FLEXIBLE EMERGENCY MESSAGING PLATFORM

USER MANUAL

DASDEC™ III

Version X.0

Revision 0621

Digital Alert Systems, Inc.

100 Housel Ave • Lyndonville, NY 14098
www.digitalalertsystems.com

FCC Information

FCC ID: R8VXXXXXX-XXX

The DASDEC-*III* complies with Part 11 (47 CFR 11) of the FCC's rules for EAS encoders and decoders, including a Declaration of Conformity for Common Alerting Protocol (CAP) compliance, and are registered with the FCC under identification number: R8VXXXXXX-XXX.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

Disclaimer

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

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

Safari is a registered trademark of Apple Inc.
CODI is a registered trademark of Chyron Corporation.
Chrome is a registered trademark of Google Inc.
VDS-830, VDS-840, Starmu and Star-8 are trademarks of Keywest Technology, Inc.
Internet Explorer is a registered trademark of Microsoft Corporation
Firefox is a registered trademark of the Mozilla Foundation
SqueezeMax is a trademark of Utah Scientific, Inc.

Contact Information:
Digital Alert Systems, Inc.
100 Housel Ave • Lyndonville, NY 14098-9508

Sales & Technical Support:
Office: 585-765-2254

Table of Contents

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

INTRODUCTION to the DASDEC *III*

The DASDEC-*III* (DAS3) Emergency Alert System (EAS) Analog and Digital CAP/ Encoder/Decoder platforms are easy to use and relatively easy to learn. Generally, the web-based interface screens (web pages) are self-explanatory. Some users may be able to experiment with features with satisfactory results. However, the platform offers many features. Referring to this manual frequently will increase understanding and decrease learning time for successful, customized operation.

Note A number of DASDEC-*III* features are licensed. Licensing these features enables users to customize the unit to the specific needsof its application. Note that this manual reviews every screen and explains all of the user's licensing permissions.

ICONS

Icons are used in this manual to highlight information.

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

HIGHLIGHTS

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

ORGANIZATION

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

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

CONVENTIONS

The following conventions are used throughout this manual.

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

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

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

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

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

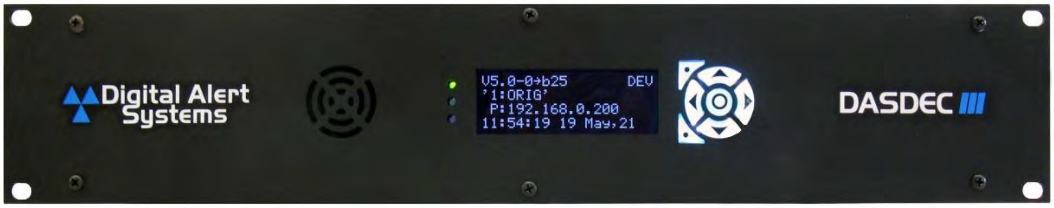
Attention
This manual is organized in a sequential fashion to assist first-time users in the step-by-step configuration of the EAS device. For best results, first-time users should follow the instructions in the order in which they are presented.

Chapter 1: Hardware Overview

INTRODUCTION

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

FRONT PANEL



Front Panel of the DASDEC-III

The front panel features a 4 line x 20 character backlit LCD that indicates power-on and real-time device status. Three LEDs (1 green, 1 red, 1 blue) are used for a variety of status indications. A small grill provides audio from an internal speaker.

Front Panel Display

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

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

Note
Server Name refers to the individual device's given name (Default is DASDEC-III). To change the Server Name, log in to the web browser interface and navigate to **Setup > Server > Main/ License**.

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

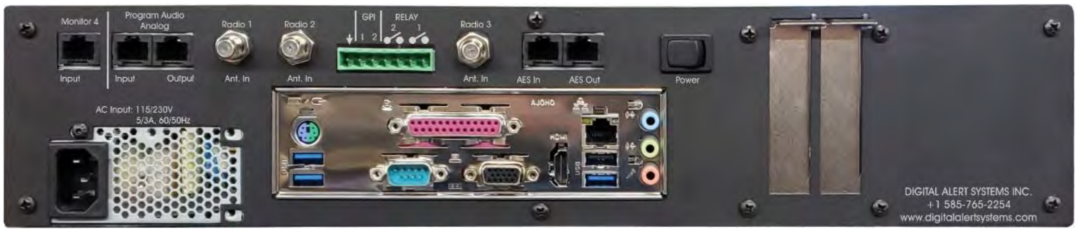
Status LEDs

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

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

BACK PANEL

The back panel provides all of the connections necessary for the EAS device. Connections as labeled:



Back Panel Connections

- **Monitor 4**
- **Program Audio Analog**
- **Radio Antenna Connectors (1, 2, & 3)**
- **AES Audio**
- **Power Switch**
- **Power Receptacle**
- **PS/2 Port**
- **USB Ports**
- **VGA**
- **Serial Port (COM 1)**
- **HDMI**
- **Main Network Interface**
- **Main Audio**
- **Expansion Slots**

Note
The image to the left includes the Triple Port GigabitEthernet Expansion and AES Audio Options. Not all DASDEC-*III* devices will contain the same rear connectors. See the DASDEC Chassis Chart for a list different models and backpanel configurations.

Note
The device provides software support for the Video Out, Ethernet Expansion, and AES Program Audio as licensed options.

Note
Two Expansion Slots are provided for optional hardware.

Chapter 2: Hardware Connections

INSTALLATION

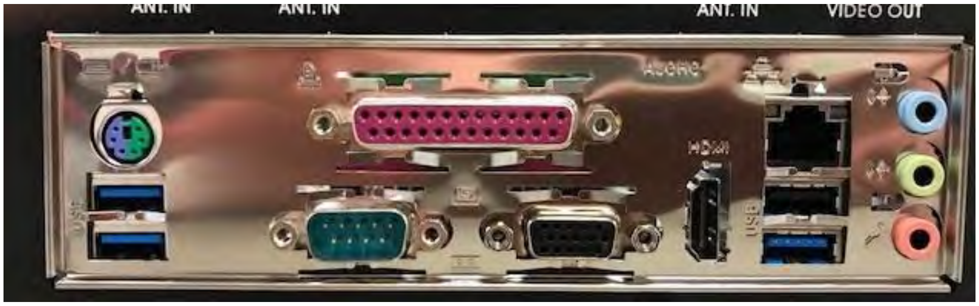
The DASDEC-*III* frame mounts in an EIA-compliant equipment rack by meansof four rack screws fastened through the front mounting ears.

For safe, long-term reliability:

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

Rack Units	Height	Depth	Width	Weight
2RU	3.50" (8.89 cm)	12.0" (30.48 cm)	19.0" (48.26 cm)	16 lbs (7.25 kg)

NETWORK CONNECTIONS



Network Connections Example (devices may vary)

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

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

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

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

Note
In facilities that require supplementary network connectivity, additional networking hardware may be installed. Optional network expansion will enable the 2nd and 3rd Network Interface ports. Navigate to **Setup > Network > Configuration** to configure the network ports via the web interface.

RADIO ANTENNAS

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

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

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

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

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

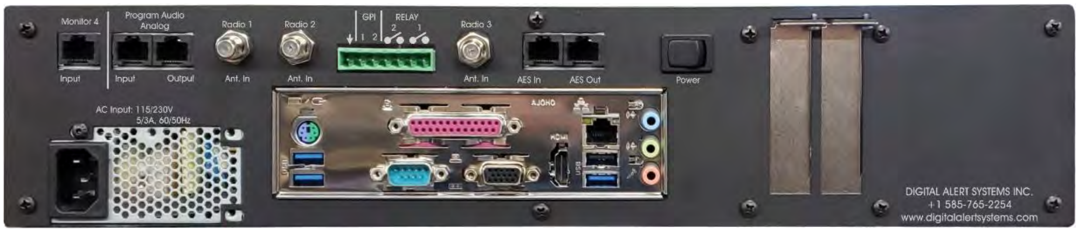
AUDIO WIRING

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

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

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

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



Back Panel

Analog Audio Wiring

The first type of inputs connects to internal EAS decoders. These inputs are utilized to process broadcast EAS messages, and are attached to external radio receivers or other EAS equipment. RJ45 connectors are used for these inputs. Each EAS decoder accepts a mono audio signal. This single stereo input jack feeds two separate EAS decoders.

The second type of analog audio inputs are connected to the main program audio when internal switching of the audio signal is to be performed within this EAS device. These balanced audio inputs are only utilized for program audio switching, and do not tie to the EAS decoders. RJ45 are used.

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

Analog Audio Outputs

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

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

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

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

AES DIGITAL AUDIO WIRING

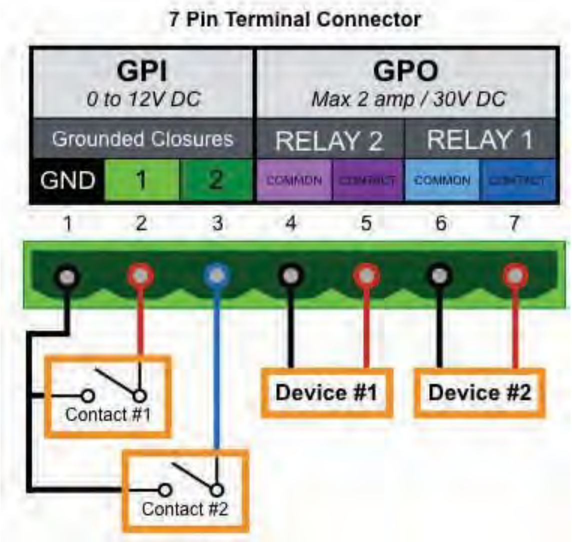
An optional AES audio input/output function is available for the DASDEC platform. This includes the capability for an AES digital audio output, along with a switching AES audio output when an AES audio input is connected. A DE-9 to Male XLR and Female XLR breakout cable is provided. Refer to the diagrams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

VIDEO WIRING

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

GENERAL PURPOSE INPUT/OUTPUT (GPIO)

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



GPIO Terminal Connector

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

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

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

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

Note
See Chapter 5 - GPIO Setup for more information and available functions.

Additional Expansion GPIO Options

For installations that require additional GPIs and GPOs, there are several options available that will expand the standard capabilities. An internal GPIO card may be installed in the PCI expansion slot to enable eight additional GPIs and eight additional GPOs. If the PCI expansion slot is not available, there are several network connected GPIO devices, such as the R190A Remote LAN Hub Controller / Net GPIO. The DASDEC platform can mix and match any combination of internaland network connected GPIO devices.

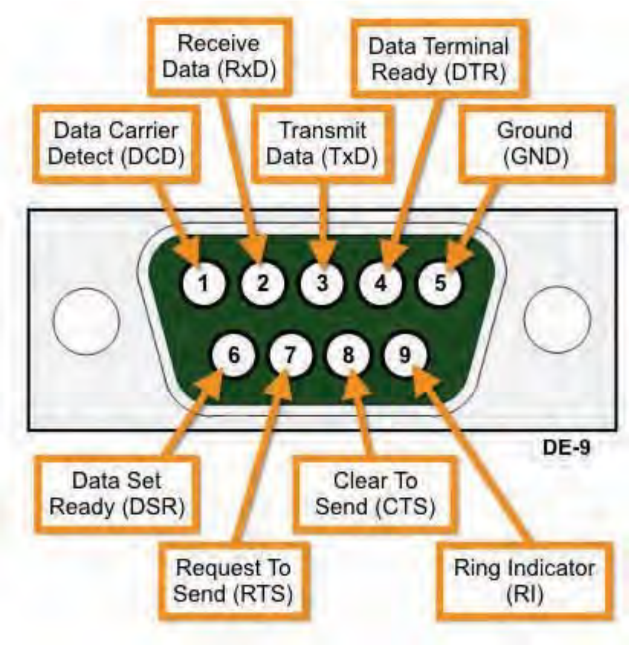
Note
See Chapter 5 - Net Alerts Setup > Hub Controller/ Net GPIO for more information.

SERIAL PORT WIRING

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

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

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



Serial Port Connections (Chassis Side)

Note
For configuration of serial port protocols, see Chapter 5 - Video/CG.

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

POWER CONNECTIONS

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

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

MAKING FIRST CONTACT

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

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

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

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

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

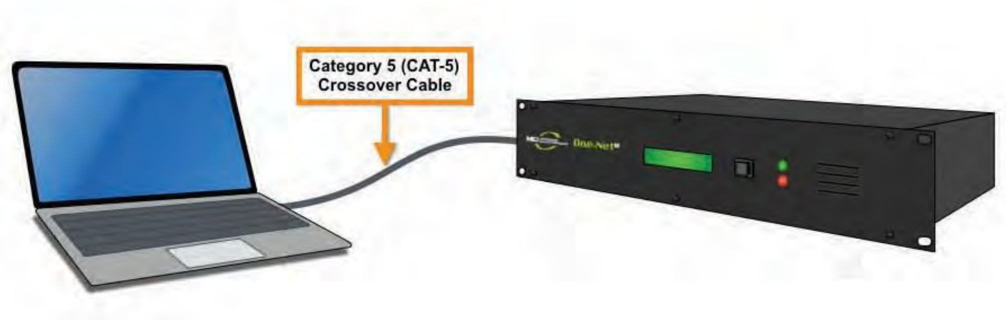
Note
The EAS device is shipped with a CAT-5 crossover cable that is intended for the direct connection scenario.

