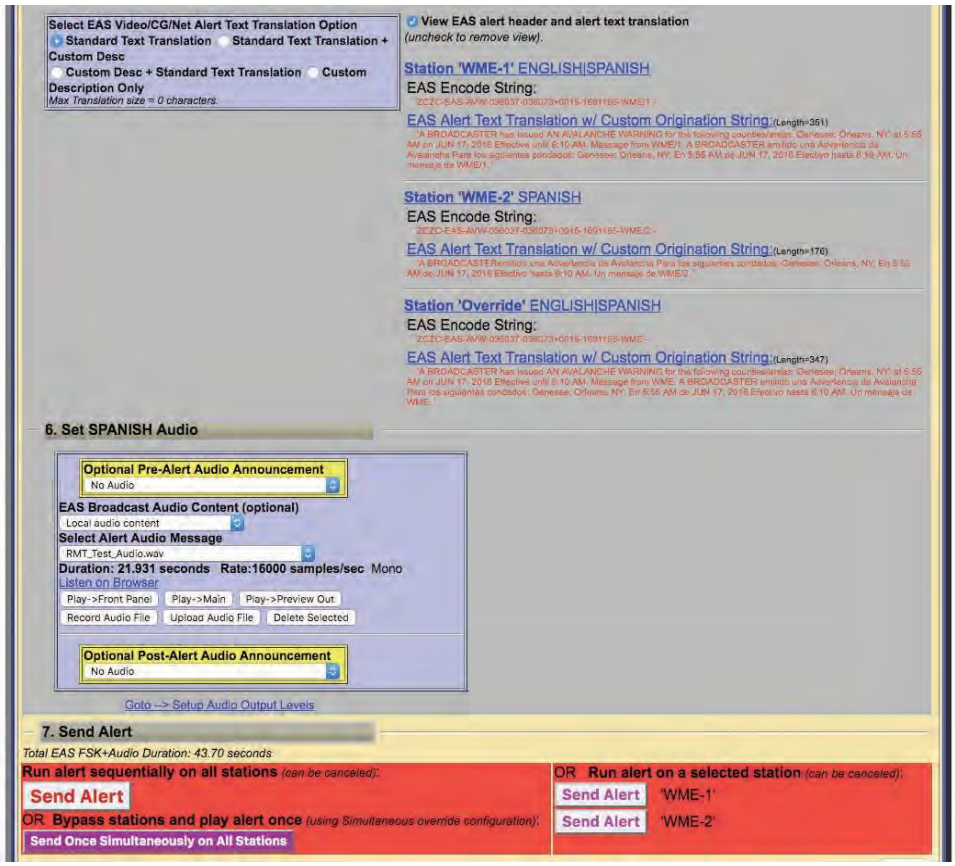
General EAS: MultiStation mode

When in MultiStation mode and at least one station is enabled, the General Alerts page displays added options to support alert origination to individual stations.

MultiStation operation allows EAS alerts to be originated using a specific subset of the hardware in order to play on a specific downstream station. In this way, up to five collocated broadcast stations or channels can use one EAS device for EAS alert origination.

The EAS protocol field for the Station ID can be programmed differently for each station as well. (see **Setup > Station > MultiStation**) This way the actual EAS alert header FSK audio (*which embeds the Station ID*) truly represents the station of alert origin.

Station configuration options can be found on the **Setup > Station >** (Station Sub-Tab).



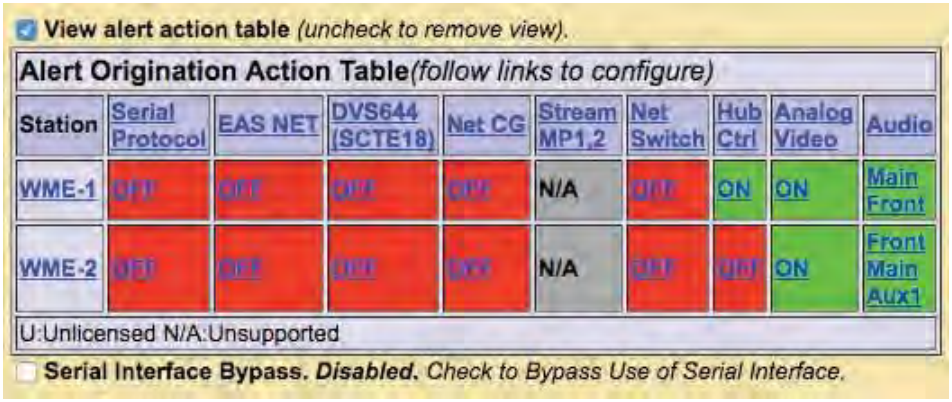
Send Alerts > General Alerts with MultiStation options

There are different Send EAS Alert buttons provided for station support. They allow you to run the alert on each station in sequence, run on individual stations, and to run the alert once to all stations at the same time using the Main station configuration. As in non-MultiStation mode, when any of the Send Alert buttons are pressed, the actual send must be confirmed on the confirmation review page.

Another difference in MultiStation mode version of the **Send Alert > General Alerts** screen is the alert text translation display. The standard translation for each station is shown. Since each station can independently set the Station ID, the Origination code, and Origination code custom translation text – the translation text varies per station. The display shows exactly the text that is sent per station to video character generators.

All other interface components of the **Send Alert > General Alerts** screen are the same as in the non-MultiStation mode. Keep in mind that the settings on this screen apply to the alert *(or alerts if sent to each station sequentially*) at the time the **Send Alert** button is pressed.

Finally, the **Alert Origination Action** table is expanded in MultiStation mode to show the actions for each configured station. This table presents a quick view of the station by station configuration.

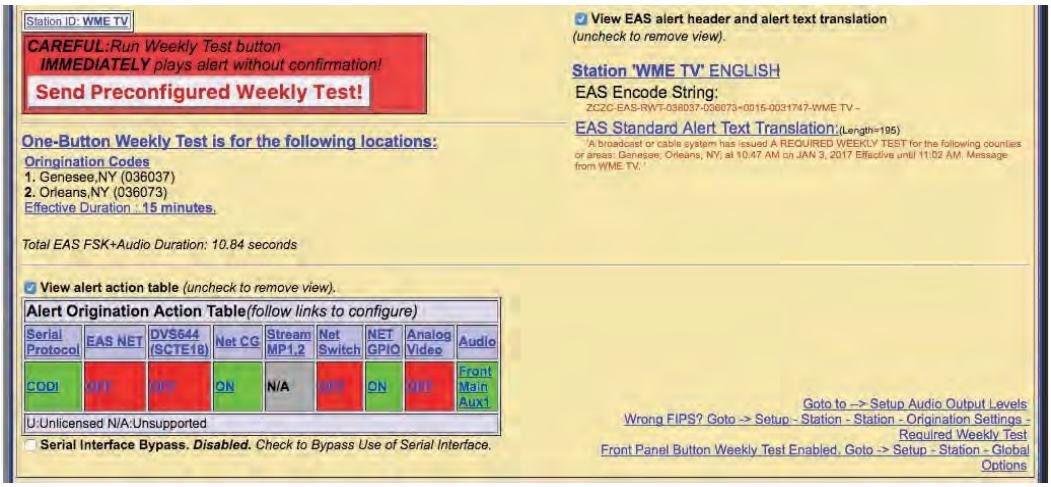


Alert Action Table – MultiStation Mode

If all of stations are disabled (*from the **Setup > Station > (Station Sub-Tabs)*** the alert origination reverts to using the Simultaneous Station Override configuration.

ONE-BUTTON ALERT

The EAS device supports configuration of a static set of Required Weekly Test parameters on the **Setup > Station > Main** screen. Once configured, the **Send Alerts > One-Button Alert** screen presents a single button (**Send Preconfigured Weekly Test!**) for issuing the weekly test alert. The Front Panel button will also trigger the test configured from this screen. This feature simplifies sending a weekly test alert.



One-Button Alert Screen

There are three ways to send reconfigured one button test alerts. In both cases, the alert is sent immediately with the current clock time as the effective alert start time. No confirmation dialog is presented.

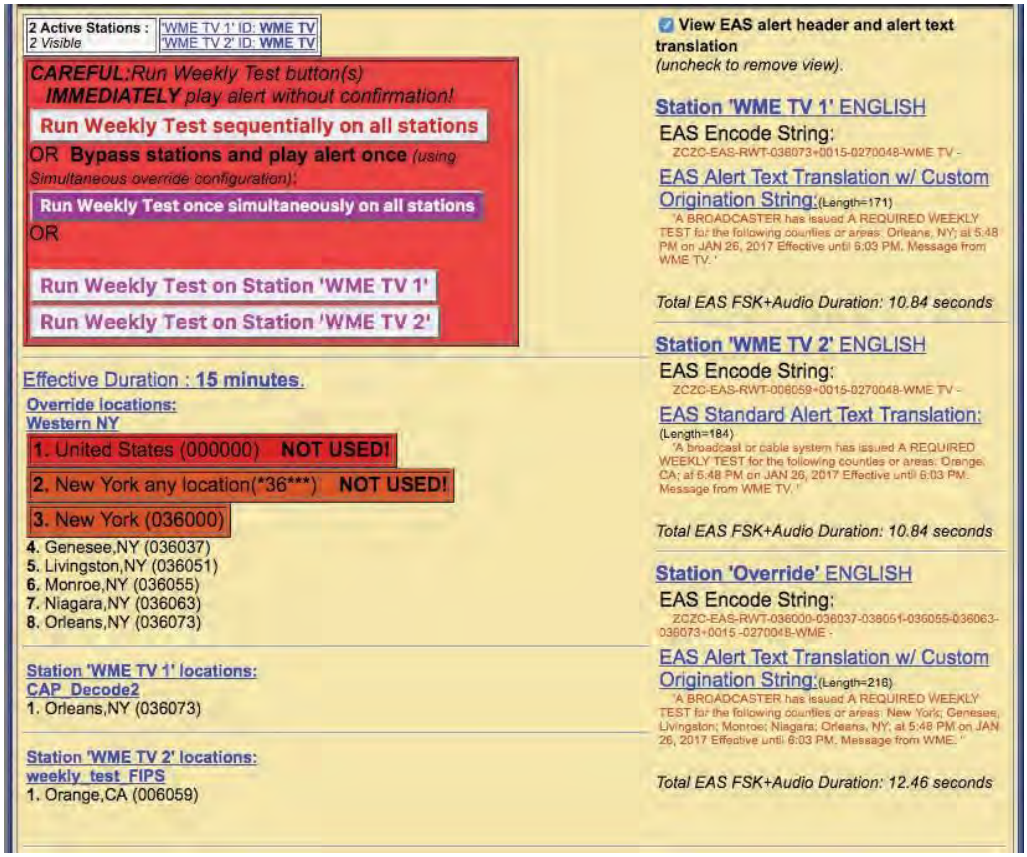
1. Click the button **Send Preconfigured Weekly Test!** on the One-Button Alert screen
2. Press the front panel button once, wait a second, press it again
3. Initiating a contact closure on a configured GPIO Input

This screen contains numerous hyperlinks throughout to aide in making configuration changes if needed. Some of the more useful hyperlinks are found in the lower right corner of the screen: Audio Output Levels, FIPS codes, and Front Panel Button enable.