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

Once the EAS device is correctly wired:

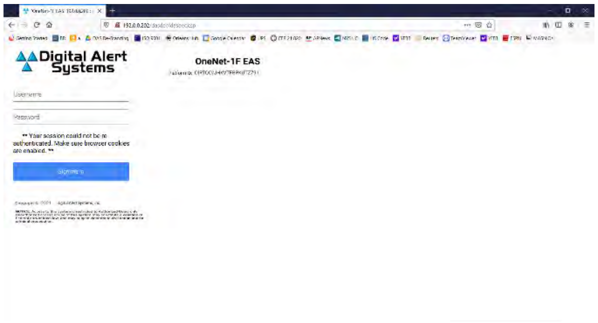
1. Turn on the EAS device by pressing and releasing the power switch **(5)** on the upper right side of the back panel.
2. The LCD screen will light during the power on.
3. Allow the device time to boot. (See the Front Panel Display section for complete startup sequence.)
4. On the front panel, a solid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

Direct Connection



Direct Connection

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



** Your session could not be re authenticated. Make sure browser cookies are enabled. **

Web Interface Login Screen

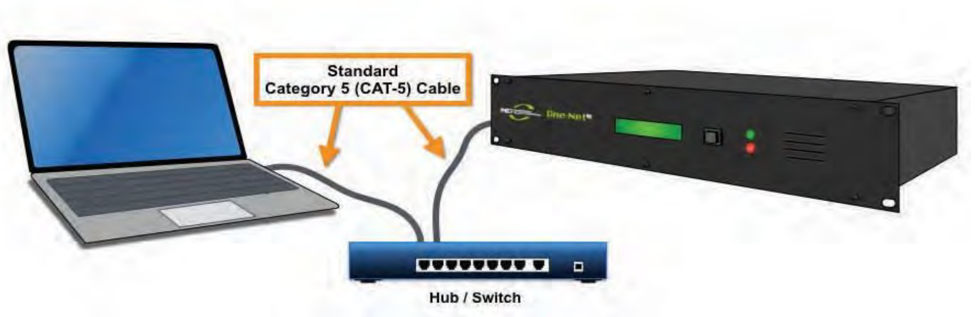
4. Once the EAS devices' IP address and subnet mask have been configured to correspond with your facilities' computer network addressing scheme, it will no longer be accessible from the standalone computer.
5. Reset the standalone computers' network configuration back to its original settings, remove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

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

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

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

Hub/Switch Connection

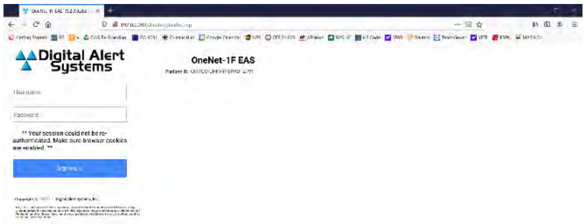


Hub/Switch Connected

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

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

WEB INTERFACE LOGIN



OneNet-1F EAS

Username

Password

** Your session could not be re-authenticated. Make sure browser cookies are enabled. **

Sign me in

Web Interface Login Screen

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

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

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

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

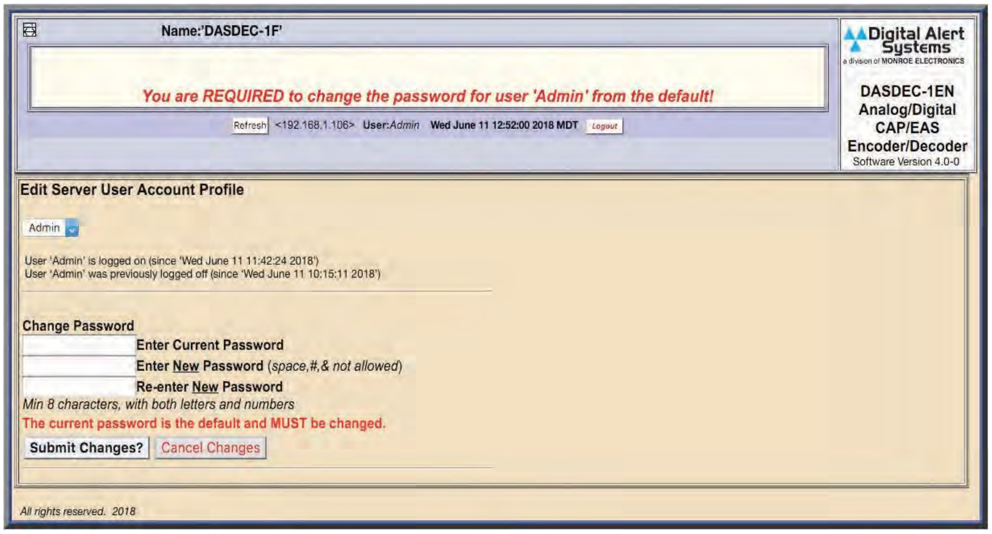
Note
Multiple login sessions are allowed at the same time.

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

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

Click the **Login** button.

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



You are REQUIRED to change the password for user 'Admin' from the default!

<192.168.1.106> User:*Admin* Wed June 11 12:52:00 2018 MDT

Edit Server User Account Profile

User 'Admin' is logged on (since 'Wed June 11 11:42:24 2018')
User 'Admin' was previously logged off (since 'Wed June 11 10:15:11 2018')

Change Password

Enter Current Password
Enter New Password (*space,#,& not allowed*)
Re-enter New Password
Min 8 characters, with both letters and numbers
The current password is the default and MUST be changed.

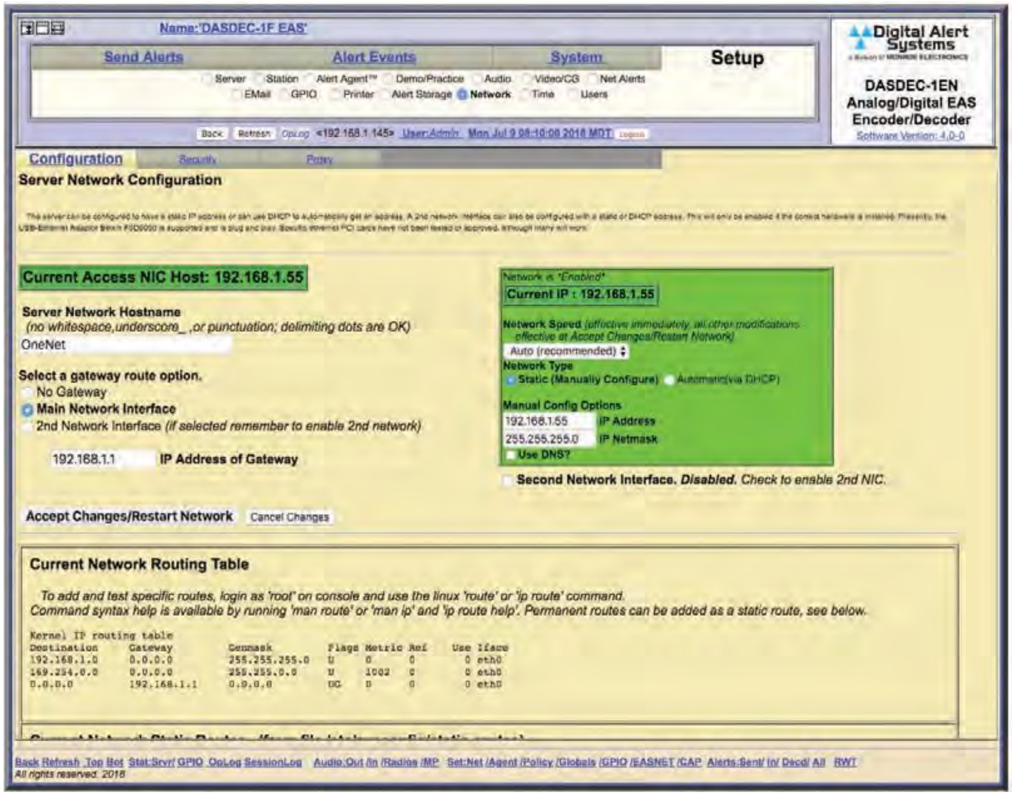
All rights reserved. 2018

Edit Server User Account Profile Screen

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

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

Note
Review the New Password Policy when creating a new password.


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
○ Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ● Network ○ Time ○ Users
Back
Refresh
OpLog
<192.168.1.145>
User:Admin
Mon Jul 9 08:10:08 2018 MDT
Logout
Digital Alert Systems
DASDEC-1EN
Analog/Digital EAS
Encoder/Decoder
Software Version: 4.0-0
Configuration
Security
Proxy
Back Refresh Top Bot Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios /MP Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2018

Server Network Configuration

The server can be configured to have a static IP address or can use DHCP to automatically get an address. A 2nd network interface can also be configured with a static or DHCP address. This will only be enabled if the correct hardware is installed. Presently, the USB-Ethernet Adaptor Belkin F5D5050 is supported and is plug and play. Specific ethernet PCI cards have not been tested or approved, although many will work.

Current Access NIC Host: 192.168.1.55

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

Select a gateway route option.
○ No Gateway
● **Main Network Interface**
○ 2nd Network Interface *(if selected remember to enable 2nd network)*

192.168.1.1 **IP Address of Gateway**

Network is "Enabled"
Current IP : 192.168.1.55

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

Network Type
● **Static (Manually Configure)** ○ Automatic(via DHCP)

Manual Config Options
192.168.1.55 **IP Address**
255.255.255.0 **IP Netmask**
□ **Use DNS?**

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

Accept Changes/Restart Network   Cancel Changes

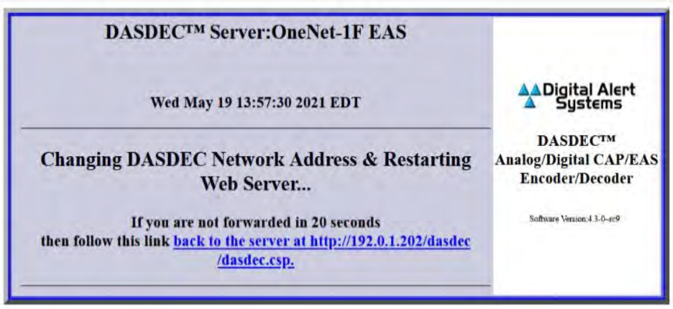
Current Network Routing Table

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

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

Server Network Configuration Screen

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



DASDEC™ Server:OneNet-1F EAS

Wed May 19 13:57:30 2021 EDT

Changing DASDEC Network Address & Restarting Web Server...

If you are not forwarded in 20 seconds
then follow this link back to the server at http://192.0.1.202/dasdec/dasdec.csp.

Network Reset Screen

The EAS device will now be set to new IP address that coincides with your house network. Reset the network settings of the standalone/remote computer back to its original configuration. Now both the EAS device and the standalone/remote computer are on the house network. Type the new EAS devices' IP address into a web browser address bar, enter the new credentials in the Login Screen that appears, and click Login.

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

Chapter 4: Web Interface and Navigation

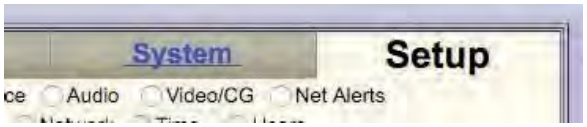
You will communicate with your EAS device by logging into the web interface via a web browser.

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

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

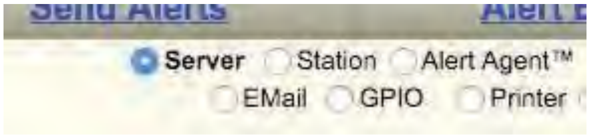
Graphical elements throughout the web interface enable users to navigate the interface and perform operations within the EAS device.

Navigation Tabs



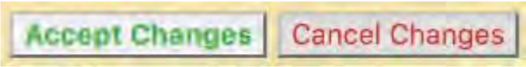
Used to navigate the web interface. Choose the desired section by clicking on the appropriate tab. When active, the tab's background color will be lighter than the other tabs. The interface has both Tabs and Sub Tabs in the Header.

Radio Buttons



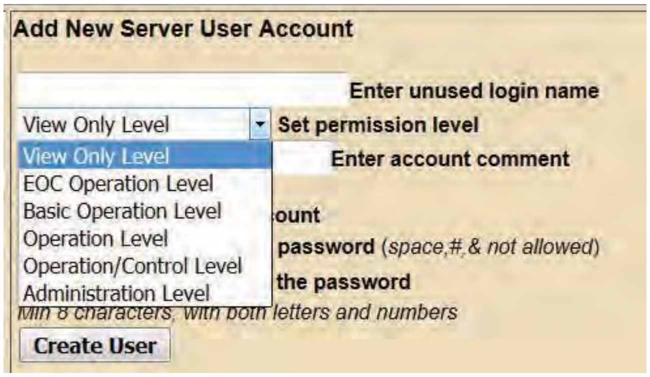
Used to navigate the web interface and report the currently selected item. These buttons are used when there are multiple options; only one radio button can be selected at a time. Clicking in the center of the button activates it. Radio buttons are most commonly used for navigation in the Header, but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

Action Buttons



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

Pull-Down Menus



Add New Server User Account

Enter unused login name

View Only Level ▾ **Set permission level**

- View Only Level
- EOC Operation Level
- Basic Operation Level
- Operation Level
- Operation/Control Level
- Administration Level

Enter account comment

ount

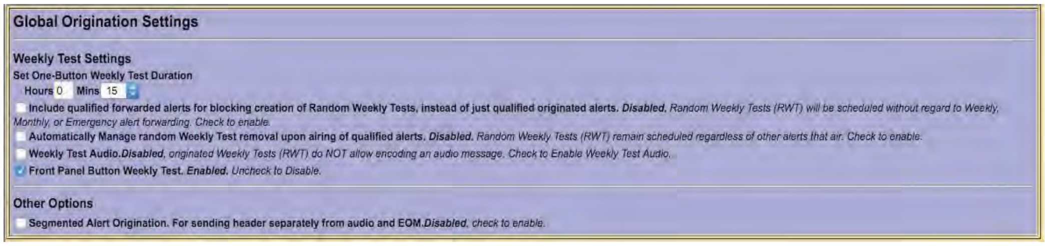
password *(space,# & not allowed)*

the password

Min 8 characters, with both letters and numbers

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

Check Boxes



Global Origination Settings

Weekly Test Settings

Set One-Button Weekly Test Duration

Hours 0 **Mins** 15

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

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

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

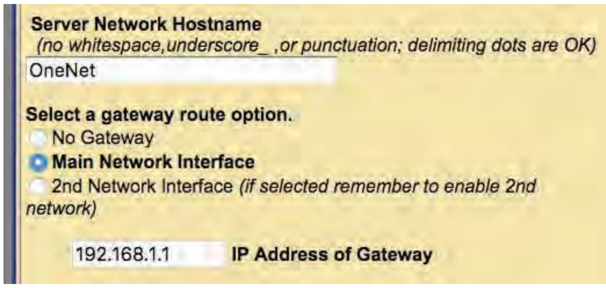
☑ **Front Panel Button Weekly Test.** ***Enabled.*** *Uncheck to Disable.*

Other Options

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

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

Text Fields



Server Network Hostname

(no whitespace,underscore_ ,or punctuation; delimiting dots are OK)

OneNet

Select a gateway route option.

○ No Gateway

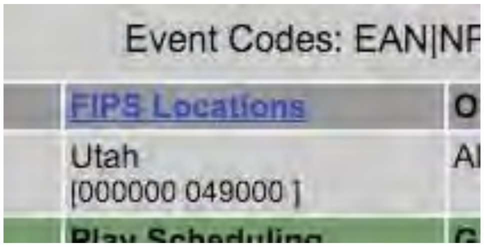
● **Main Network Interface**

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

192.168.1.1 **IP Address of Gateway**

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

Hyperlinks



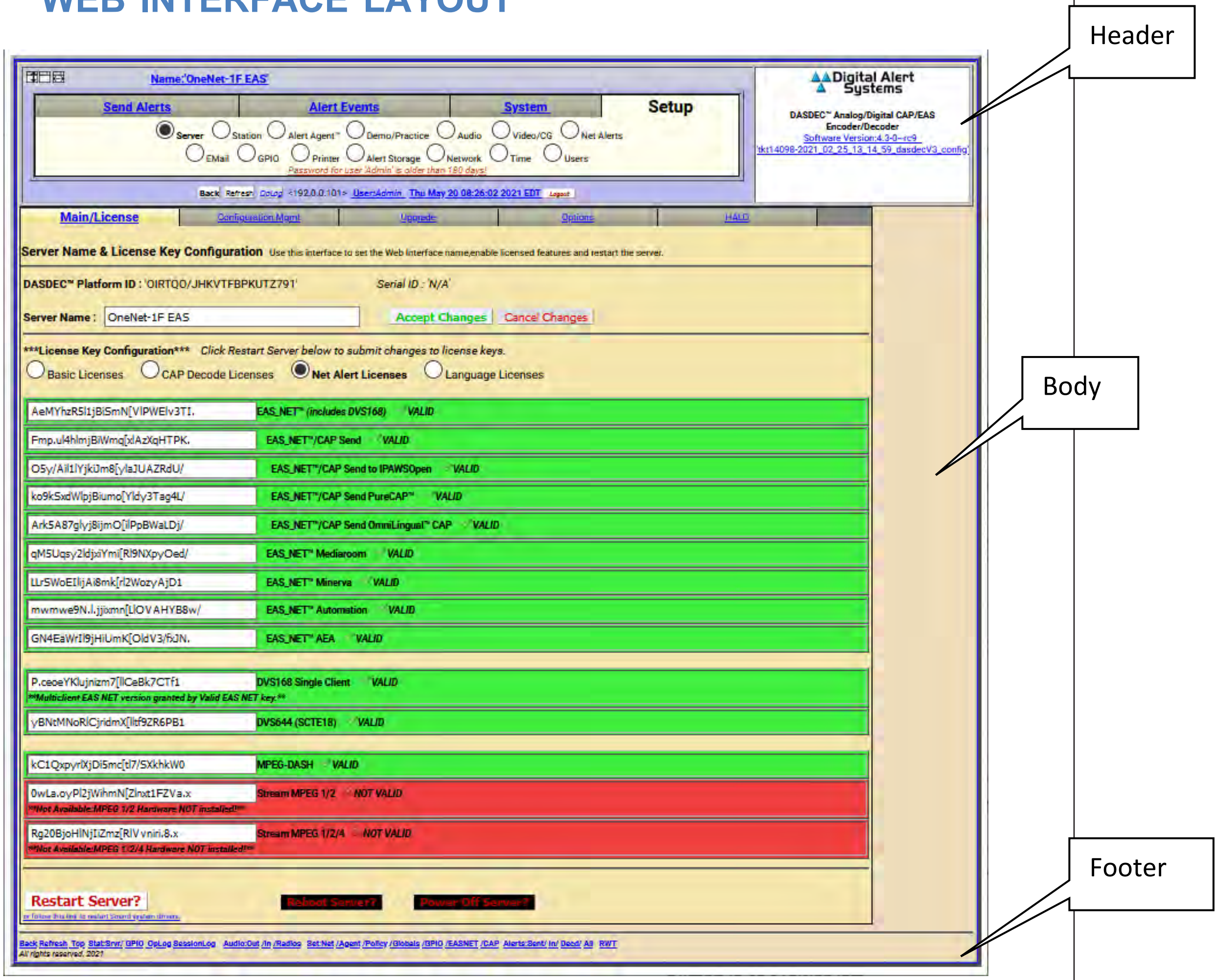
Event Codes: EAN|NF

FIPS Locations

Utah
[000000 049000]

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

WEB INTERFACE LAYOUT



Header
Body
Footer
Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0--rc9
'tkt14098-2021_02_25_13_14_59_dasdecV3_config'
Back
Refresh
OpLog
UserAdmin
Logout
Main/License
Configuration Mgmt
Upgrade
Options
HALO
Accept Changes
Cancel Changes
Restart Server?
or follow this link to restart Sound system drivers.
Reboot Server?
Power Off Server?
Back Refresh Top Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2021

● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users

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

<192.0.0.101> Thu May 20 08:26:02 2021 EDT

Server Name & License Key Configuration Use this interface to set the Web Interface name/enable licensed features and restart the server.

DASDEC™ Platform ID : 'OIRTQO/JHKVTFBPKUTZ791' *Serial ID : 'N/A'*

Server Name : OneNet-1F EAS

*****License Key Configuration***** *Click Restart Server below to submit changes to license keys.*

○ Basic Licenses ○ CAP Decode Licenses ● **Net Alert Licenses** ○ Language Licenses

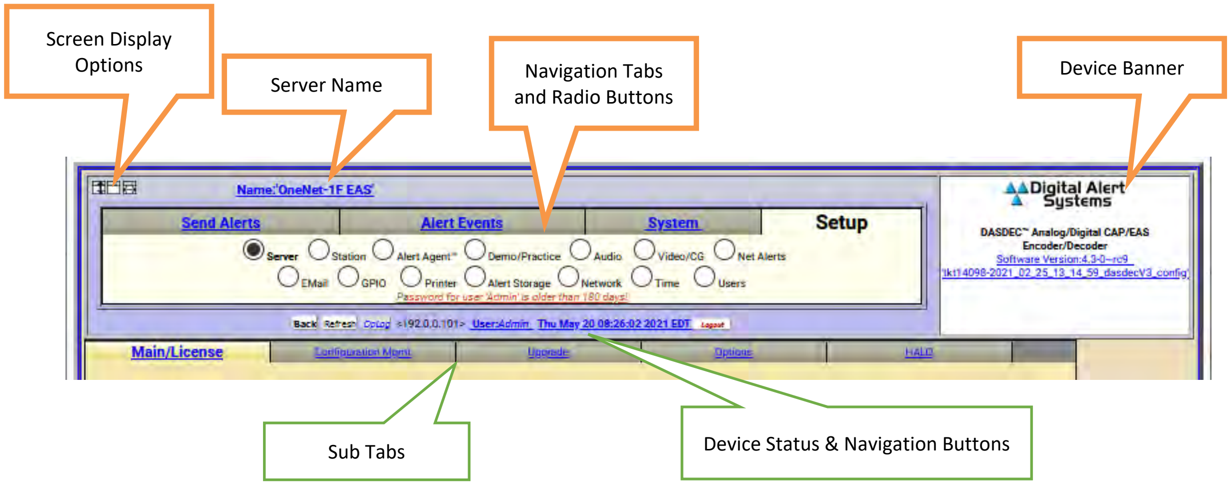
AeMYhzR5l1jBiSmN[VlPWElv3TI.	EAS_NET™ *(includes DVS168)*	*VALID*
Fmp.ul4hlmjBiWmq[xlAzXqHTPK.	EAS_NET™/CAP Send	*VALID*
O5y/Ail1lYjkiJm8[ylaJUAZRdU/	EAS_NET™/CAP Send to IPAWSOpen	*VALID*
ko9kSxdWlpjBiumo[Yldy3Tag4L/	EAS_NET™/CAP Send PureCAP™	*VALID*
Ark5A87glyj8ijmO[ilPpBWaLDj/	EAS_NET™/CAP Send OmniLingual™ CAP	*VALID*
qM5Uqsy2ldjxiYmi[Rl9NXpyOed/	EAS_NET™ Mediaroom	*VALID*
LLrSWoEIlijAi8mk[rl2WozyAjD1	EAS_NET™ Minerva	*VALID*
mwmwe9N.l.jjixmn[LlOVAHYB8w/	EAS_NET™ Automation	*VALID*
GN4EaWrIl9jHiUmK[OldV3/fxJN.	EAS_NET™ AEA	*VALID*
P.ceoeYKlujnizm7[llCeBk7CTf1 ***Multiclient EAS NET version granted by Valid EAS NET key.***	DVS168 Single Client	*VALID*
yBNtMNoRlCjridmX[lltf9ZR6PB1	DVS644 (SCTE18)	*VALID*
kC1QxpyrlXjDi5mc[tl7/SXkhkW0	MPEG-DASH	*VALID*
0wLa.oyPl2jWihmN[Zlnxt1FZVa.x ***Not Available:MPEG 1/2 Hardware NOT installed!***	Stream MPEG 1/2	*NOT VALID*
Rg20BjoHlNjIiZmz[RlVvniri.8.x ***Not Available:MPEG 1/2/4 Hardware NOT installed!***	Stream MPEG 1/2/4	*NOT VALID*

Web Interface Sections

This interface is made up of the following three sections:

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

Header


Screen Display Options
Server Name
Navigation Tabs and Radio Buttons
Device Banner
Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Password for user 'Admin' is older than 180 days!
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0--rc9
1kt14098-2021_02_25_13_14_59_dasdecV3_config
Back Refresh Cptog <192.0.0.101> User:Admin Thu May 20 08:26:02 2021 EDT Logout
Main/License
Configuration Mgmt
Upgrade
Options
HALO
Sub Tabs
Device Status & Navigation Buttons

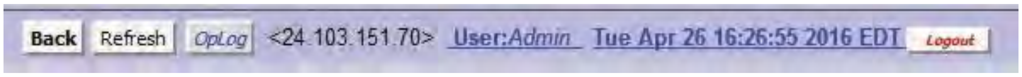
Web Interface - Header Section

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

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

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

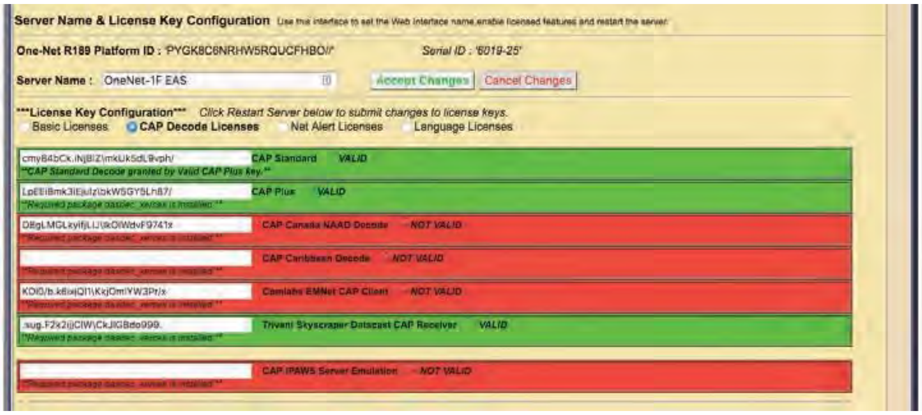
- **Navigation Tabs & Radio Buttons**: The web interface contains dozens of unique screens; they are organized with a system of tabs and radio buttons. The main tabs located across the top of the header are: **Setup**, **System**, Alert Events, and **Send Alerts**. Within each tab are subsections organized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



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

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

Body



Server Name & License Key Configuration Use this interface to set the Web interface name, enable licensed features and restart the server.

One-Net R189 Platform ID : 'PYGK8C6NRHW5RQUCFHBO//' *Serial ID : '6019-25'*

Server Name : OneNet-1F EAS

*****License Key Configuration***** *Click Restart Server below to submit changes to license keys.*

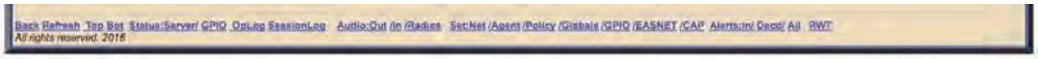
○ Basic Licenses ● **CAP Decode Licenses** ○ Net Alert Licenses ○ Language Licenses

cmyB4bCk.iNjBIZ\mkUk5dL9vph/	CAP Standard	VALID
CAP Standard Decode granted by Valid CAP Plus key.		
LpEEiBmk3IEjulz\bkW5GY5Lh87/	CAP Plus	VALID
Required package dasdec_xercas is installed.		
DBgLMGLkyifjLIJ\kOlWdvF9741x	CAP Canada NAAD Decode	NOT VALID
Required package dasdec_xercas is installed.		
	CAP Caribbean Decode	NOT VALID
Required package dasdec_xercas is installed.		
KDI0/b.k6ixjQI1\KkjOmIYW3Pr/x	Comlabs EMNet CAP Client	NOT VALID
Required package dasdec_xercas is installed.		
.sug.F2x2@CIW\CkJIGBdo999.	Triveni Skyscraper Datacast CAP Receiver	VALID
Required package dasdec_xercas is installed.		
	CAP IPAWS Server Emulation	NOT VALID
Required package dasdec_xercas is installed.		

Web Interface - Body Section

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

Footer



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

Web Interface - Footer Section

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

Navigation:

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

Status:

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

Audio:

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

Set:

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

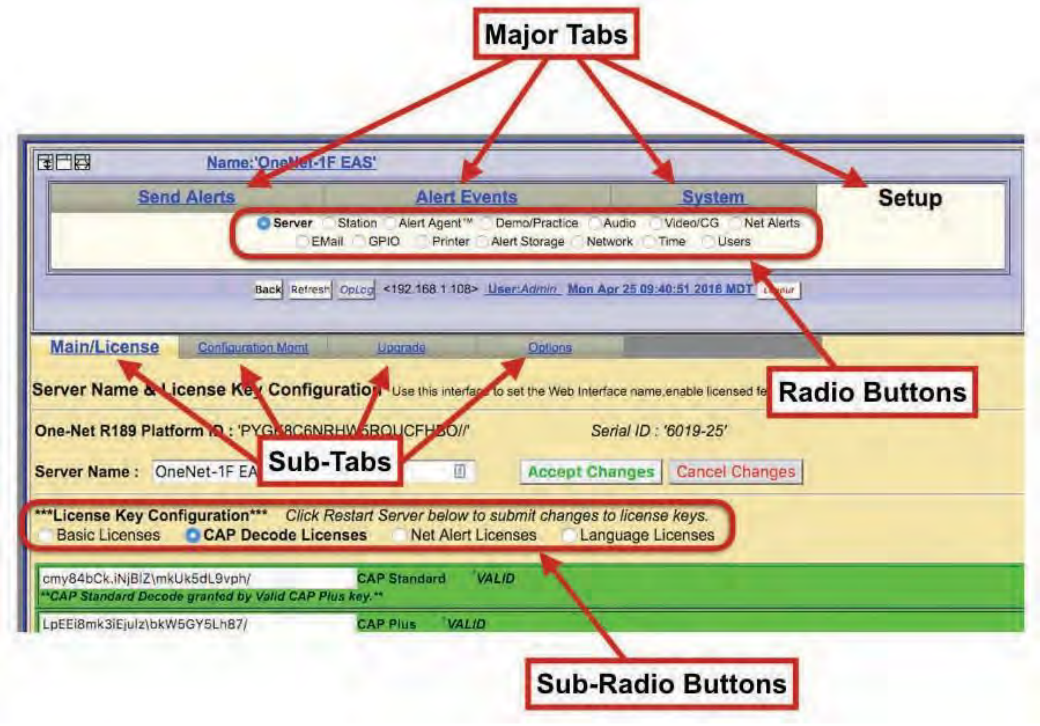
Alerts:

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

WEB INTERFACE NAVIGATION

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

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


Major Tabs
Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Back
Refresh
OpLog
<192.168.1.108>
User:Admin
Mon Apr 25 09:40:51 2016 MDT
Radio Buttons
Main/License
Configuration Mgmt
Upgrade
Options
Sub-Tabs
Accept Changes
Cancel Changes
○ Basic Licenses ● CAP Decode Licenses ○ Net Alert Licenses ○ Language Licenses
Sub-Radio Buttons

Server Name & License Key Configuration Use this interface to set the Web Interface name,enable licensed fe

One-Net R189 Platform ID : 'PYGK8C6NRHW5ROUCFHBO//' Serial ID : '6019-25'

Server Name : OneNet-1F EA

License Key Configuration *Click Restart Server below to submit changes to license keys.*

cmy84bCk.iNjBlZ\mkUk5dL9vph/ CAP Standard *VALID*
CAP Standard Decode granted by Valid CAP Plus key.

LpEEi8mk3iEjulz\bkW5GY5Lh87/ CAP Plus *VALID*

Web Interface Navigation

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

To navigate:

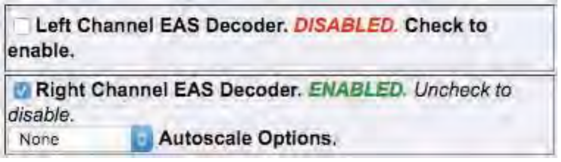
1. Select one of the major tab menus at the top of the header.
2. Select a radio button.
3. If a level of sub-tabbed pages is shown, choose the desired page.

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

HOW TO MAKE CHANGES AND UPDATES

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

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



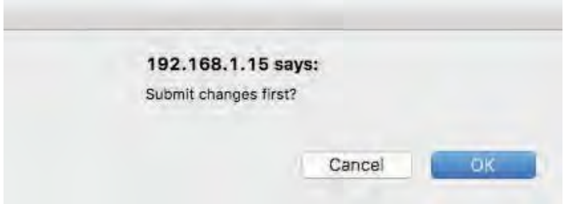
□ Left Channel EAS Decoder. *DISABLED.* Check to enable.

☑ Right Channel EAS Decoder. *ENABLED. Uncheck to disable.*

Pages with an Accept Changes Button

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

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



192.168.1.15 says:

Submit changes first?