The **View alert header and alert translation** check box and the **Alert Origination Action** table operates the same as on the **General Alerts** screen.

One-Button Alert: MultiStation mode

When in MultiStation mode and at least one station is enabled, the One-Button Alert screen displays added options to support individual station origination. See the screen shot below.



One-Button Alert – MultiStation Mode

One-Button MultiStation operation allows EAS Required Weekly Tests to be originated using a specific subset of controlled hardware in order to play on a specific downstream station. In this way, up to five collocated broadcast stations or channels can use one unit for EAS Weekly Test origination.

Individual station configuration settings are located at **Setup > Station > (Station Sub-Tabs)** with **Simultaneous Station Override** sub-tab used for any un-configured station.

The screen shot demonstrates the different **Run Weekly Test** buttons provided for station support:

- **Run Weekly Test sequentially on all stations**
- **Run Weekly Test once simultaneously on all stations**
- **Run Weekly Test on Station *'insert station name'*** (one for each station)

As in non-MultiStation mode, when any of the **Run Weekly Test** buttons are pressed, the test is done immediately without confirmation.

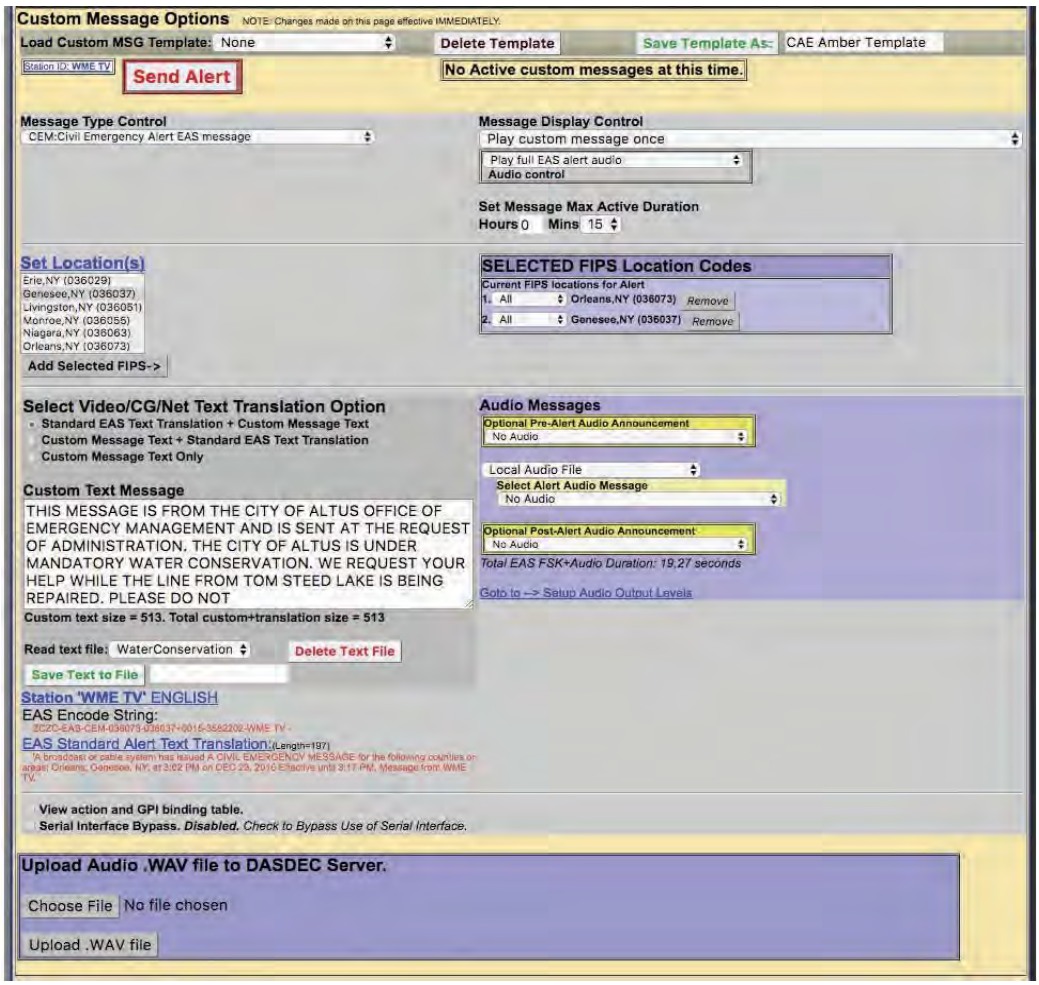
If all of the stations are disabled the alert origination reverts to using the settings configured within the Simultaneous Station Override sub-tab.

CUSTOM MESSAGE PRO

The EAS device supports a licensed feature called **Custom Messaging** for playing out Child Abduction Emergency (CAE), Civil Emergency Alert (CEM), and Administrative (ADR) EAS alert messages as well as non-EAS audio/video messages. Using Custom Messaging, the unit can be used to:

- broadcast custom text messages
- play audio messages multiple times
- use automatic text to speech conversion
- play Pre-Alert and Post-Alert audio files
- assign local audio files or use text-to-speech for Alert Audio messages
- create, save, recall, and delete custom message templates
- create, save, recall, and delete custom text message files
- upload audio (.wav) files
- generate FSK headers tones for EAS messages
- assign custom messages to GPI inputs

Custom Messaging Pro can originate both EAS and non-EAS messages, which means the EAS device can be used as a custom warning or information system as well as an EAS message originator.



Custom Message Pro Screen

Note
Custom Messaging is not available when the MultiStation feature is active with enabled stations.

The Custom Messaging Pro screen is divided into three functional sections. At the top of the interface screen is where Custom Message templates are loaded, deleted, saved, and sent (Template Management). The center (gray) section is used to compose the message and includes the Message Type Control, Message Display Control, Message Duration, Custom Text Message, and Audio Messages selections. The bottom most section contains the Upload Audio .WAV file controls.

Template Management

This first section of this screen allows for quick and easy access to stored message templates. The following controls are available:

Load Custom MSG Template:
This pull-down menu enables users quick and easy access to saved (or pre-configured) Custom Messages. A saved Custom Message will recall all saved configuration settings within the gray message composition area of this interface.

Load Custom MSG Template Pull-Down Menu

To load a Custom Message Template, click once on the pull-down menu and select the desired template by clicking on that menu item. The template will immediately populate the message composition section with the pre-configured (saved) settings.

Loaded Custom Message Templates can be sent as-is, or they can be modified just prior to being sent. For example, a Civil Emergency Alert (CEM) template may be stored advising the residents of six counties to boil water due to concerns of water contamination. A similar emergency may arise, however, this time it only affects three out of the six counties within the EAS devices' service area. Simply recall the original CEM, remove the unaffected counties, and send the CEM Alert.

Delete Template Button
The process of deleting Custom Message Templates is a three step process. First, load the desired template from the **Load Custom MSG Template** pull-down menu. Second, click the Delete Template button next to the pull-down menu. This will change the screen to a confirmation page where the user may perform the third and final step - choosing to continue to delete the template or cancel the delete process. To delete the template, click the **Yes, delete template** button and return to the Custom Messaging Pro screen. Click the **No, cancel** button to abort the deletion process and return to the Custom Messaging Pro screen.

Save Template As:
Custom Messages templates may be saved for later recall. All of the configuration settings found in the (gray) message composition area can be stored and easily recalled.

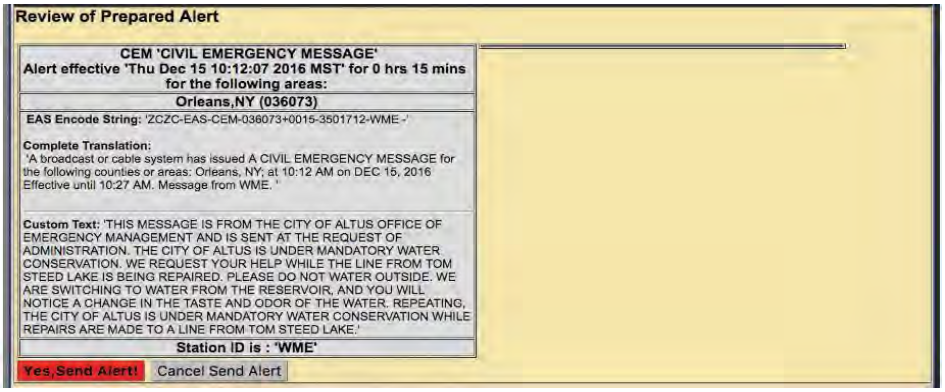
Once the user has composed the desired message – including Custom Text, Message Type, Display Controls, Custom Text, and audio settings – type a name for the Custom Message template into the text box adjacent to this button and click the **Save Template As:** button. The template will be saved and available in the **Load Custom MSG Template:** pull-down menu.

NOTE
Selecting ***None*** from the **Load Custom MSG Template** pull-down menu will clear all the text fields and reset all the controls to their default configuration settings.

Note
Use a descriptive and short template name. Avoid special characters such as; <, >, |, \, :, (,), &, ;, and quote marks – as well as wildcard such as ? and *.