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

Pages without an Accept Changes Button

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

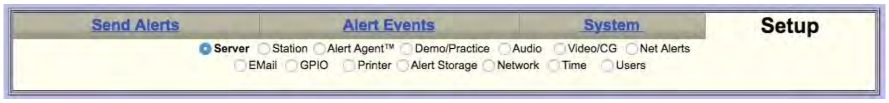
Text Entry Restrictions

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

Illegal HTML Characters: **& < > \ ” ’ `**

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

Chapter 5: Setup Tab

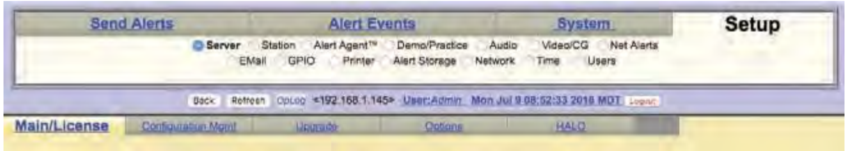


Setup Tab

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

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

SERVER SETUP



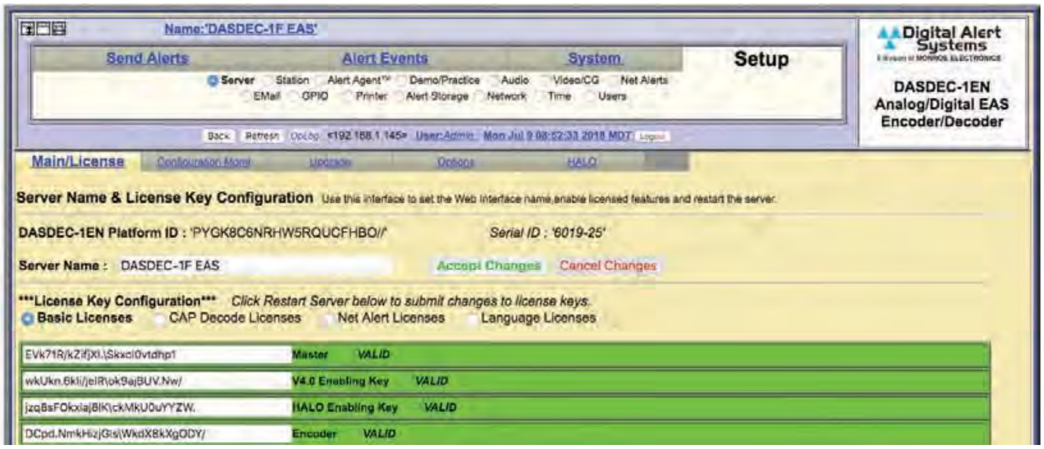
Server Setup Header

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

- Main/License
- Configuration Mgmt
- Upgrade
- Options

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

Main/License: Server Name & License Key Configuration


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Back
Refresh
OpLog
<192.168.1.145>
User:Admin
Mon Jul 9 08:52:33 2018 MDT
Logout
Digital Alert Systems
DASDEC-1EN
Analog/Digital EAS
Encoder/Decoder
Main/License
Configuration Mgmt
Upgrade
Options
HALO
Accept Changes
Cancel Changes
● Basic Licenses ○ CAP Decode Licenses ○ Net Alert Licenses ○ Language Licenses

Server Name & License Key Configuration Use this interface to set the Web Interface name,enable licensed features and restart the server.

DASDEC-1EN Platform ID : 'PYGK8C6NRHW5RQUCFHBO//' *Serial ID : '6019-25'*

Server Name : DASDEC-1F EAS

*****License Key Configuration***** *Click Restart Server below to submit changes to license keys.*

EVk71R/kZifjXI.\Skxcl0vtdhp1	Master	VALID
wkUkn.6kli/jelR\ok9ajBUV.Nw/	V4.0 Enabling Key	VALID
jzq8sFOkxiajBlK\ckMkU0uYYZW.	HALO Enabling Key	VALID
DCpd.NmkHizjGis\WkdX8kXgODY/	Encoder	VALID

Main/License Sub-Tab Screen

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

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

DASDEC II-1EN Platform ID

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

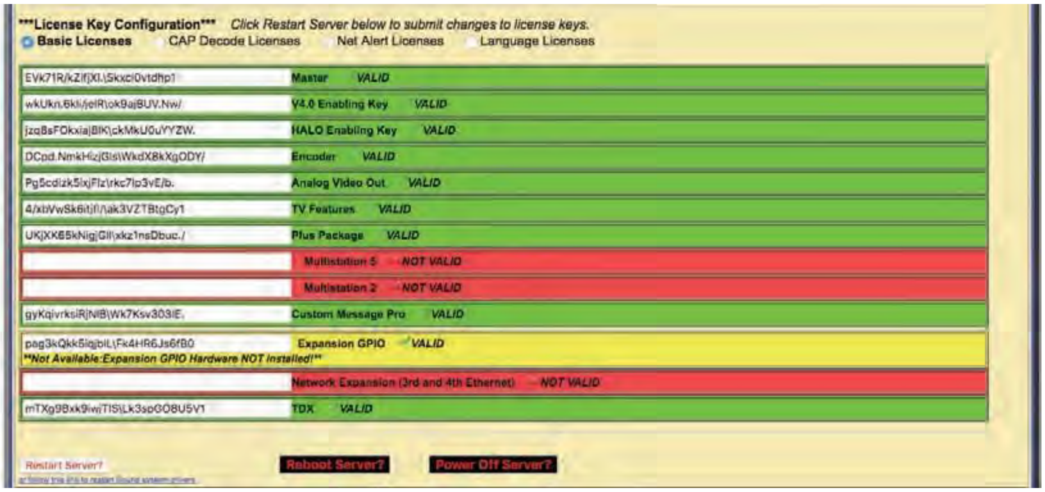
Serial ID

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

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

Server Name

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



License Key Configuration *Click Restart Server below to submit changes to license keys.*

● Basic Licenses ○ CAP Decode Licenses ○ Net Alert Licenses ○ Language Licenses

EVk71R/kZIfjXI.\Skxcl0vtdhp1	Master	VALID
wkUkn.6kli/jelR\ok9ajBUV.Nw/	V4.0 Enabling Key	VALID
jzq8sFOkxiajBIK\ckMkU0uYYZW.	HALO Enabling Key	VALID
DCpd.NmkHizjGls\WkdX8kXgODY/	Encoder	VALID
Pg5cdizk5ixjFlz\rkc7lp3vE/b.	Analog Video Out	VALID
4/xbVwSk6itjfI/\ak3VZTBtgCy1	TV Features	VALID
UKjXK65kNigjGll\xkz1nsDbuc./	Plus Package	VALID
	Multistation 5	NOT VALID
	Multistation 2	NOT VALID
gyKqivrksiRjNIB\Wk7Ksv303IE.	Custom Message Pro	VALID
pag3kQkk5iqjbIL\Fk4HR6Js6fB0 **Not Available:Expansion GPIO Hardware NOT installed!**	Expansion GPIO	VALID
	Network Expansion (3rd and 4th Ethernet)	NOT VALID
mTXg9Bxk9iwjTIS\Lk3spGO8U5V1	TDX	VALID

License Key Configuration Section

License Key Configuration

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

License keys have three different labels:

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

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

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

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

Restart Server?

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

Reboot Server?

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

Power Off Server?

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

Or Follow this Link to restart Sound System drivers

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

Basic Licenses

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

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

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

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

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

New Feature
Support for HALO is new in version 4.0.

License Key	Description
Encoder	A license key for control of the encoder alert origination functionality. A valid Encoder key enables users to configure and use the encoder to run general alert origination. Decoder-only configurations do not need this feature enabled. Decoder only configurations can only issue Weekly tests. The following license keys require a valid Encoder license: • Plus Package • Multistation 2/5 • Custom Messaging • TDX • CAP Canada NAAD Decode • CAP Caribbean Decode • All EAS NET options • DVS168 Single Client • DVS644 (SCTE18) • Streaming MPEG 1/2 & 1/2/4
Analog Video Out	Will enable the video output port for displaying emergency message details as composite NTSC on systems with the necessary hardware. Standard on all One-Net models and DASDEC TV packages (DASLPTV, DASLPTVR, DASTV, DASTVR). Consult factory for more information.
TV Features	This option unlocks support for television specific features, including specific serial port protocols, to support a number of external video display devices. Standard on all DASDEC television models.
Plus Package	This option unlocks support for a set of advanced functions. Together with the TV Features license, certain specific broadcast TV options are enabled, including Manual Forward Text review/edit and network control of Chyron Digibox CODI character generators. • Support for the USB4R232 4-port serial expander 4x serial ports • Front panel audible announcement of decoded alerts • Custom text modification for ORG codes and CGs • Custom message modification allows both text and audio message editing • Live sequencing of manually forwarded alerts • Adds serial support for Chyron Codi and Net CG support for Cayman Graphics™, Chyron™ Intelligent Interface (ChyTV, and Codi Net CG), Compix™ NewsScroll, and Compix AutoCast character generators • Supports Fox Splicer™ (Cisco DCM™)
Multistation 5 **Multistation 2**	When the Plus Package license is enabled, two more options are available for licensing the MultiStation modes. MultiStation-2 supports independent control and management of two program streams from a single DASDEC, while MultiStation-5 supports independent control for up to five program streams from a single DASDEC. Each station will be branded with its own individual station IDs and logging. GPIOs can be set for each stream according to Station ID, FIPS, and/or Event Code. Provides sequential or simultaneous station playout and staggered playout with optional MultiPlayer™.

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

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

More information on network expansion is available on the Digital Alert Systems website: www.digitalalertsystems.com/pdf/exp-3nic_datasheet.pdf EAS_pages/pdf/3-nic_datasheet.pdf.

CAP Decode Licenses

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

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

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

Net Alert Licenses

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

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

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

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

Language Licenses

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

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

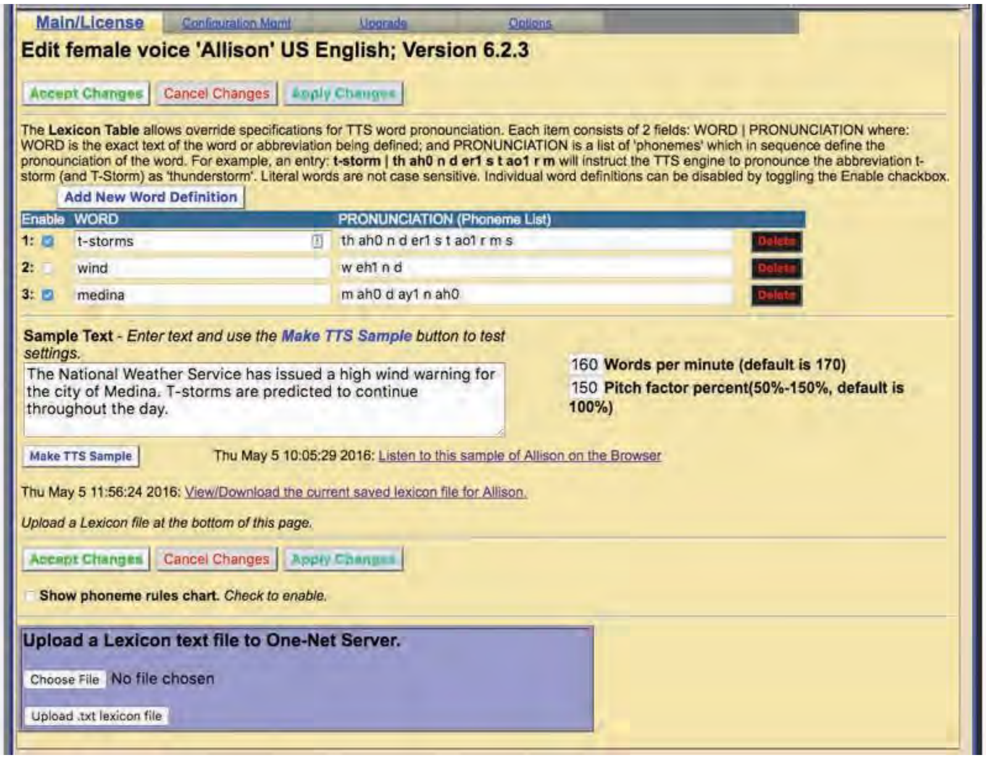
Note
OmniLingual™ Enable Key: Requires appropriate Premium TTS module for proper Text-To-Speech conversion. See Premium Text-To-Speech Options below.

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

Editing Premium Text-To-Speech Voices

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

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



Edit female voice 'Allison' US English; Version 6.2.3

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

Enable	WORD	PRONUNCIATION (Phoneme List)
1: ☑	t-storms	th ah0 n d er1 s t ao1 r m s
2: □	wind	w eh1 n d
3: ☑	medina	m ah0 d ay1 n ah0

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

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

160 **Words per minute (default is 170)**

150 **Pitch factor percent(50%-150%, default is 100%)**

Thu May 5 10:05:29 2016: Listen to this sample of Allison on the Browser

Thu May 5 11:56:24 2016: View/Download the current saved lexicon file for Allison.

Upload a Lexicon file at the bottom of this page.

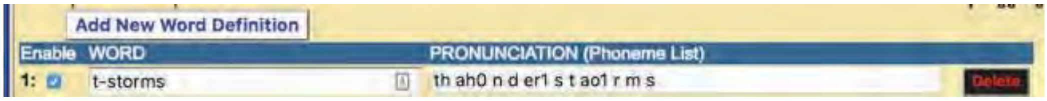
□ **Show phoneme rules chart.** *Check to enable.*

Upload a Lexicon text file to One-Net Server.

No file chosen

Edit Voice Screen

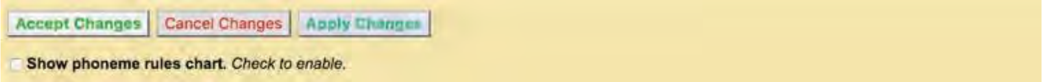
At the top of this screen are three action buttons: **Accept Changes**, **Cancel Changes**, and **Apply Changes**. For convenience purposes, they are replicated farther down the screen. The **Apply Changes** button will activate any changes made within the word definition area, along with the Words per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



Enable	WORD	PRONUNCIATION (Phoneme List)
1: ☑	t-storms	th ah0 n d er1 s t ao1 r m s

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

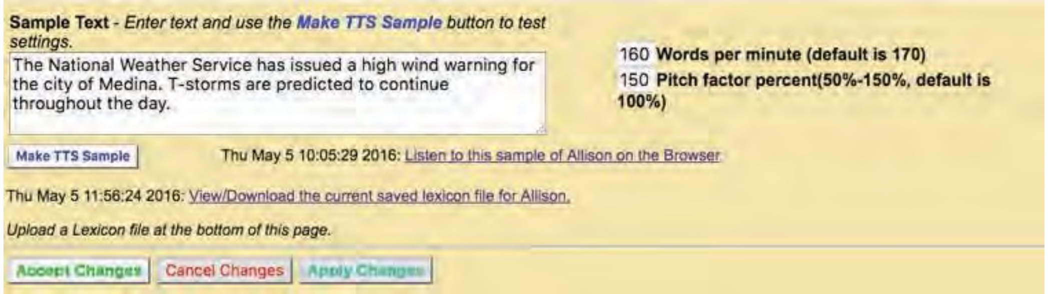
Pronunciations are based on phonemes, the smallest unit of speech used to make one word. A list of phonemes rules is available by clicking the **Show phoneme rules chart** check box towards the bottom of the screen.