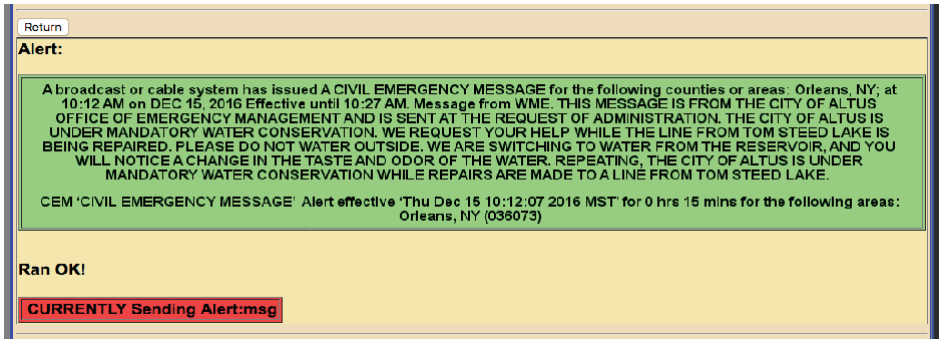
Send Custom Message/Send Alert Button

This white button with red text / border is used to initiate the origination of either a Custom Message or EAS Alert. The button will change depending on which type of message is configured to send. When sending a Custom Message, the button will read Send Custom Message and when sending a CEM, ADR, or CAE, it will read Send Alert. This is a quick and visual way to determine an EAS or non-EAS message is being sent.



Review of Prepared Alert Screen

Once a Custom Message or EAS Alert has been configured (see below to configure both EAS and non-EAS messages/alerts) or loaded, the user may click the Send Custom Message/Send Alert button. The interface will change to a review screen where the user can review the message details. The interface displays two options to the user: start the message or cancel the message. If for any reason the message is not configure properly, use the Cancel Send Message button, make the necessary changes and begin the send message/alert process again. Otherwise, click the Yes, Start Message! button to send the configured message/alert.



Confirmation Screen

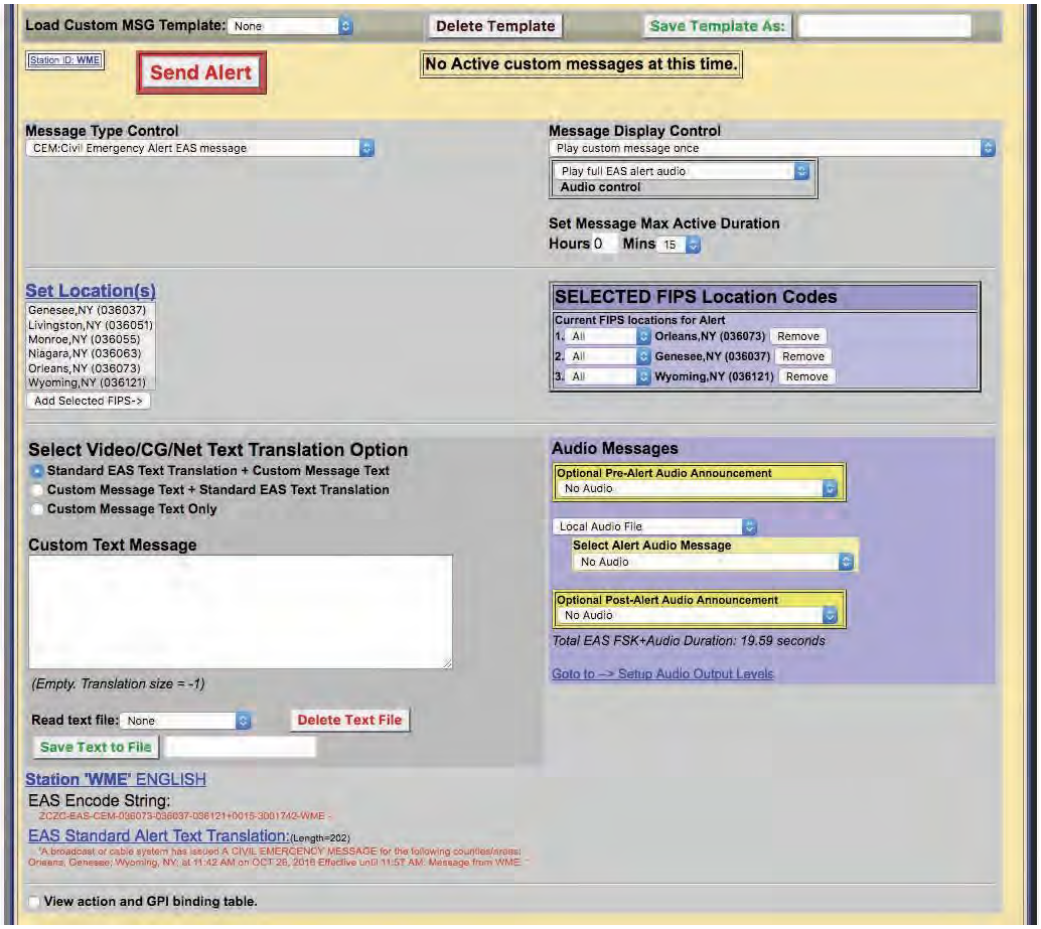
A confirmation screen will then appear showing the status of the active message/alert for a few seconds before returning to the main Custom Message screen.

Custom Message Screen with Active Message/Alert

The Custom Message interface shows the current status of the custom messaging operation. While a custom message is being broadcast, the interface will display the message play-out status along with a **STOP Active Message** button. This button can be pressed throughout the duration of the message/alert to force an early end to the message broadcast.

When a custom message is active, the **Alert Events > Originated/Forwarded Alerts** and **Originated Alerts** event status screens display the message as an active originated event. The display includes the same force **Stop Active Message** button.

Below the **Send Custom Message/Send Alert** button is a gray-background section for composing message/alerts. This section has numerous configuration settings. Several settings are universal to both Custom Messages and EAS Alerts. EAS Alerts have additional settings, such as FIPS codes and EAS Text Translation, are added to the interface when CEM, ADR, and CAE message types are selected. When composing EAS Alerts, the bottom of this section will display the EAS Encode String and the EAS Standard Alert Text Translation.



Custom Messaging Pro Screen – EAS Alert

Message Type Control

The interface allows selection of a message type, which can be a fully custom message or one of three EAS-specific alerts. This pull-down menu is used to select the type of custom message being sent. The menu contains the following four selections:

Message Type	Description
Non-EAS Custom Message	Custom messages that do not include EAS specific information – including FIPS location codes and the generation of FSK tones. These messages are usually intended for closed systems, such as corporate campuses and educational institutions to broadcast both audio and visual emergency alert information.
CEM: Civil Emergency Alert EAS Message	An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. For example, a CEM could be used to alert the public to a public water contamination issue and provide guidance to boil tap water or where to obtain clean water.
ADR: Administrative EAS Message	A non-emergency message that provides updated information about an event in progress, an event that has expired or concluded early, pre-event preparation or mitigation activities, post-event recovery operations, or other administrative matters pertaining to the Emergency Alert System. The ADR is to be used for all follow-up messages pertaining to an original warning.
CAE: Child Abduction Emergency (Amber Alert) EAS Message	An emergency message regarding a specific Child Abduction Emergency. Alerts usually contain a description of the child, the likely abductor, and specific information about the abductors vehicle. To avoid false alarms, the criteria for issuing an alert are rather strict. Each state's or province's AMBER alert plan sets its own criteria for activation. The U.S. Department of Justice issues the following "guidance", which most states are said to "adhere closely to" (in the U.S.): 1. Law enforcement must confirm that an abduction has taken place 2. The child must 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

Select the desired **Message Type** by clicking the menu once and selecting the desired type by clicking again one that selection.

NOTE

Many law enforcement agencies have replaced CAE #2 criterion with *'The child's whereabouts is unknown of is assumed to be at risk of serious injury or death'*.

Message Display Control
There are many options available for the playout of both video and audio content during the active alert duration (see **Set Message Max Active Duration** below). The five available options may be selected through this pull-down menu. These options are quite descriptive and are as follows:

- Play custom message once
- Repeat custom message playout for the defined max duration (or until stopped)
- Repeat custom message playout until stopped
- Repeat custom message playout for a specific duration (or until stopped)
- Repeat custom message playout for a fixed number of times (or until stopped)

Select the desired **Message Display Control** by clicking the menu once and selecting the desired type by clicking again one that selection.

The **Message Display Control** and **Audio Control** interfaces will change depending on the chosen selection. For example, when selecting **Repeat custom message playout for a fixed number of times**, the interface will automatically add a **Number of repetitions**: text entry box. These interface changes are self-explanatory.

Audio Control
Due to the tight relationship between video and audio, the **Audio Control** pull-down menu is located directly below the **Message Display Control** pull-down menu. This setting enables the user to select one of the following three options:

- Do not play any alert audio
- Play full EAS alert audio
- Play just alert voice audio message portion

It is important to understand what components are contained within the *'full EAS alert audio'*. The *'full EAS alert audio'* contains the header tones, attention signal, alert voice audio, and the End of Message (EOM) tones. All these components are required to send a valid EAS alert.

When originating an EAS message, the EAS device may use a pre-recorded Alert Audio Message file or utilize text-to-speech of the **Custom Text Message** for the *'alert voice audio'*.

Selecting any of the repeating options in the **Message Display Control** pull-down menu will change the options available within the **Audio Control** pull-down menu:

- Do not play any alert audio
- Play full EAS alert audio with every display repetition
- Play full EAS alert audio just during the first display
- Play full EAS alert audio once and alert voice audio message portion during repetitions
- Play just alert voice audio message portion with every display repetition
- Play just alert voice audio message portion during the first display

Link
Refer to the EAS Protocol section this manual for additional information about the structure of EAS messages.

Set Message Max Active Duration
Every message/alert contains an active duration. This time is useful for several reasons:

- Used to calculate the 'Effective until…' time displayed in an EAS alert
- When selecting Repeat custom message playout for the defined max duration, the message/alert will remain active in the EAS device for the defined duration

The **Message Max Active Duration** does not always mean the message/alert will be active within the EAS device for the entire configured duration. For example, a CEM alert is configured to inform the public of contaminated water and advise them to boil tap water for 24 hours. Setting the **Message Max Active Duration** to **24 Hours** and **0 Mins** will add 24 hours to the date and time the alert is sent and display that as the 'Effective until…' time within the EAS alert:

> 'A broadcast or cable system has issued A CIVIL EMERGENCY MESSAGE for the following counties or areas: Orleans; Genesee; Wyoming, NY; at 8:41 PM on OCT 26, 2016 Effective until 8:41 PM OCT 27, 2016. Message from WME.'

This CEM alert may only be broadcast once. In this case the alert is only active in the EAS device for the time of that broadcast.

Note
The FCC has defined the minimum EAS duration as 15 minutes. As such, the smallest duration available in this interface is 15 minutes.

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 and EAS alert message.