□ **Show phoneme rules chart.** *Check to enable.*

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

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



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

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

160 **Words per minute (default is 170)**

150 **Pitch factor percent(50%-150%, default is 100%)**

Thu May 5 10:05:29 2016: Listen to this sample of Allison on the Browser

Thu May 5 11:56:24 2016: View/Download the current saved lexicon file for Allison.

Upload a Lexicon file at the bottom of this page.

Sample Text Section

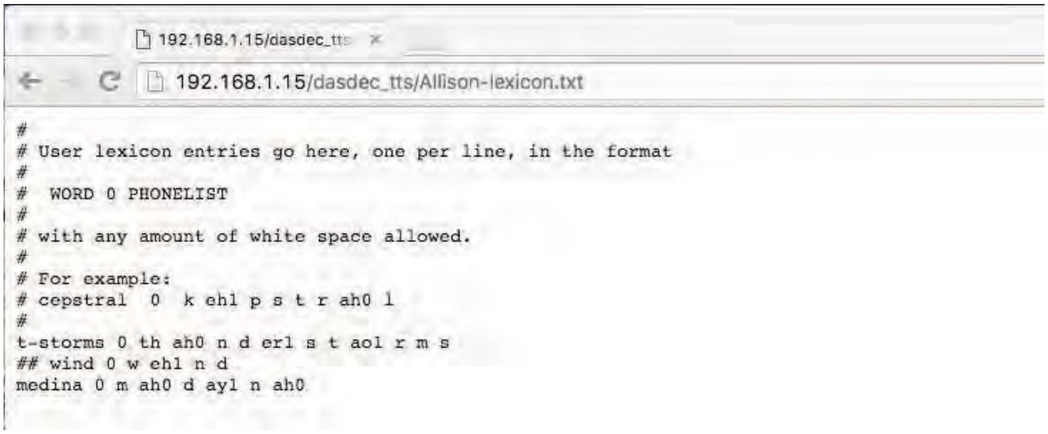
Below the Lexicon Table is the Sample Text section. It is in the section where individual words and sentences can be sampled by the TTS engine. This section also includes the speed and pitch settings for this specific voice, along with saving/viewing the lexicon table files.

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

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

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

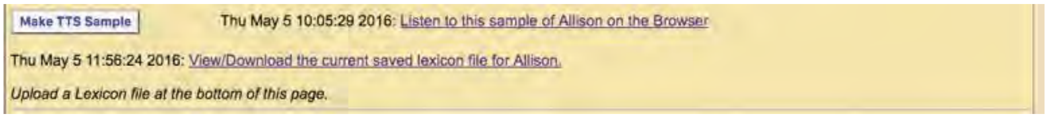
The speed of each Premium Voice can be adjusted by entering a new numeric value into the **Words per minute** text field. The default value is 170. Lower numeric values slow down the voice, and higher values increase its speed. The pitch of each voice can be adjusted with the **Pitch factor percent**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



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

Lexicon Table Text File

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



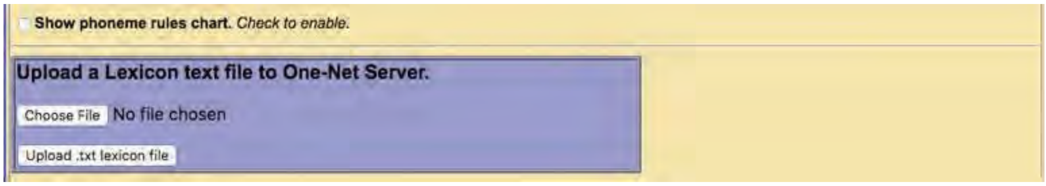
Thu May 5 10:05:29 2016: Listen to this sample of Allison on the Browser

Thu May 5 11:56:24 2016: View/Download the current saved lexicon file for Allison.

Upload a Lexicon file at the bottom of this page.

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

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



□ **Show phoneme rules chart.** *Check to enable.*

Upload a Lexicon text file to One-Net Server.

No file chosen

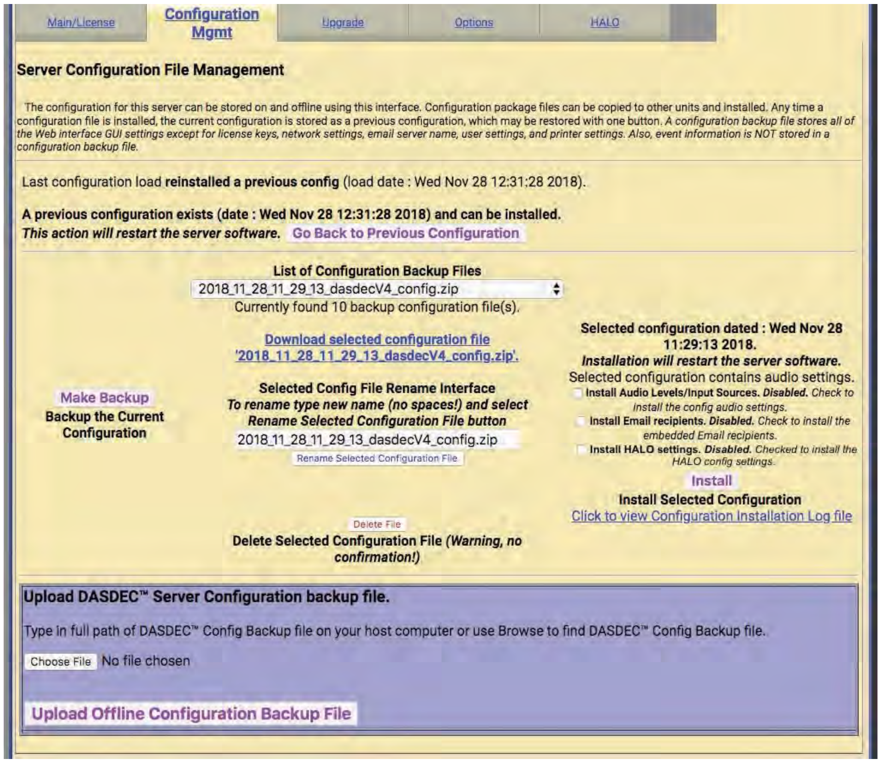
Upload a Lexicon Text File Section

To upload a Lexicon Table text file:

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

Server Configuration File Management

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



Main/License
Configuration Mgmt
Upgrade
Options
HALO
Go Back to Previous Configuration
Make Backup
Rename Selected Configuration File
Delete File
Install
Choose File
Upload Offline Configuration Backup File

Server Configuration File Management

The configuration for this server can be stored on and offline using this interface. Configuration package files can be copied to other units and installed. Any time a configuration file is installed, the current configuration is stored as a previous configuration, which may be restored with one button. *A configuration backup file stores all of the Web interface GUI settings except for license keys, network settings, email server name, user settings, and printer settings. Also, event information is NOT stored in a configuration backup file.*

Last configuration load **reinstalled a previous config** (load date : Wed Nov 28 12:31:28 2018).

A previous configuration exists (date : Wed Nov 28 12:31:28 2018) and can be installed.
This action will restart the server software.

List of Configuration Backup Files
2018_11_28_11_29_13_dasdecV4_config.zip
Currently found 10 backup configuration file(s).

Download selected configuration file '2018_11_28_11_29_13_dasdecV4_config.zip'.

Backup the Current Configuration

Selected Config File Rename Interface
To rename type new name (no spaces!) and select Rename Selected Configuration File button
2018_11_28_11_29_13_dasdecV4_config.zip

Delete Selected Configuration File *(Warning, no confirmation!)*

Selected configuration dated : Wed Nov 28 11:29:13 2018.
Installation will restart the server software.
Selected configuration contains audio settings.
□ **Install Audio Levels/Input Sources. *Disabled.*** *Check to install the config audio settings.*
□ **Install Email recipients. *Disabled.*** *Check to install the embedded Email recipients.*
□ **Install HALO settings. *Disabled.*** *Checked to install the HALO config settings.*

Install Selected Configuration
Click to view Configuration Installation Log file

Upload DASDEC™ Server Configuration backup file.

Type in full path of DASDEC™ Config Backup file on your host computer or use Browse to find DASDEC™ Config Backup file.

No file chosen

Server Configuration File Management Screen

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

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

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

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

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

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

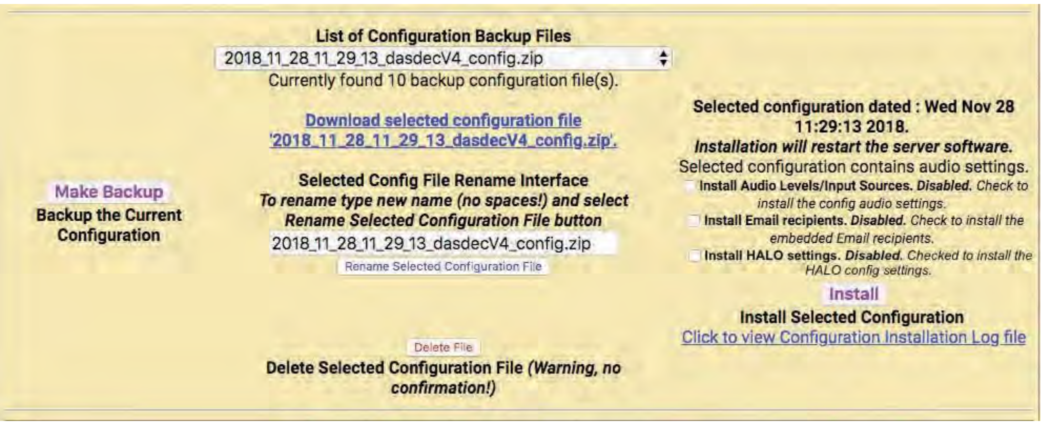
Software upgrades result in the creation of a configuration update file. This serves as a precaution in the rare event that an upgrade mangles an existing configuration. It can be used to attempt to restore settings to the pre-update state.

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

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

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

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



Backup the Current Configuration

List of Configuration Backup Files

2018_11_28_11_29_13_dasdecV4_config.zip

Currently found 10 backup configuration file(s).

Download selected configuration file '2018_11_28_11_29_13_dasdecV4_config.zip'.

Selected Config File Rename Interface
To rename type new name (no spaces!) and select Rename Selected Configuration File button

2018_11_28_11_29_13_dasdecV4_config.zip

Delete Selected Configuration File *(Warning, no confirmation!)*

Selected configuration dated : Wed Nov 28 11:29:13 2018.
Installation will restart the server software.
Selected configuration contains audio settings.

☐ **Install Audio Levels/Input Sources. *Disabled.*** *Check to install the config audio settings.*

☐ **Install Email recipients. *Disabled.*** *Check to install the embedded Email recipients.*

☐ **Install HALO settings. *Disabled.*** *Checked to install the HALO config settings.*

Install Selected Configuration

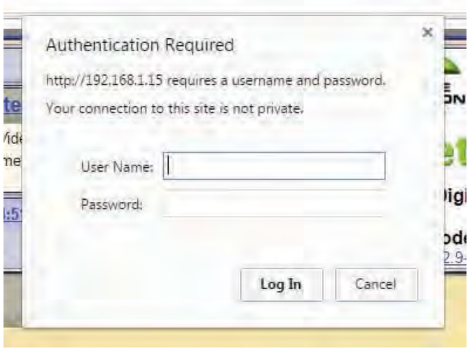
Click to view Configuration Installation Log file

Configuration Backup File Section

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

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

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



Authentication Required

http://192.168.1.15 requires a username and password.

Your connection to this site is not private.

Authentication Prompt

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

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

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

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

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

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

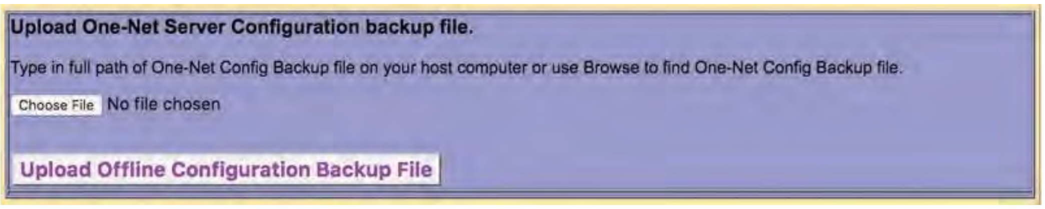
E-mail recipients include (found on the **EMail Server** sub-tab screen):

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

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

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

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


Upload One-Net Server Configuration backup file.

Type in full path of One-Net Config Backup file on your host computer or use Browse to find One-Net Config Backup file.

Upload Server Configuration Backup File Section

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

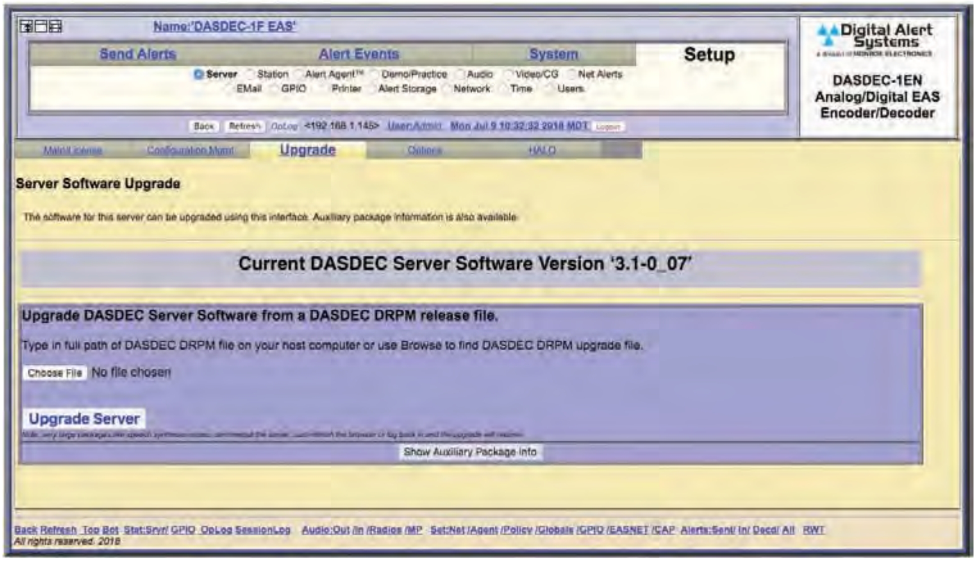
Caution
Installing V3 configuration files (created when running version 3.x software) will overwrite the HALO settings. Make sure to NOT check the **Install HALO settings** checkbox if installing a V3 configuration and HALO is licensed.

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

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

Upgrade: Server Software Upgrade

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


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
Digital Alert Systems
DASDEC-1EN
Analog/Digital EAS
Encoder/Decoder
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Back
Refresh
OpLog
<192.168.1.145>
User:Admin
Mon Jul 9 10:32:32 2018 MDT
Logout
Main License
Configuration Mgmt
Upgrade
Options
HALO
Choose File
Upgrade Server
Show Auxiliary Package Info
Back Refresh Top Bot Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios /MP Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT

Server Software Upgrade

The software for this server can be upgraded using this interface. Auxiliary package information is also available.

Current DASDEC Server Software Version '3.1-0_07'

Upgrade DASDEC Server Software from a DASDEC DRPM release file.