Set Location(s) Section - EAS Alert

Note
The EAS device does not sort Pre-Alert, Alert, or Post-Alert audio files separately. All audio files will be displayed in each of these pull-down menus.

To modify this list, follow the **Set Location(s)** hyperlink to the **Setup > Alert Agent™ > FIPS Groups** screen. At the bottom of this page is the **Configure Available FIPS for Encoder Alert Origination** section.

Returning to the Custom Messaging screen, configure the FIPS location codes by clicking the desired county/FIPS code and then click the **Add Selected FIPS->** button at the bottom of the list. Repeat this process until all the desired FIPS codes are listed in the purple **Current FIPS locations for Alert** list. Multiple FIPS codes can be added by holding either the Ctrl or Alt key while selecting. Only the FIPS codes in the purple area will be used in the origination of the EAS alert message. FIPS subdivisions may be configured for each FIPS code by using the pull-down menu next to each FIPS code. The **Remove** button adjacent to each FIPS code will remove that code from the **Current FIPS locations for Alert** list.

Notice the color coding of the state-wide code (New York in the above example) in orange. The state-wide code is colored orange in an effort to highlight the use of this FIPS code to the operator. Originating a state-wide alert is allowed, but not very common.

Select Video/CG/Net Text Translation Option *[EAS Specific Setting]*
The EAS device will send text information to either internal or external video devices. These radio buttons configure the information sent to those devices:

- Standard EAS Text Translation + Custom Message Text
- Custom Message Text + Standard EAS Text Translation
- Custom Message Text Only

Custom Text Message
This text entry field is used to augment a standard EAS alert message or provide text for a custom message. Information contained in this field will be sent to internal or external character generators for visual alerting. It may also be used for text-to-speech (TTS) generation within the EAS device.

Just below this text entry field is a count of the number of characters found within the Custom Text Message. The screen requires a refresh in order to provide an accurate count.

Custom text messages can be loaded, deleted, and saved – similar to Custom MSG Templates. The next three items discuss how to perform these functions.

Read text file:
Text files may be recalled by clicking this pull-down menu and selecting the desired file. Once a text file has been selected, the Custom Text Message field is cleared and populated with the selected file.

Delete Text File Button
To delete an existing text file, follow the process above to read the desired text file and click the **Delete Text File** button. The text file is immediately deleted without additional confirmation.

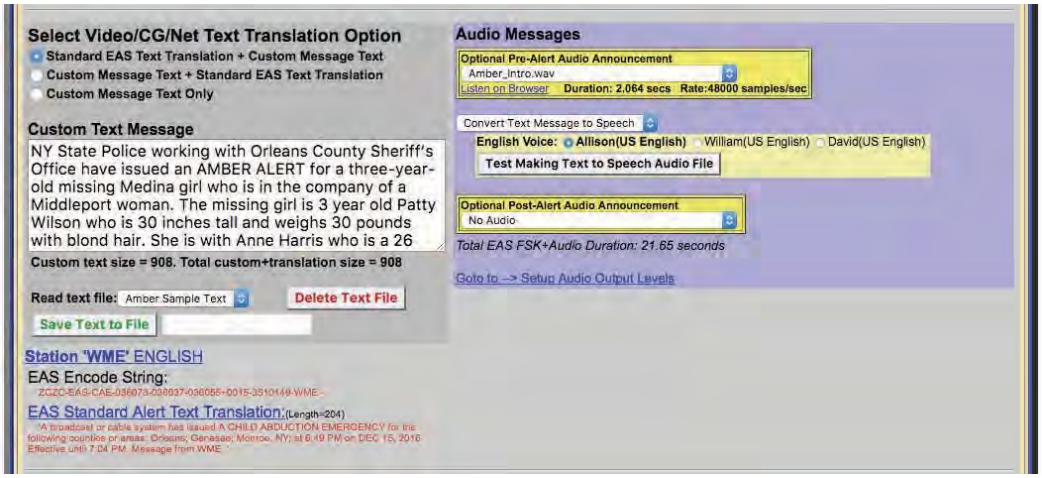
Save Text to File Button / Text Entry Field
Saving text files is a useful feature when wanting to quickly and reliably recall Custom Text Messages. In many instances it is easier to modify existing/recalled text than completely re-type it.

Type the custom text in the **Custom Text Message** field. Move down to the text field directly to the right of the **Save Text to File** button and enter a file name for this text file. Click the **Save Text to File** button and the text file with be saved. To double check the file is available to recall, click the **Read text file:** pull-down menu and make sure the new text file is in the list.

Audio Messages

There are three main pull-down settings within the purple Audio Messages sections of the interface. These settings determine what audio, if any, will be utilized during the Pre-Alert, Alert, and Post-Alert segments of the message/alert. Both the Pre-Alert and Post-Alert are optional settings and are not required during and EAS or Non-EAS message, but may also be useful in enhancing the total message/alert. For example, a pre-alert audio file might contain alert tones since they are not standard for non-EAS messages. Another example might utilize a personalized station ID audio file as pre-alert audio when sending an EAS message. These are just a few examples of how pre and post alert audio may be used. With valid premium Language Licenses, TTS may be generated for Alert Audio to streamline the creation of message/alerts.

Audio files may be uploaded to the EAS device via the **Upload Audio .WAV file** section at the bottom of this screen. (see below for more detailed information on loading audio .wav files)



Audio Messages Section (TTS Enabled)

Optional Pre-Alert Audio Announcement

Pre-Alert Audio is played prior to the Header tones in an EAS alert and prior to the alert audio in a non-EAS message. These audio files are selected by clicking once on the **Optional Pre-Alert Audio Announcement** pull-down menu and selecting the desired item from that list with a second click.

When an audio file is selected, additional text will appear below the pull-down menu. The **Listen on Browser** hyperlink text will play the selected audio file through the local computers speakers. It may be useful to access the EAS device from a quieter office rather than a noisy equipment room. The selected audio file's duration (in seconds) and sample rate are also displayed here.

Select Alert Audio Message

This audio selection is the audio used within both an EAS and non-EAS message/ alert. This interface allows for the playout of pre-recorded audio files or the generation of TTS (of the **Custom Text Message**) to be used for the Alert Audio Message. The pull-down menu contains the following options:

- Local Audio File
- Convert Text Message to Speech

With **Local Audio File** selected, the interface displays a pull-down menu titled Select Alert Audio Message. From that pull-down menu, users can select a pre-recorded audio file for playout.

When **Convert Text Message to Speech** is selected, the interface displays selections for available premium voices. Select the desired voice by clicking the radio button to the left of listed voice. There is also a **Test Making Text to Speech Audio File** button for creating the TTS audio file. Click either the **Play->Front Panel** button or **Play on browser** hyperlink to listen to this audio file. This section of the interface also displays the audio files' creation date/time, duration, and sample rate information.

Optional Post-Alert Audio Announcement

Audio played after the Alert Audio in non-EAS applications or following the EOM tones of an EAS alert is considered Post-Alert Audio. The pull-down menu located in this section of the interface will display all the available audio files. These audio files are selected by clicking once on the **Optional Post-Alert Audio Announcement** pull-down menu and selecting the desired item from that list with a second click.

Note
Multiple GPI's may be configured to trigger the same Custom Message Template. The GPI Binding Table will display all the configured GPI's assigned to trigger the selected Custom Message Template. However, a single GPI may not be assigned to multiple templates.

When configuring EAS alerts, the total duration of the EAS alert is displayed just below this pull-down menu – labeled **Total EAS FSK+Audio Duration:**

The interface also contains a hyperlink to the **Setup Audio Output Levels** for easy access to audio output levels.

EAS Encode String and EAS Standard Alert Text Translation *[EAS Specific]*

It is useful, when configuring an EAS alert message, to view the outgoing text information for accuracy. The ZC string will be sent out to encode the Header information. Based on the information contained in the ZC string, the EAS device generates the Standard Alert Text Translation. This is a good place to review the outgoing EAS alert, prior to clicking the **Send Alert** button.

View action and GPI binding table

This check box allows the user to view the Alert Origination Action Table. It contains active hyperlinks displaying the current status of the various peripheral interfaces that can be activated by a custom message/alert. The table displays which peripheral interfaces are available and which are enabled. The active links point to the associated page under **Setup**. Click the interface name to follow the hyperlink and change any specific peripheral used during alert origination.

Alert Origination Action & GPI Binding Tables

The GPI Binding Table (to the right of the Alert Origination Action Table) displays the GPI(s) configured to trigger the selected **Custom Message Template**. A Custom Message Template must be selected (at the top of the screen) in order to see what GPI(s) are configured to trigger that specific Custom Message Template, otherwise the table will display **Message template not selected above**. Load each Custom Message Template to view what GPI's are assigned to that template.

The hyperlink text within the GPI Binding Table will direct the user to the **Setup > GPIO** screen for assigning GPI to Custom Message Templates. (see **Assigning GPI Triggers To Custom Message Templates** (below) for more detailed information)

Upload Audio .WAV file

The interface at the bottom of this screen allows .wav and .mp3 audio files to be uploaded into the EAS device for playout from the EAS device.

Upload Audio .WAV file Section

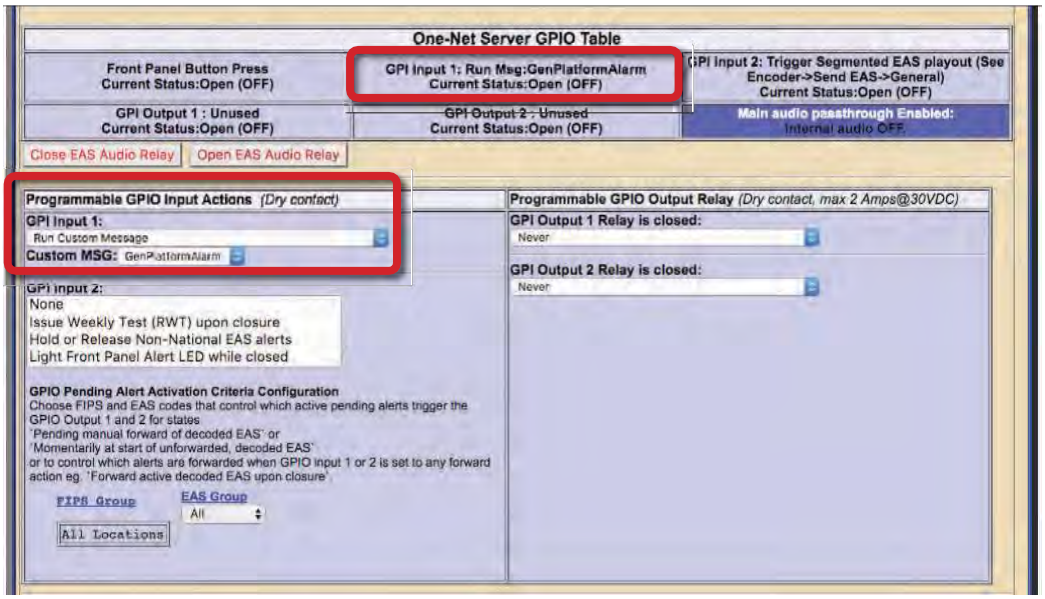
- Click the **Browse** button to locate the file on the local computer
- Click the **Upload .WAV file** button. MP3 files are automatically converted into a WAV files.