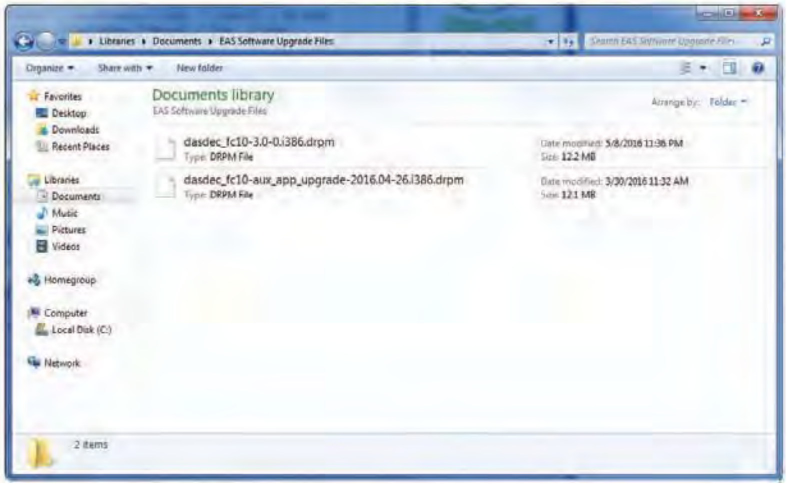
Type in full path of DASDEC DRPM file on your host computer or use Browse to find DASDEC DRPM upgrade file.

No file chosen

All rights reserved. 2018

Server Software Upgrade Screen

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



dasdec_fc10-3.0-0.i386.drpm
Type: DRPM File
Date modified: 5/8/2016 11:36 PM
Size: 12.2 MB

dasdec_fc10-aux_app_upgrade-2016.04-26.i386.drpm
Type: DRPM File
Date modified: 3/30/2016 11:32 AM
Size: 12.1 MB

2 items

Choose File - Windows Explorer

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

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

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

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

To perform a server software upgrade:

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

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

Version 4.0 Specific Upgrade Instructions

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

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

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

In preparation for the V4.0 upgrade:

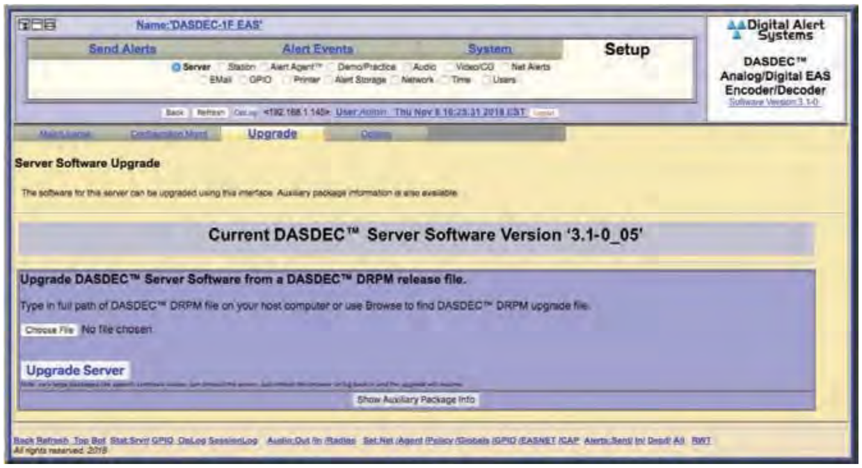
- Confirm the EAS device is 2nd generation hardware — DASDEC-III or One-Net SE
- Verify the EAS device is running V3.x software or higher *(if not, contact customer support)*
- Obtain a valid V4.0 Enabling Key for the specific device
- Download the file ***DAS_Upgrader.drpm*** from the Digital Alert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

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

1. Load the initial DRPM File

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

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


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Back
Refresh
<192.168.1.145>
User:Admin Thu Nov 8 16:25:31 2018 CST
Digital Alert Systems
DASDEC™
Analog/Digital EAS
Encoder/Decoder
Software Version 3.1-0
Upgrade
Choose File
Upgrade Server
Show Auxiliary Package Info
Back Refresh Top Bot Stat:Srvr/ GPIO DaLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2018

Server Software Upgrade

The software for this server can be upgraded using this interface. Auxiliary package information is also available.

Current DASDEC™ Server Software Version '3.1-0_05'

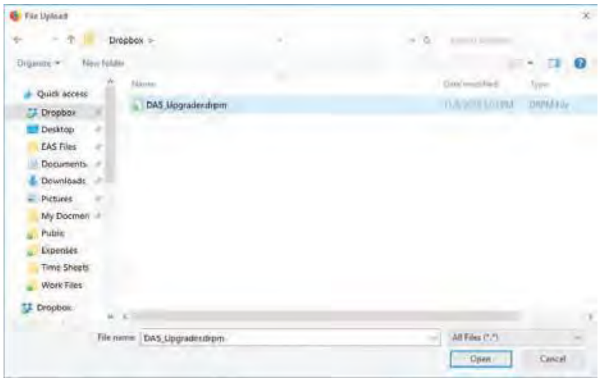
Upgrade DASDEC™ Server Software from a DASDEC™ DRPM release file.

Type in full path of DASDEC™ DRPM file on your host computer or use Browse to find DASDEC™ DRPM upgrade file.

Choose File No file chosen

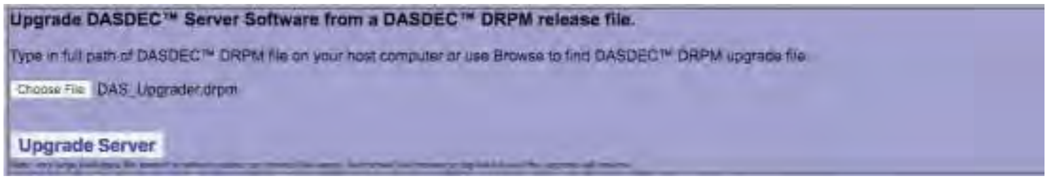
Server Software Upgrade Screen (DASDEC version example)

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



Choose File - Windows Explorer

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



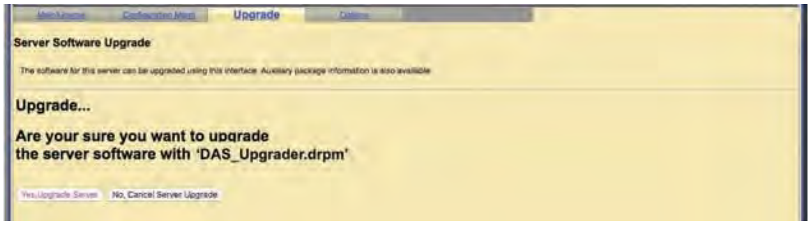
Upgrade DASDEC™ Server Software from a DASDEC™ DRPM release file.

Type in full path of DASDEC™ DRPM file on your host computer or use Browse to find DASDEC™ DRPM upgrade file.

Choose File DAS_Upgrader.drpm

Server Software Upgrade Screen with proper file selected

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



Server Software Upgrade

The software for this server can be upgraded using this interface. Auxiliary package information is also available

Upgrade...

Are your sure you want to upgrade
the server software with 'DAS_Upgrader.drpm'

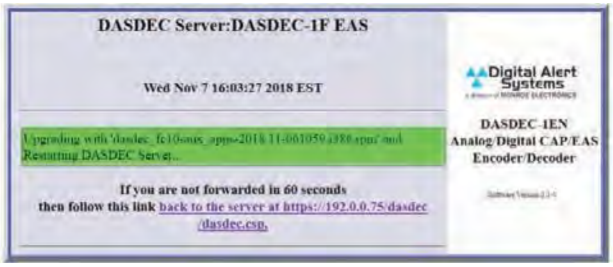
Upgrade - Confirmation Screen

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

Note
Intructions to backup the current configuration settings are found in the Server Configuration Management section. Use the Backing Up EAS Event Log instructions in Section 6 of this manual.

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

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



DASDEC Server:DASDEC-1F EAS

Wed Nov 7 16:03:27 2018 EST

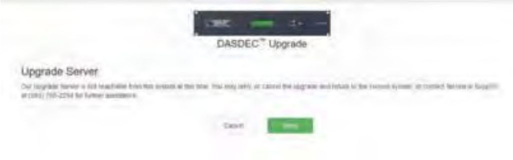
Upgrading with 'dasdec_fc10snx_apps-2018.11-001059.i386.rpm' and Restarting DASDEC Server...

If you are not forwarded in 60 seconds
then follow this link back to the server at https://192.0.0.75/dasdec/dasdec.csp.

Initial Upgrading... Screen

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

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



Upgrade Server

[illegible]

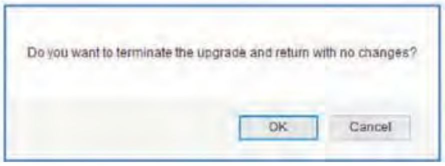
Upgrade Retry Screen

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

Proceed to Step 2.

Welcome to the 4.0 Software Upgrade Screen

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



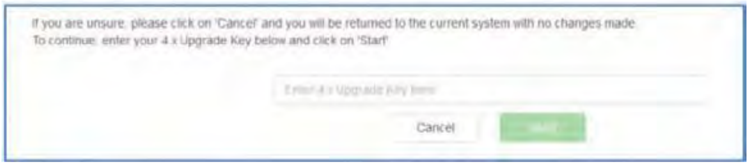
Do you want to terminate the upgrade and return with no changes?

Cancel Confirmation Dialog Box

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

2. Upgrade the DASDEC/One-Net Device

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

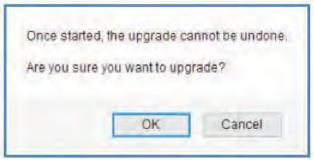


If you are unsure, please click on 'Cancel' and you will be returned to the current system with no changes made
To continue, enter your 4.x Upgrade Key below and click on 'Start'

‘Enter 4.x Upgrade Key here’ Text Box

2.1. Locate the V4.0 Enabling Key for the EAS device and enter it into the text box. Note: it’s typically easiest to cut & paste the key from the email. Be sure to include all characters. If the key is improperly entered it can be corrected in the verification steps after installation is completed.

2.2. Click the **Start** button to proceed and the upgrade confirmation dialog box will appear on the screen.



Once started, the upgrade cannot be undone.

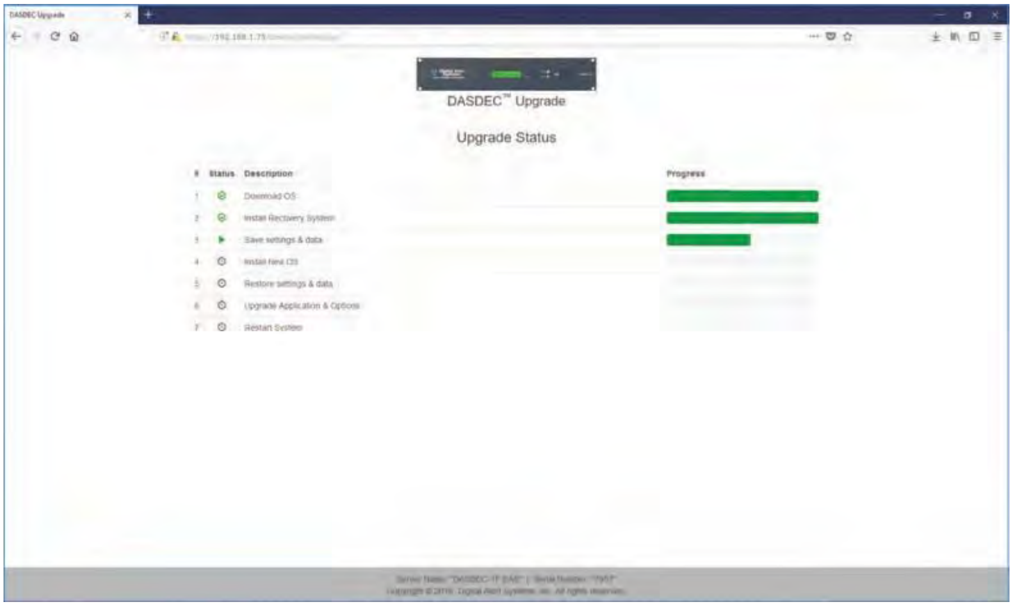
Are you sure you want to upgrade?

Upgrade Confirmation Dialog Box

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

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

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



DASDEC™ Upgrade

Upgrade Status

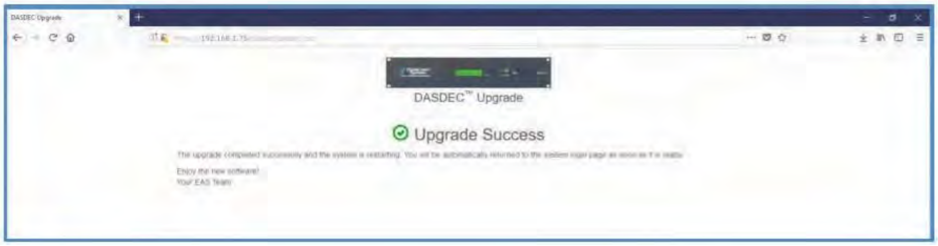
#	Status	Description	Progress
1	✓	Download OS	🟩🟩🟩🟩
2	✓	Install Recovery System	🟩🟩🟩🟩
3	▶	Save settings & data	🟩🟩
4	○	Install New OS	
5	○	Restore settings & data	
6	○	Upgrade Application & Options	
7	○	Restart System	

V4.0 Upgrade Status Screen

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

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

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



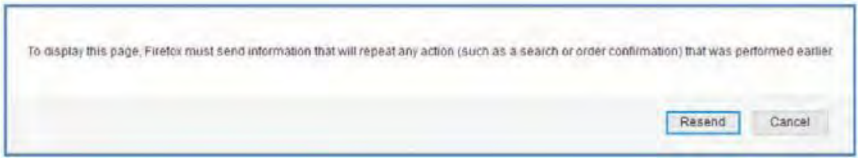
Upgrade Success

The upgrade completed successfully and the system is restarting. You will be automatically returned to the system login page as soon as it is ready.

Enjoy the new software!
Your EAS Team

Upgrade Success Screen

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

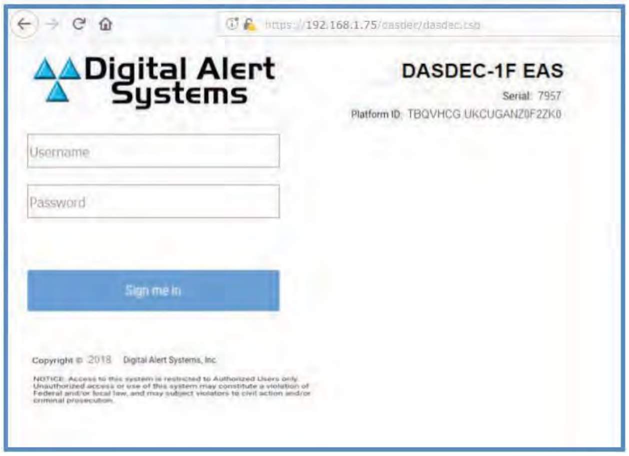


To display this page, Firefox must send information that will repeat any action (such as a search or order confirmation) that was performed earlier.