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

ASSIGNING GPI TRIGGERS TO CUSTOM MESSAGE TEMPLATES

Custom Message Templates may be triggered by GPIs. This process is performed from the **Setup > GPIO** screen. A hyperlink is available in the GPI Binding Table at the bottom of the Custom Message Pro interface screen or simply navigate using the tab/radio buttons at the top of the user interface.

Any GPI may be assigned to a template – including internal and external/networked GPI's. More than one GPI may be assigned to a single template. However, a single GPI may not be assigned to multiple templates.



GPI Setup Screen

At the top of the GPI Setup screen is the GPIO Table. In the above screen capture, the table displays **GPI Input 1** as being assigned to the **GenPlatformAlarm** custom message template. To configure this relationship:

- Locate the GPI Input 1 pull-down menu on the left side of the interface
- Click the pull-down menu to view the available options
- Select **Run Custom Message** at the bottom of the pull-down menu
- Another pull-down menu will appear titled **Custom MSG:**
- Click on this pull-down menu and select the desired Custom Message Template

Repeat this process for each, individual GPI requiring configuration.

The various GPIO Tables will be updated with these GPI/template assignments. They will also be visible within the GPI Binding Table for each Custom Message Template.

Chapter 8: System Tab

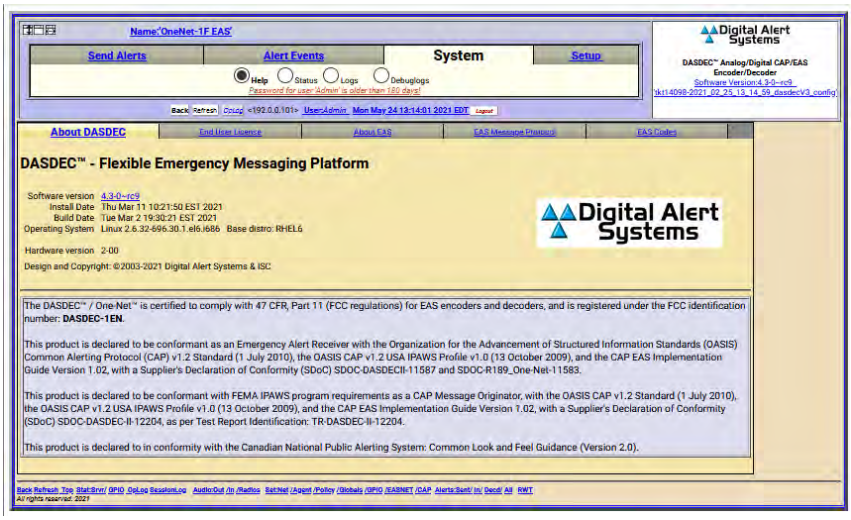
The **System** tab presents system, system status, and log information for the EAS device along with useful Emergency Alert System information. There are no configuration settings contained in these screens. Some display features and hyperlinks to different parts of the web interface are available. The **System** tab has the following radio buttons:

Radio Button	Description
Help	Useful information about the EAS device, End User License agreement, and general information about EAS.
Status	Displays the current status of components such a decoders, GPIOs, network(s), Operating Systems, USB, CPU, PCI, IO devices, and e-mail.
Logs	The EAS device keeps extensive logs on web sessions, operation, OS, security, boot, and e-mail.
Debuglogs	When enabled, displays detailed logs for the decoder, main server, serial ports, audio, video, network(s), and web server. Only use this feature when needed.

HELP

The **System > Help** menu displays basic information about the DASDEC II-1EN, End User License, About EAS EAS Message Protocol, and EAS Codes.

Sub-Tab	Description
About DASDEC-1EN	Displays basic system information about the EAS device, OS version, software version, installation date, software build date, and description of the EAS device.
End User License	Shows a copy of the End User License Agreement
About EAS	Provides a description of the Emergency Alert System
EAS Message Protocol	Illustrates the EAS Message Protocol
EAS Codes	Displays a list of current EAS Codes



Help Screen

About DASDEC II-1EN
Presents information about the installed operating system, software version, install date and build date. This screen additionally displays information about Digital Alert Systems and the EAS device. The software version indicator in the box on the top right side of each screen is a hyperlink to the **Setup > Server > Upgrade** screen.

End User License
A copy of the Digital Alert Systems End User License Agreement isdisplayed on this sub-tab.

About EAS
Emergency Alert System information: purpose, operation, management, your responsibilities as a broadcaster, and the future of EAS and DASDEC.

EAS Message Protocol
Displays EAS message protocol information from the FCC. This text discusses audio FSK, EAS message protocol content and the different elements that comprise an EAS alert message.

EAS Codes
A list of current National, State and Local EAS Event Codes along with a description and severity for each code. This list coincides with available EAS Codes throughout the web interface.

STATUS
The **Status** radio button menu screen has several sub-tab options. Each sub-tab displays a different set of information. The following is a list of sub-tabs and a description of the status information displayed:

Sub-Tab	Description
Main	Displays Platform ID, Server Name, Uptime, Decoder Setting, GPIO, Alert Forwarding and Alert Origination Action Tables along with Printer, Disk Usage and TTS information
GPIO	Presents the current state of GPIO closures
Network	Presents Links, Routes, Net Status Dump, Firewall information along with scripts info for Master and any installed network ports. The SSH Public Encryption Key and Authorized Remote SSH Public Encryption Keys are displayed.
Operating System	Information about the OS including Hostname, Kernel, Uptime, Memory, Temperatures, Disk Usage, Kernel Modules and Sound System are displayed.
USB	A list of Universal Serial Bus (USB) Serial Devices, Basic USB Devices, and a Detailed USB Device List is presented
CPU	Detailed information about the CPU and Run Status
PCI	A detailed list of Peripheral Component Interconnect (PCI) components
IO	A detailed list of Input/Output (IO) device port mapping and memory
Email	Displays the Email Configuration settings

Main Status Screen

LOGS

The **Logs** screen has six sub-page options: Web Session Log, Operation Log, Operating System Log, Security Log, Boot Log, and Email Log.

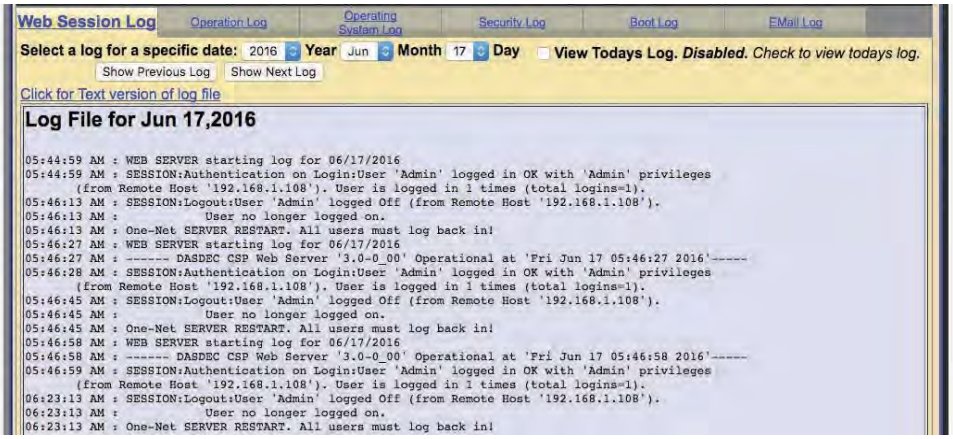
Sub-Tab	Description
Web Session Log	Displays user access to the EAS device
Operation Log	Shows EAS device operation log including EAS event information
Operating System Log	Presents the last 500 lines of current and previous backup log
Security Log	Presents the last 500 lines of security log
Boot Log	Presents the last 500 lines of boot log
EMail Log	Presents the last 500 lines of Email log

Web Session Log

Presents time stamped information about user access to the unit. It shows exactly who and when users logged on or attempted to log on the unit. The Web Session Log is an important part of the security auditing for the unit and should be reviewed often if security is an issue with your installation. Two settings are available.

- Check the **View Today's Log** check box to show the Web session log for the current day.
- Uncheck the box to view archived web session log files. Then select a log for a specific date. You can then show the log for the previous or the next day.

Log files a day old or more old can be deleted using the delete button. The page can be refreshed by a button at the bottom of the page to show new information.



Web Session Log Screen

View a text version of a log page by clicking on the provided **Click for Text Version of log file** hyperlink.

Operation Log

Presents time stamped information about the EAS devices' operation. This interface works the same as the one for the Web Session Log. Important EAS events will be shown here. At the top of every page is an **OpLog** button that navigates to this page.

View a text version of a log page by clicking on the provided link **"Click for Text Version of log file"**.

Operating System Log

Presents the last 500 lines of the current and previous backup of the Linux System Log.

Security Log

Presents the last 500 lines of the Linux System Security Log.

Boot Log

Presents the last 500 lines of the Linux System Boot Log.

EMail Log

Presents the last 500 lines of the Linux System Email Log. Also, has list of the Email Submission Queue and the Email Send Queue.

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

DEBUG LOGS

The Server Debug logs screen is only available when the **Server Debug Log Interface** check box is enabled within the **Setup > Server > Options** screen. These logs provide customer service engineers a better view of what is happening within the EAS device. For each of these sub-tabs categories, a pull-down menu enables users to set Basic, Extra Debug Log Detail Level or None at all. These pull-down menus allow users to turn on specific debug logs for any of the above sub-tab categories. When debugging is no longer needed, make sure to uncheck the **Server Debug Log Interface** check box.