Resend Information Dialog Box

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

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



DASDEC-1F EAS

Serial: 7957

Platform ID: TBQVHCG UKCUGANZ0F2ZK0

Copyright © 2018 Digital Alert Systems, Inc

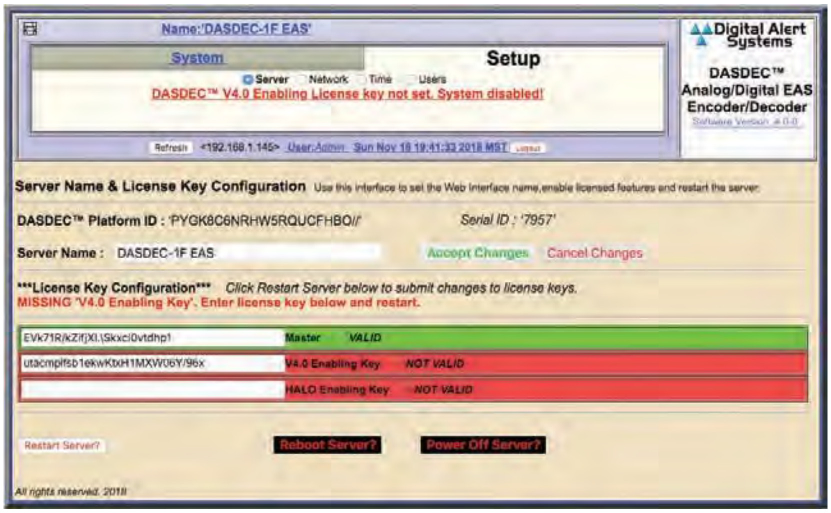
NOTICE: Access to this system is restricted to Authorized Users only. Unauthorized access or use of this system may constitute a violation of Federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

V4.0 Login Screen

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

3.1. Log into the EAS device as usual.

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



DASDEC™ V4.0 Enabling License key not set. System disabled!

<192.168.1.145> User:Admin Sun Nov 18 19:41:33 2018 MST

Server Name & License Key Configuration Use this interface to set the Web Interface name,enable licensed features and restart the server.

DASDEC™ Platform ID : 'PYGK8C6NRHW5RQUCFHBO//' Serial ID : '7957'

Server Name : DASDEC-1F EAS

License Key Configuration Click Restart Server below to submit changes to license keys.
MISSING 'V4.0 Enabling Key'. Enter license key below and restart.

EVk71R/kZifjXI.\Skxci0vtdhp1	Master	VALID
utacmplfsb1ekwKtxH1MXW06Y/96x	V4.0 Enabling Key	NOT VALID
	HALO Enabling Key	NOT VALID

All rights reserved. 2018

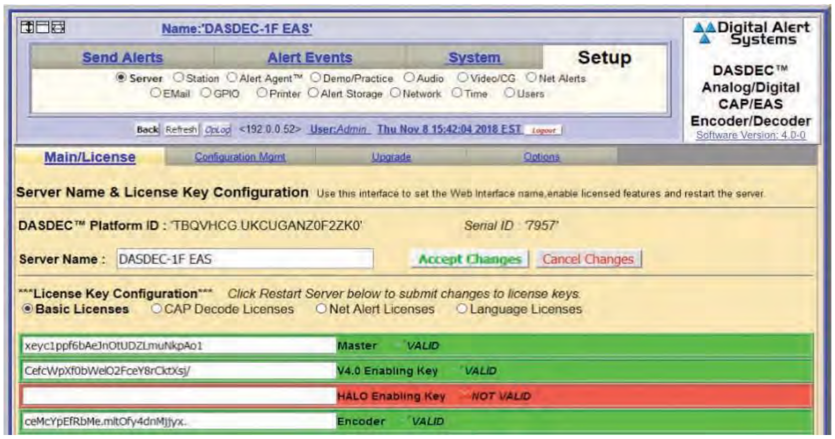
Setup > Server > Main/License screen with example of an invalid V4.0 Enabling

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

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

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

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


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version: 4.0-0
Back
Refresh
OpLog
Logout
Main/License
Configuration Mgmt
Upgrade
Options
Accept Changes
Cancel Changes

<192.0.0.52> User:Admin Thu Nov 8 15:42:04 2018 EST

Server Name & License Key Configuration Use this interface to set the Web Interface name,enable licensed features and restart the server.

DASDEC™ Platform ID : 'TBQVHCG.UKCUGANZ0F2ZK0' Serial ID : '7957'

Server Name : DASDEC-1F EAS

License Key Configuration Click Restart Server below to submit changes to license keys.
● Basic Licenses ○ CAP Decode Licenses ○ Net Alert Licenses ○ Language Licenses

xeyc1ppf6bAeJnOtUDZLmuNkpAo1	Master	VALID
CefcWpXf0bWelO2FceY8rCktXsj/	V4.0 Enabling Key	VALID
	HALO Enabling Key	NOT VALID
ceMcYpEfRbMe.mltOfy4dnMjjyx.	Encoder	VALID

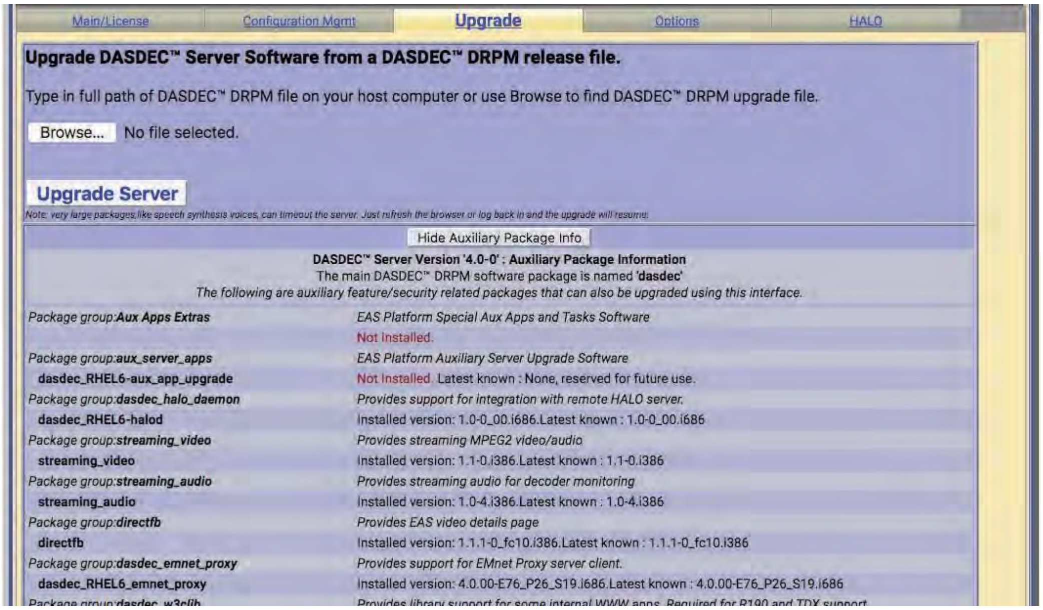
Setup > Server > Main/License screen example showing a valid V4.0 Enabling Key

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

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

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

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



Upgrade DASDEC™ Server Software from a DASDEC™ DRPM release file.

Type in full path of DASDEC™ DRPM file on your host computer or use Browse to find DASDEC™ DRPM upgrade file.

No file selected.

Note: very large packages,like speech synthesis voices, can timeout the server. Just refresh the browser or log back in and the upgrade will resume.

DASDEC™ Server Version '4.0-0' : Auxiliary Package Information

The main DASDEC™ DRPM software package is named **'dasdec'**

The following are auxiliary feature/security related packages that can also be upgraded using this interface.

*Package group:***Aux Apps Extras**	*EAS Platform Special Aux Apps and Tasks Software*
	Not Installed.
*Package group:***aux_server_apps**	*EAS Platform Auxiliary Server Upgrade Software*
dasdec_RHEL6-aux_app_upgrade	Not Installed. Latest known : None, reserved for future use.
*Package group:***dasdec_halo_daemon**	*Provides support for integration with remote HALO server.*
dasdec_RHEL6-halod	Installed version: 1.0-0_00.i686.Latest known : 1.0-0_00.i686
*Package group:***streaming_video**	*Provides streaming MPEG2 video/audio*
streaming_video	Installed version: 1.1-0.i386.Latest known : 1.1-0.i386
*Package group:***streaming_audio**	*Provides streaming audio for decoder monitoring*
streaming_audio	Installed version: 1.0-4.i386.Latest known : 1.0-4.i386
*Package group:***directfb**	*Provides EAS video details page*
directfb	Installed version: 1.1.1-0_fc10.i386.Latest known : 1.1.1-0_fc10.i386
*Package group:***dasdec_emnet_proxy**	*Provides support for EMnet Proxy server client.*
dasdec_RHEL6_emnet_proxy	Installed version: 4.0.00-E76_P26_S19.i686.Latest known : 4.0.00-E76_P26_S19.i686
*Package group:***dasdec_w3clib**	*Provides library support for some internal WWW apps. Required for R190 and TDX support.*

Auxiliary Package Info Session

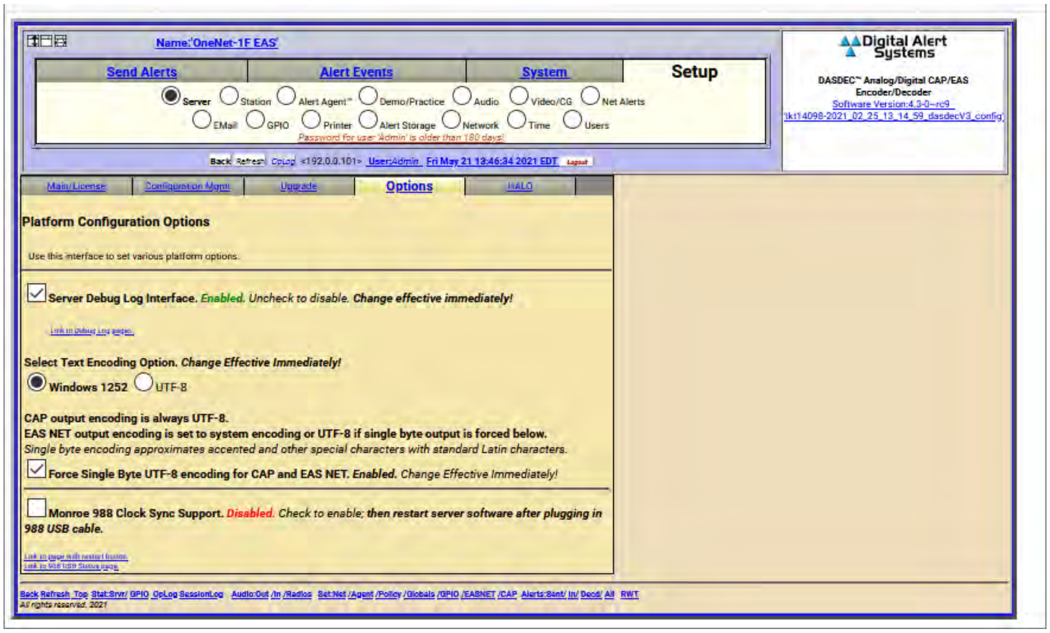
This expanded view also includes a special **Rebuild RPM Package Database** button for repairing the internal package database. Use this button to repair the RPM package database in case of package installation failure due to RPM database corruption. This command should rarely, if ever, be needed, and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

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

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

Options: Platform Configurations Options

The **Setup > Server > Options** screen is designed to interface with various platform options. These include enabling debug logging, USB port speed, text encoding, and CAPoutput encoding.


Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Password for user 'Admin' is older than 180 days!
Back Refresh OpLog <192.0.0.101> User:Admin Fri May 21 13:46:34 2021 EDT Logout
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0~rc9
'lkt14098-2021_02_25_13_14_59_dasdecV3_config'
Main/License
Configuration Mgmt
Upgrade
Options
HALO
Back Refresh Top Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2021

Platform Configuration Options

Use this interface to set various platform options.

☑ **Server Debug Log Interface.** *Enabled. Uncheck to disable.* ***Change effective immediately!***

Link to Debug Log pages.

Select Text Encoding Option. ***Change Effective Immediately!***

● **Windows 1252** ○ UTF-8

CAP output encoding is always UTF-8.
EAS NET output encoding is set to system encoding or UTF-8 if single byte output is forced below.
Single byte encoding approximates accented and other special characters with standard Latin characters.

☑ **Force Single Byte UTF-8 encoding for CAP and EAS NET.** ***Enabled.*** *Change Effective Immediately!*

□ **Monroe 988 Clock Sync Support.** *Disabled. Check to enable;* ***then restart server software after plugging in 988 USB cable.***

Link to page with restart button.
Link to 988 USB Status page.

Platform Configuration Options Screen

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

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

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

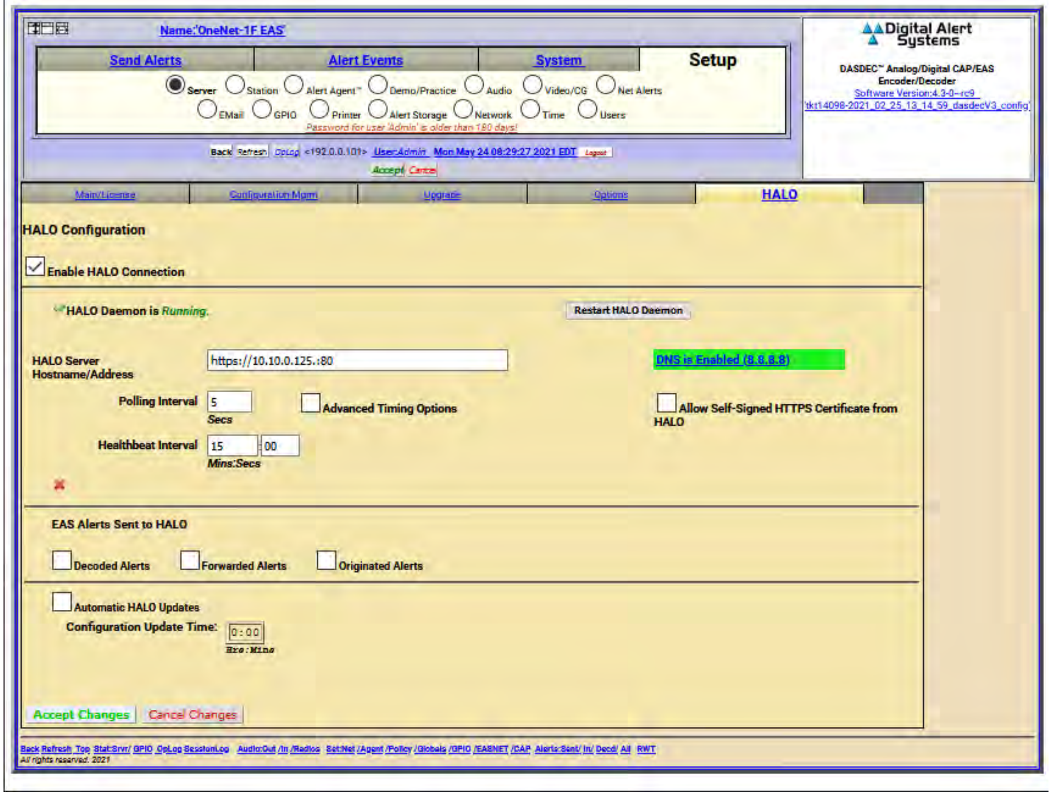
Note
The Server Debug Log Interface feature is typically used by and under the direction of a qualified customer service engineer. Do not turn this feature on unless directed by a Digital Alert Systems customer service engineer.

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

HALO Configuration

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

New Feature
Version 4.0 introduces support for HALO - the industries first Enterprise-Level EAS Management System. Additional information on HALO is found at the Digital Alert Systems website.


Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
● Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Password for user 'Admin' is older than 180 days!
Back Refresh OpLog <192.0.0.101> User:Admin Mon May 24 08:29:27 2021 EDT Logout
Accept Cancel
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0-rc9
'tkt14098-2021_02_25_13_14_59_dasdecV3_config'
Main/License
Configuration Mgmt
Upgrade
Options
HALO
Restart HALO Daemon
Accept Changes
Cancel Changes
Back Refresh Top Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2021

HALO Configuration

☑ Enable HALO Connection

HALO Daemon is *Running*.