Appendix

HARDWARE AND SOFTWARE SPECIFICATIONS

An Emergency Alert System Analog/Digital Encoder/Decoder Platform

The DASDEC II is a State-of-the-Art Emergency Alert System (EAS) Analog/Digital Encoder/Decoder platform. First introduced in 2005, this system is being deployed around the United States in a wide variety of Cable, Broadcast, IPTV, and Emergency Operation facilities. The EAS device is built with the latest digital PC computer technology along with software based encoding/decoding technology and isbuilt upon the Linux OS. The core hardware is a standard PC motherboard and digital audio sound cards. The EAS device is easy to upgrade, not requiring custom ROMS. TheEAS device also exploits the benefits of modern network technology. It is fully operableover a LAN using secure network protocols. In addition, it supports existing methods of device control using a serial port. This platform is representative of the continuing advancement of PC hardware into technological areas that only a few years ago required custom hardware.

Hardware Specs

- Intelligent alphanumeric LCD for monitoring unit and decoder status
- Operational status LED
- Alert decoding/output LED
- Cool running, low power CPU
- Ethernet port for network access
- Base unit has one 3.5mm mini-jack audio input port that supports Scanning/ decoding EAS on two radio channels
- Hard drive or flash drive options
- 3.5mm mini-jack stereo audio output port
- 3.5mm mini-jack microphone input
- 1 RS-232 Serial port supports a variety of serial control protocols, including industry standards like TFT Standard and Sage Generic.
- 1 parallel port will support a variety of printers
- 2 USB ports - will support a 2nd Ethernet port, extra serial ports, printers, modems, wireless Ethernet, flash drives, etc.
- HDMI out for console or desktop GUI interface
- One NTSC video output
- Standard PS/2 keyboard/mouse ports
- Supports two PCI expansion cards, use with audio card for scanning two more Audio inputs (total of up to six EAS audio sources)
- Internal speaker for monitoring
- Can be safely powered off/on without disk damage
- Optional 3 internal radio receivers, GPI input/output and balanced audio output module.

General Software Features/Specs

- CentOS release 6.9 (Final)
- Built in multi-user, password protected Web interface for control/status/ monitoring of all activity.
- Web interface supports 128-bit encrypted Secure Socket Layer (SSL).
- Email for decoded/forwarded/originated/error alerts & system status
- Supports 2nd network interface via USB
- Supports a variety of printers via USB/Parallel
- Operational status indication via LED and LCD
- Web interface for easy software update
- Programmable GPI input to trigger actions and GPI output relays during alerts.
- English and English/Spanish EAS text translations. Editable EAS translations.
- Configurable audio output port selection for alert origination and forwarding.
- Audio level input/output controls via Web Interface.
- Audio file upload.
- Configurations file download/upload.

Decoder/Forwarding Features

- Decodes FCC EAS codes and NOAA SAME codes from radio transmissions or other analog audio input.
- Automatic audio level correction for reliable operation. Advanced error detection, correction, and logging for noisy EAS transmissions and troubleshooting quality of service problems.
- Supports fully unattended operation.
- Supports manual and user configurable filtered automatic alert auto-forwarding. Easy to use web interface for configuration of auto-forwarding locations and codes.
- Web interface makes it easy to review and print logs of active and expired decoded/forwarded alerts.
- Automatic alert storage management.
- Manages and displays multiple unique simultaneous active decoded alerts.
- Decoding status displayed on unit LCD and LED & Web interface.
- Stores each audio section of EAS alerts into digital files.
- Supports TFT-911 serial protocol for alert audio playback and alert translation data transfer from devices requiring TFT. Supports a variety of other serial protocols for operating CGs.
- Will support scanning up to six decoder input channels (depends on hardware expansion)
- Optional support for a variety of network forwarding protocols: EAS NET (with DVS-168), DVS-644(SCTE-18), and streaming MPEG2 and MPEG4 output digital interfaces.

Encoder/Origination Features

- Easy to use Web interface for creating and sending FCC EAS alerts.
- Web interface makes it easy to configure commonly used locations and alert types.

- Web interface makes it easy to review and print logs of active and expired originated alerts.
- All audio sections of encoded alerts are stored into separate digital audio files.
- Automatic originated alert storage management.
- Supports multiple unique simultaneous active originated alerts.
- Automatic randomized weekly test generation within user configurable calendar time spans.
- Web interface upload feature for digital audio files makes it easy to encode the audio portion of EAS alerts.
- Supports direct recording of EAS alert audio into digital files.
- GPI input controlled alert audio dubbing.
- Optional support for a variety of network origination protocols: EAS NET (with DVS-168), DVS-644(SCTE-18), and streaming MPEG2 and MPEG4 output digital interfaces.

THE EMERGENCY ALERT SYSTEM

Purpose

According to the FCC, "The EAS is designed to provide the President with a means to address the American people in the event of a national emergency. Through the EAS, the President would have access to thousands of broadcast stations, cable systems and participating satellite programmers to transmit a message to the public. The EAS and its predecessors, CONELRAD and the Emergency Broadcast System (EBS), have never been activated for this purpose. But beginning in 1963, the President permitted state and local level emergency information to be transmitted using the EBS."

However, the EAS system is used for much more than to support a method of communication that has never been (and hopefully never will be) used. The EAS system provides state and local officials with a method to quickly send out important local emergency information targeted to a specific area. This includes weather alerts as well as local emergency alerts such as child abductions and disasters. The EAS system also runs test alerts on a weekly and monthly basis in order to insure operability.

Operation

The EAS system digitally encodes data into audible audio in order to distribute messages. This information can be sent out through a broadcast station and cable system. The EAS digital signal uses the same encoding employed by the National Weather Service (NWS) for weather alerts broadcast over NOAA Weather Radio (NWR). Broadcasters and cable operators can decode NWR alerts and then retransmit NWS weather warning messages almost immediately to their audiences. With the proper equipment and setup, EAS alerts can be handled automatically, making EAS information useful for unattended stations. Other specially equipped consumer products, built into some televisions, radios, pagers and other devices, can decode user selectable EAS messages.

The device is designed to facilitate the management side of encoding and decoding EAS alerts within cable and broadcast facilities. It is especially easy to use since it is IP addressable and accessible over a LAN.

Management

The FCC designed the EAS system, working in cooperation with the broadcast, cable, emergency management, alerting equipment industry, the National Weather Service (NWS) and the Federal Emergency Management Administration (FEMA).

The FCC provides information to broadcasters, cable system operators, and other participants in the EAS regarding the requirements of this emergency system. Additionally, the FCC ensures that EAS state and local plans developed by industry conform to the FCC EAS rules and regulations and enhance the national level EAS structure.

NWS provides emergency weather information used to alert the public of dangerous conditions. Over seventy percent of all EAS and EBS activations were a result of natural disasters and were weather related. Linking NOAA Weather Radio digital signaling with the EAS digital signaling will help NWS save lives by reaching more people with timely, site-specific weather warnings.

FEMA provides direction for state and local emergency planning officials to plan and implement their roles in the EAS.

What you need to do as a Broadcaster

The encoder/decoder allows your facility to decode EAS alerts originated from alert sources in your area. These sources can be radio, TV, and cable TV stations. These stations can be forwarding alerts received from a web of broadcasters, or originating alerts if designated as a primary source. **To meet minimum requirements of the FCC, you must send randomized weekly tests, forward monthly tests, and forward National alerts**. Your state and local EAS plan may also impose other requirements.

A good source of information is the EAS website at https://www.fcc.gov/general/emergency-alert-system-eas. The FCC provides handbooks in Adobe PDF format for AM and FM radio, for TV and for Cable TV.

PERIPHERALS

The DASDEC supports many peripheral devices, from character generators toprinters. As of this release, the EAS device can replace most commercial EAS encoder/decoder units, depending upon the peripheral hardware to which they have been connected.

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 overplayed on live video on these units. The Digibox CODI provides SDI digital video input and output. The EAS device also supports simultaneous network based control of multiple CODI Digibox units that provide a built-in LAN port. This valid TV and Plus Package license keys. See www.chyron.com.

Evertz Keyers

Evertz Logo Inserters, Media Keyers, and other digital and analog Evertz character generators are supported by the EAS device using the SAGE generic CG protocol. The Evertz unit must support an EAS option and be pre-programmed to recognize EAS communication on the specific COM port being used. For digital operation the EAS device must be equipped with an optional AES audio output or the EAS device Analog audio needs to be encoded into AES digital audio with an A to D converter. The GPI EAS Audio output of the EAS device is used as an input to trigger voice-over activation on the Evertz unit. The Evertz units handle all switching between normal program video/ audio to EAS play-out. The EAS device offers manual alert forwarding notification with GPI output relay indication of pending alerts. This allows EAS to be forwarded when appropriate, either manually by an operator or by automation. See the diagram below.

The directions provided by Evertz for the SAGE generic protocol has been tested by Evertz and will work with the EAS device. See www.evertz.com.

XBOB CG

The EAS device can generate a crawl on a single video channel that is passed through an XBOB. This option requires a valid TV license key.

BetaBrite LED sign

The EAS device supports driving the wide range of BetaBrite LED signs from a EAS device serial port. A special cable is usually needed to connect the EAS device RS-232 serial ports to a BetaBrite. The BetaBrite protocol on the EAS device supports running EAS alert text crawls immediately upon decoding as well as during alert origination and forwarding.

Other Character Generators

Any character generator or turnkey system that can operate the standard TFT 911 EAS serial control protocol or supports the SAGE Generic protocol can interface to a EAS device. A Null modem cable from the CG serial port must be connected to the EAS device serial port for TFT emulation. The serial cable required for units using the SAGE Generic CG protocol depends on the unit.

Character generators that can be run from the SAGE generic CG protocol include Evertz Keyers and Miranda ImageStore units.

Utah Scientific SqueezeMax

Interfacing to a TV system with Utah Scientific SqueezeMax HD system with Utah Scientific 2020 switcher, downstream mode.

The EAS device can interface to multiple SqueezeMax units using the LAN based EAS NET protocol, but the alert must be played on all SqueezeMax units at the same time. EAS NET sends alert text to each interfaced SqueezeMax unit and then goes into a pending alert play-out state. The text alert sent to the SqueezeMax places it into a pending EAS play-out mode. The EAS crawl can then be triggered manually on the SqueezeMax via 2020 Master Control switcher when desired (within a few minutes). Master Control supports this action via a custom macro, associated with a panel button, which triggers the SqueezeMax EAS preset, switches audio output to the EAS device input, and produces a GPI contact closure for triggering alert play-out on the EAS device. The EAS device goes out of pending alert mode and plays the alert audio until finished. When the alert is finished, SqueezeMax is taken out of EAS display and Master Control returns audio back to normal program audio.

The EAS device can also be directly connected to a single SqueezeMax using a serial connection.

Interfacing to a TV system with Utah Scientific SqueezeMax SD system with Utah Scientific 2020 switcher, upstream mode.

Refer to the description above for the SqueezeMax. An EAS device can interface to mixed SD and HD SqueezeMax units, but as described above, the alert must be played on all units at the same time.

For additional information refer to the Digital Alert Systems website's application notes. (http://www.digitalalertsystems.com/resources_application_notes.htm#)

EAS PROTOCOL

The EAS device encodes the EAS messages per FCC rules for the EAS protocol. The EAS protocol from the FCC is described as follows (printed directly from the FCC ruling).

The EAS uses a four-part message for an emergency activation of the EAS. The four parts are; Preamble and EAS Header Codes, audio Attention Signal, message, and, Preamble and EAS End Of Message Codes.

The Preamble and EAS Codes must use Audio Frequency Shift Keying at a rate of 520.83 bits per second to transmit the codes. Mark frequency is 2083.3 Hz and space frequency is 1562.5 Hz. Mark and space time must be 1.92 milliseconds. Characters are ASCII seven bit characters as defined in ANSI X3.4-1977 ending with an eighth null bit (either 1 or 0) to constitute a full eight-bit byte.

The Attention Signal must be made up of the fundamental frequencies of 853 and 960 Hz. The two tones must be transmitted simultaneously. The Attention Signal must be transmitted after the EAS header codes.

The message may be audio, video or text.

The ASCII dash and plus symbols are required and may not be used for any other purpose. Unused characters must be ASCII space characters. FM or TV call signs must use a slash ASCII character number 47 (/) in lieu of a dash.

The EAS protocol, including any codes, must not be amended, extended or abridged without FCC authorization. The EAS protocol and message format are specified in the following representation. Examples are provided in FCC Public Notices.

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-
(one second pause)
[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-
(one second pause)
[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-
(At least a one second pause)
(Transmission of 8 to 25 seconds of Attention Signal)
(Transmission of audio, video or text messages)
(at least a one second pause)
[PREAMBLE]NNNN
(One second pause) [PREAMBLE]NNNN
(One second pause) [PREAMBLE]NNNN
(At least one second pause)

[PREAMBLE] This is a consecutive string of bits (sixteen bytes of AB hexadecimal [8 bit byte 10101011]) sent to clear the system, set AGC and set asynchronous decoder clocking cycles. The preamble must be transmitted before each header and End Of Message code.

ZCZC- This is the identifier, sent as ASCII characters ZCZC to indicate the start of ASCII code.

ORG- This is the Originator code and indicates who originally initiated the activation of the EAS. These codes are specified in paragraph (d) of this section.

EEE- This is the Event code and indicates the nature of the EAS activation. The codes are specified in paragraph (e) of this section. The Event codes must be compatible with the codes used by the NWS Weather Radio Specific Area Message Encoder (WRSAME).

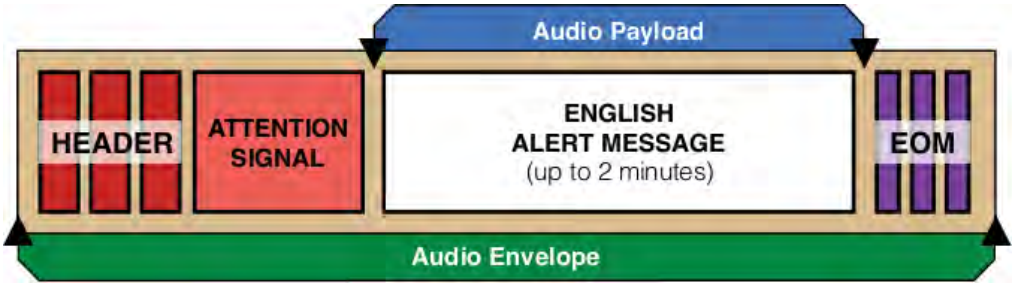
PSSCCC- This is the Location code and indicates the geographic area affected by the EAS alert. There may be 31 Location codes in an EAS alert. The Location code uses the Federal Information Processing Standard (FIPS) numbers as described by the U.S. Department of Commerce in National Institute of Standards and Technology publication FIPS PUB 6-4. Each state is assigned an SS number as specified in paragraph (f) of this section. Each county and some cities are assigned a CCC number. A CCC number of 000 refers to an entire State or Territory. P defines county subdivisions as follows: 0 = all or an unspecified portion of a county, 1 = Northwest, 2 = North, 3 = Northeast, 4 = West, 5 = Central, 6 = East, 7 = Southwest, 8 = South, 9 = Southeast. Other numbers may be designated later for special applications. The use of county subdivisions will probably be rare and generally for oddly shaped or unusually large counties. Any subdivisions must be defined and agreed to by the local officials prior to use.

+TTTT- This indicates the valid time period of a message in 15 minute segments up to one hour and then in 30 minute segments beyond one hour; i.e., +0015, +0030, +0045, +0100, +0430 and +0600.

JJJHHMM- This is the day in Julian Calendar days (JJJ) of the year and the time in hours and minutes (HHMM) when the message was initially released by the originator using 24 hour Universal Coordinated Time (UTC).

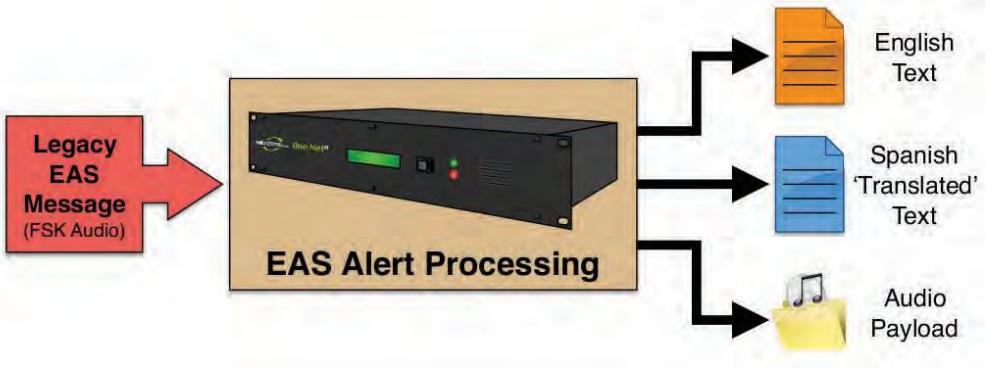
LLLLLLLL- This is the identification of the broadcast station, cable system, MDS/MMDS/ ITFS station, NWS office, etc., transmitting or retransmitting the message. These codes will be automatically affixed to all outgoing messages by the EAS encoder.

NNNN- This is the End of Message (EOM) code sent as a string of four ASCII N characters.

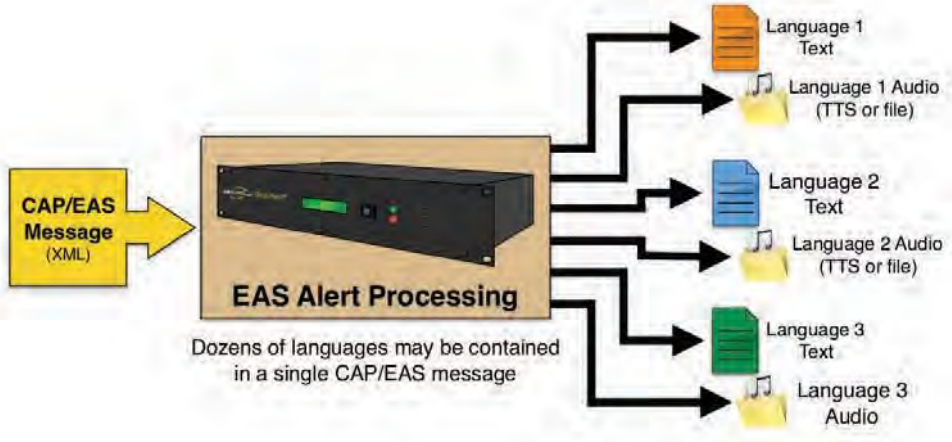


Incoming EAS Alert Message
(FSK Audio)

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



Legacy EAS Message Processing



CAP/EAS Message Processing
(XML)

The only originator codes are:

Originator Description	Originator Code
Code Broadcast station or cable system	EAS
Civil authorities	CIV
National Weather Service	WXR
Primary Entry Point System	PEP

The following Event (EEE) codes are presently authorized:

The following tables includes four columns describing EAS Codes: Nature of Action (description of Event Code), Event Code, Type, and maximum amount of time Delay allowed when forwarding the EAS alert.

National Codes (Required):

Nature of Action	Event Code	Type	Delay (:MM)
Emergency Action Notification	EAN (National only)	Emergency	:00
National Periodic Test	NPT (National only)	Test	:00
National Information Center	NIC (National only)	Advisory	:15
Required Monthly Test	RMT	Test	:60
Required Weekly Test	RWT	Test	:15

State and Local Codes (Optional):

Nature of Action	Event Code	Type	Delay (:mm)
Administrative Message	ADR	Advisory	:15
Avalanche Warning	AVW	Warning	:15
Avalanche Watch	AVA	Watch	:15
Blizzard Warning	BZW	Warning	:15
Blue Alert	BLU	Warning	:15
Child Abduction Emergency	CAE	Emergency	:15
Civil Danger Warning	CDW	Warning	:15
Civil Emergency Message	CEM	Emergency	:15
Coastal Flood Warning	CFW	Warning	:15
Coastal Flood Watch	CFA	Watch	:15
Demo / Practice Warning	DMO	Test	:15
Dust Storm Warning	DSW	Warning	:15
Earthquake Warning	EQW	Warning	:15
Extreme Wind Warning	EWW	Warning	:15
Evacuation Immediate	EVI	Emergency	:15
Fire Warning	FRW	Warning	:15
Flash Flood Warning	FFW	Warning	:15
Flash Flood Watch	FFA	Watch	:15
Flash Flood Statement	FFS	Advisory	:15

New Feature
The Blue Alert EAS event code (BLU) has been added to version 4.0 in compliance with the Federal Communications Commission's 47 CFR Part 11 final rule.

Nature of Action	Event Code	Type	Delay (:mm)
Flood Warning	FLW	Warning	:15
Flood Watch	FLA	Watch	:15
Flood Statement	FLS	Advisory	:15
Hazardous Materials Warning	HMW	Warning	:15
High Wind Warning	HWW	Warning	:15
High Wind Watch	HWA	Watch	:15
Hurricane Warning	HUW	Warning	:15
Hurricane Watch	HUA	Watch	:15
Hurricane Statement	HLS	Advisory	:15
Law Enforcement Warning	LEW	Warning	:15
Local Area Emergency	LAE	Emergency	:15
Network Message Notification	NMN	Advisory	:15
911 Telephone Outage Emergency	TOE	Emergency	:15
Nuclear Power Plant Warning	NUW	Warning	:15
Radiological Hazard Warning	RHW	Warning	:15
Severe Thunderstorm Warning	SVR	Warning	:15
Severe Thunderstorm Watch	SVA	Watch	:15
Severe Weather Statement	SVS	Advisory	:15
Shelter in Place Warning	SPW	Warning	:15
Special Marine Warning	SMW	Warning	:15
Special Weather Statement	SPS	Advisory	:15
Storm Surge Watch	SSA	Watch	:15
Storm Surge Warning	SSW	Warning	:15
Tornado Warning	TOR	Warning	:15
Tornado Watch	TOA	Watch	:15
Tropical Storm Warning	TRW	Warning	:15
Tropical Storm Watch	TRA	Watch	:15
Tsunami Warning	TSW	Warning	:15
Tsunami Watch	TSA	Watch	:15
Volcano Warning	VOW	Warning	:15
Winter Storm Watch	WSA	Watch	:15
Winter Storm Warning	WSW	Warning	:15

TERMS AND DEFINITIONS

Term	Definition
AEA	A key component of ATSC 3.0 - the next generation broadcasting standard. Advanced Emergency Alert (AEA) is still in the implementation phase, but promises to create enhanced value for viewers, broadcasters, electronics manufacturers, and emergency alerting authorities with on-screen, rich media emergency alerting information.
AES	Is a standard for the exchange of digital audio signals between professional audio devices. AES was jointly developed by the Audio Engineering Society (AES) and the European Broadcasting Union (EBU). Also known as AES3 or AES/EBU.
BNC	A round, quick connect/disconnect radio frequency connector used for coaxial cable. It features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. The connector was named the BNC (for Bayonet Neill–Concelman) after its bayonet mount locking mechanism and its inventors, Paul Neill and Carl Concelman.
CAP	The Common Alerting Protocol (CAP) is an XML-based data format for exchanging public warnings and emergencies between alerting technologies. CAP allows a warning message to be consistently disseminated simultaneously over many warning systems to many applications. CAP is an international standard that has been adapted by several countries to communicate emergency warnings including, Australia (CAP-AU-STD), Canada (CAP-CP/NPAS), Germany (MoWaS), and the United States (IPAWS-OPEN).
CAT-5 Cable	Category 5 cable (or CAT-5), is a twisted pair cable for carrying signals. This type of cable is used in structured cabling for computer networks such as Ethernet. The cable standard provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet). Category 5 was superseded by the category 5e (enhanced) specification, and later category 6 cable.
CG	A character generator (CG) is a device or software that produces static or animated text (such as crawls and credits rolls) for keying into a video stream.
EAS	The Emergency Alert System (EAS) is a national warning system in the United States put into place on January 1, 1997, when it replaced the Emergency Broadcast System (EBS), which in turn replaced the CONELRAD System. EAS is also designed to alert the public of local weather, law enforcement, and civil emergencies.
Ethernet	Ethernet is a family of computer networking technologies commonly used in local area networks (LANs). Frequently used wiring is CAT5/6 twisted pair cables with RJ-45 connectors (or 8P8C modular connectors).

Term	Definition
FCC	An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. The commission is the United States' primary authority for communications laws, regulation and technological innovation.
FIPS Codes	Geographic codes developed by the Federal Information Processing Standards (FIPS) that establish six digit numeric values for US states, counties, subdivision of counties and other predefined geographic boundaries.
FSK	Frequency-shift keying (FSK) is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal. FSK is used to transmit data within the EAS header.
GPIO	General-purpose input/output (GPIO) is a generic pin on an integrated circuit whose behavior—including whether it is an input or output pin—is controllable by the user at run time.
Hyperlink	A hyperlink is a reference to data the reader can directly follow either by clicking or hovering over. A hyperlink points to a whole document or to a specific element within a document. Hyperlinks are typically displayed in blue, underlined text: FIPS Groups.
IP Address	An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. Because of the growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed. IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6).
LED	A light-emitting diode (LED) is a two-lead semiconductor light source. When a suitable voltage is applied to the leads, electrons release energy in the form of photons – also called electroluminescence.
MPEG	The Moving Picture Experts Group (MPEG) is a working group of authorities that was formed by ISO and IEC to set standards for audio and video compression and transmission.

Term	Definition
NOAA	The National Oceanic and Atmospheric Administration (NOAA) is an American scientific agency within the United States Department of Commerce focused on the conditions of the oceans and the atmosphere. NOAA warns of dangerous weather, charts seas, guides the use and protection of ocean and coastal resources, and conducts research to improve understanding and stewardship of the environment.
NTP	Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).
PS/2	The PS/2 connector is a 6-pin mini-DIN connector used for connecting some keyboards and mice to a PC compatible computer system.
RCA Connector	Sometimes called a phono connector or Cinch connector, is a type of electrical connector commonly used to carry audio and video signals. The name “RCA” derives from the Radio Corporation of America, which introduced the design by the early 1940s for internal connection of the pickup to the chassis in home radio-phonograph consoles.
RJ45 Connector	The RJ45 connector (also known as 8 position 8 contact (8P8C)) is a modular connector commonly used to terminate twisted pair and multi-conductor flat cable. These connectors are commonly used for Ethernet over twisted pair.
RG6	RG-6 is a common type of coaxial cable and is generally used to refer to coaxial cables with an 18 AWG center conductor and 75 ohm characteristic impedance.
SCTE-18	A standard developed by the Society of Cable Telecommunication Engineers (SCTE) that defines an Emergency Alert signaling method for use by cable TV systems to signal emergencies to digital receiving devices that are offered for retail sale. Such devices include digital settop boxes that are sold to consumers at retail, digital TV receivers, and digital video recorders. Also referred to as DVS644.
Serial Port	A serial communication interface through which information transfers in or out one bit at a time. The term “serial port” identifies hardware compliant to the RS-232/422 standards, intended to interface with external CG’s.

Term	Definition
TRS Connector	A three-contact phone connector (also known as phone jack, audio jack or jack plug) where T stands for “tip”, R stands for “ring” and S stands for “sleeve”. Is derived from a common family of connector typically used for analog audio signals. The outside diameter of the “sleeve” conductor is 1⁄4 inch (exactly 6.35 mm). The “mini” connector has a diameter of 3.5 mm (approx. 1⁄8 inch) and the “sub-mini” connector has a diameter of 2.5 mm (approx. 3⁄32 inch).
USB	Universal Serial Bus (USB) is an industry standard that defines the cables, connectors and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices.
VGA	Video Graphics Array (VGA) refers to the analog computer display standard found within the 15-pin D-subminiature VGA connector.
Web Browser	Commonly referred to as a browser - is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI/URL) and may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources. The major web browsers are Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Opera.
XLR Connector	The XLR connector is a style of electrical connector, primarily found on professional audio, video, and stage lighting equipment. The connectors are circular in design and have between 3 and 7 pins. They are most commonly associated with balanced audio, including AES3 digital audio.

END USER LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS ("Agreement") CAREFULLY. USE OF THE SOFTWARE defined below) PROVIDED BY DIGITAL ALERT SYSTEMS, INC. IS PERMITTED ONLY UNDER AND IN ACCORDANCE WITH THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, PLEASE DO NOT USE THIS SOFTWARE.

1. Grant of License. This Agreement permits you to have a limited, non-transferable, non-exclusive, license for use of the Software or the software included in this device ("Software"). For each software licensee, the program can be "in use" on, or in conjunction with the DASDEC™, DASDEC-III, DASEOC™, ("Device"). **IF YOU DO NOT AGREE TO BE LEGALLY BOUND TO BY THIS AGREEMENT IN ITS ENTIRETY, AND WITHOUT CHANGE TO ITS TERMS AND CONDITIONS, YOU DO NOT HAVE A LICENSE TO USE THIS SOFTWARE.**

2. License Restrictions. YOU MAY NOT RENT, LEASE, SUBLICENSE, SELL, ASSIGN, LOAN OR OTHERWISE TRANSFER THE SOFTWARE OR ANY OF YOUR RIGHTS AND OBLIGATIONS UNDER THIS AGREEMENT. You may not modify, translate, reverse assemble, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate or otherwise circumvent any software protection mechanisms in the Software, including without limitation any such mechanism used to restrict or control the functionality of the Software, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the Software (except to the extent that such activities may not be prohibited under applicable law). However, you may transfer all your right to use the Software to another person or organization, provided that (a) the followings are also transferred with the Software, (i) this Agreement;(ii) other software if contained in the original package, and/or hardware that the Software is bundled;(iii) any original or updated version of the Software; (b) no copies including back-up and installed in your computer or other device are at your possession after the transfer, and (c) the recipient accepts all the terms of this Agreement. In no event shall you transfer the Software obtained as a trial, test version, or otherwise specified as not for resale. A special license permit from DIGITAL ALERT SYSTEMS is required if the program is going to be installed on a network server for the sole purpose of distribution to other computers.

3. Copyright. The Software or the Software contained in this package or device is protected by United States copyright laws, international treaty provisions, and all other applicable national laws. The Software must be treated like all other copyrighted materials (e.g. books and musical recordings). This license does not allow the Software to be rented or leased, and the written materials accompanying the Software (if any) may not be copied.

4. Ownership. Title, ownership rights, and all intellectual property rights in and to the Software and any accompanying documentation, and any copy of the foregoing, and any sample contents shall remain the sole and exclusive property of Digital Alert Systems and/or its third party licensors. You agree to abide by the copyright law and all other applicable laws. You acknowledge that the Software contains valuable confidential information and trade secrets of Digital Alert Systems and/or its third party licensors.

5. Warranty Disclaimer. THE SOFTWARE IS MADE AVAILABLE TO YOU ON "AS IS" BASIS. NO WARRANTIES, EITHER EXPRESS OR IMPLIED, AREMADEWITHRESPECT 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.