HALO Server Hostname/Address: https://10.10.0.125.:80

DNS is Enabled (8.8.8.8)

Polling Interval: 5 Secs

□ Advanced Timing Options

□ Allow Self-Signed HTTPS Certificate from HALO

Healthbeat Interval: 15 : 00 Mins:Secs

EAS Alerts Sent to HALO

□ Decoded Alerts □ Forwarded Alerts □ Originated Alerts

□ Automatic HALO Updates

Configuration Update Time: 0:00 Hrs:Mins

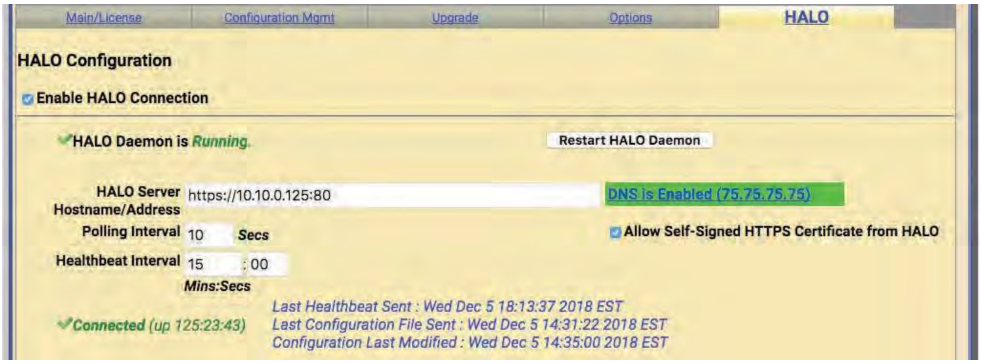
HALO Configuration Screen

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

HALO Connection Section

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

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



HALO Configuration

☑ Enable HALO Connection

✓HALO Daemon is *Running*.

HALO Server Hostname/Address: https://10.10.0.125:80 — DNS is Enabled (75.75.75.75)

Polling Interval: 10 *Secs*

☑ Allow Self-Signed HTTPS Certificate from HALO

Healthbeat Interval: 15 : 00 *Mins:Secs*

✓*Connected (up 125:23:43)*

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

HALO Sub-Tab - HALO Connection Section

Enable HALO Connection check box

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

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

HALO Daemon Status

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

Restart HALO Daemon

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

HALO Server Hostname / Address

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

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

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

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

Allow Self-Signed HTTPS Certificate from HALO

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

Polling Interval

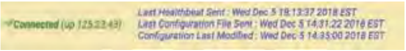
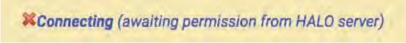
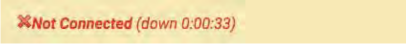
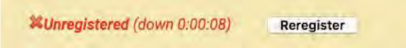
Each EAS device reaches out to the HALO server using the frequency set by this Polling Interval. This value can range from 2 to 120 seconds. The default value is 10 seconds.

Healthbeat Interval

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

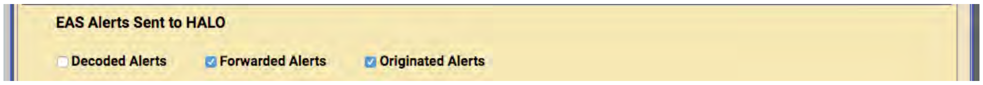
Connection Status

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

Connection Status	Description
Connected  ✓Connected (up 125:23:43) Last Healthbeat Sent : Wed Dec 5 19:13:37 2018 EST Last Configuration File Sent : Wed Dec 5 14:31:22 2018 EST Configuration Last Modified : Wed Dec 5 14:35:00 2018 EST	This status will display a check mark, status text and the ‘up’ time for this connection in a green color. To the right of this status are three date/ time values for the following: Last Healthbeat Sent Last Configuration File Sent Configuration Last Modified
Connecting (awaiting permission from HALO server)  ✖Connecting (awaiting permission from HALO server)	The EAS device has successfully made contact with the HALO server and is awaiting permission to be added to HALO. This device will show up in the HALO interface in the left pane - Queued tab.
Not Connected  ✖Not Connected (down 0:00:33)	This status is displayed for one of two reasons: no connection has been established to the HALO server OR the established connection has been broken. When a connection has been broken there will be additional text displaying the amount of time the connection has been lost.
Unregistered  ✖Unregistered (down 0:00:08) 	The EAS device has been removed from HALO by an authorized user. The amount of time the device has been unregistered is displayed to the right of the status. The device is no longer communicating with HALO. To reregister the device with HALO, click the **Reregister** button. The device will again be available in the Queued tab of HALO.

EAS Alerts Section

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



EAS Alerts Sent to HALO

□ Decoded Alerts ☑ Forwarded Alerts ☑ Originated Alerts

HALO Sub-Tab - EAS Alerts Section

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

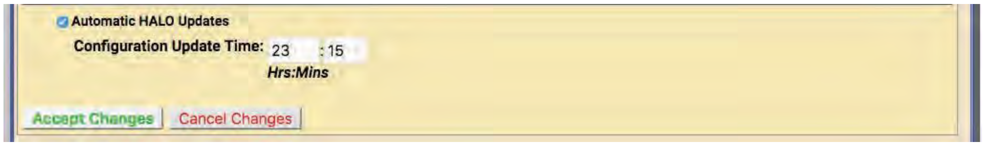
- Decoded Alerts
- Forwarded Alerts
- Originated Alerts

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

Automatic HALO Updates Section

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

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



☑ Automatic HALO Updates

Configuration Update Time: 23 : 15

Hrs:Mins

HALO Sub-Tab - Automatic HALO Updates Section

Automatic HALO Updates check box

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

Configuration Update Time

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

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

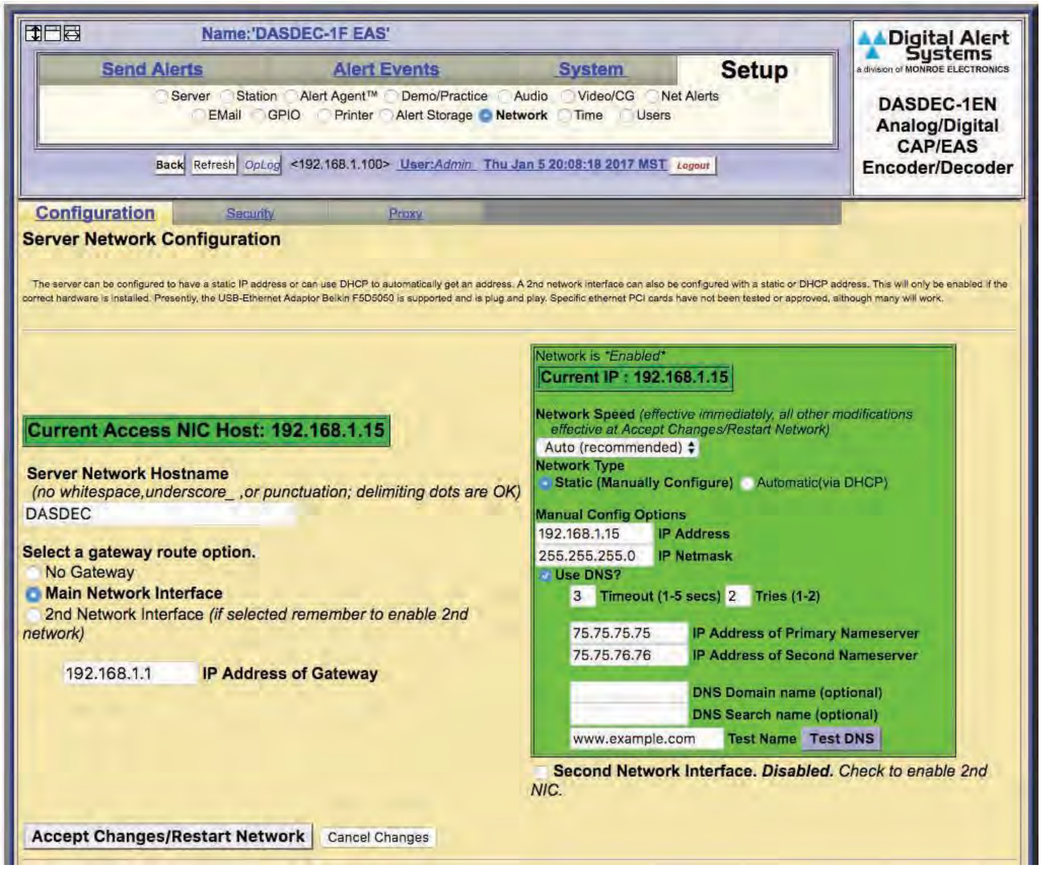
Note

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

NETWORK SETUP

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

Configuration: Server Network Configuration


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
Digital Alert Systems
a division of MONROE ELECTRONICS
DASDEC-1EN Analog/Digital CAP/EAS Encoder/Decoder
○ Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ● Network ○ Time ○ Users
Back
Refresh
OpLog
<192.168.1.100>
User:Admin
Thu Jan 5 20:08:18 2017 MST
Logout
Configuration
Security
Proxy

Server Network Configuration

The server can be configured to have a static IP address or can use DHCP to automatically get an address. A 2nd network interface can also be configured with a static or DHCP address. This will only be enabled if the correct hardware is installed. Presently, the USB-Ethernet Adaptor Belkin F5D5050 is supported and is plug and play. Specific ethernet PCI cards have not been tested or approved, although many will work.

Current Access NIC Host: 192.168.1.15

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

Select a gateway route option.
○ No Gateway
● Main Network Interface
○ 2nd Network Interface *(if selected remember to enable 2nd network)*

192.168.1.1 IP Address of Gateway

Network is **Enabled**
Current IP : 192.168.1.15

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

Network Type
● Static (Manually Configure) ○ Automatic(via DHCP)

Manual Config Options
192.168.1.15 IP Address
255.255.255.0 IP Netmask
☑ Use DNS?
3 Timeout (1-5 secs) 2 Tries (1-2)

75.75.75.75 IP Address of Primary Nameserver
75.75.76.76 IP Address of Second Nameserver

DNS Domain name (optional)
DNS Search name (optional)
www.example.com Test Name Test DNS

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

Accept Changes/Restart Network
Cancel Changes

Server Network Configuration Screen (top half)

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

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

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

Server Network Hostname

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

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

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

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

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

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

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

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

Gateway Configuration

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

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

- No Gateway
- Main Interface
- 2nd Network Interface

If a gateway is required:

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

If a gateway option is selected:

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

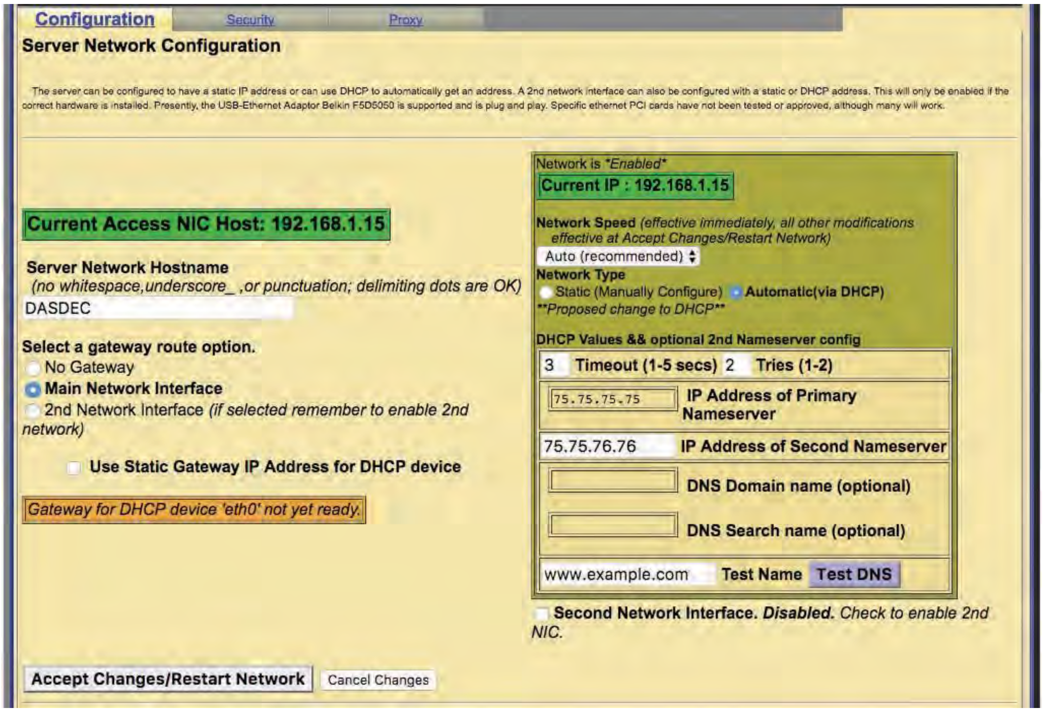
Network Interface Configuration

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

For Static IP Addresses:

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

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



Server Network Configuration

The server can be configured to have a static IP address or can use DHCP to automatically get an address. A 2nd network interface can also be configured with a static or DHCP address. This will only be enabled if the correct hardware is installed. Presently, the USB-Ethernet Adaptor Belkin F5D5050 is supported and is plug and play. Specific ethernet PCI cards have not been tested or approved, although many will work.

Current Access NIC Host: 192.168.1.15

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

Select a gateway route option.
○ No Gateway
● Main Network Interface
○ 2nd Network Interface *(if selected remember to enable 2nd network)*

□ Use Static Gateway IP Address for DHCP device

Gateway for DHCP device 'eth0' not yet ready.

Network is **Enabled**
Current IP : 192.168.1.15

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

Network Type
○ Static (Manually Configure) ● Automatic(via DHCP)
Proposed change to DHCP

DHCP Values && optional 2nd Nameserver config
3 Timeout (1-5 secs) 2 Tries (1-2)
75.75.75.75 IP Address of Primary Nameserver
75.75.76.76 IP Address of Second Nameserver
DNS Domain name (optional)
DNS Search name (optional)
www.example.com Test Name Test DNS

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

Accept Changes/Restart Network   Cancel Changes

Server Network Configuration Screen (unaccepted changes)

For DHCP:

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

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

To enable DNS:

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

Timeout

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

Tries

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

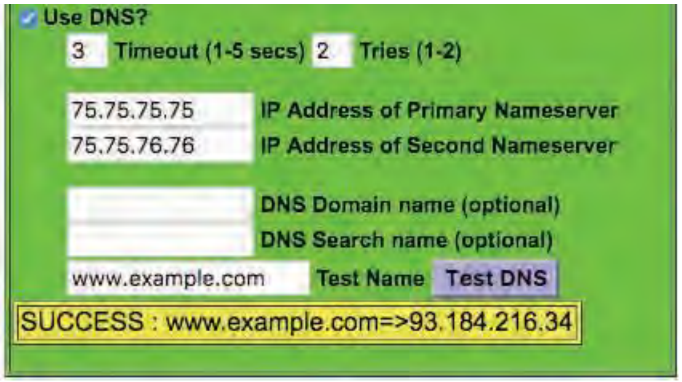
Test Name

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

Test DNS

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

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



☑ Use DNS?

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

75.75.75.75 IP Address of Primary Nameserver

75.75.76.76 IP Address of Second Nameserver

DNS Domain name (optional)

DNS Search name (optional)

www.example.com Test Name Test DNS

SUCCESS : www.example.com=>93.184.216.34

Successful DNS Test

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

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

The Network Interface box has three different color status:

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

Default settings:

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

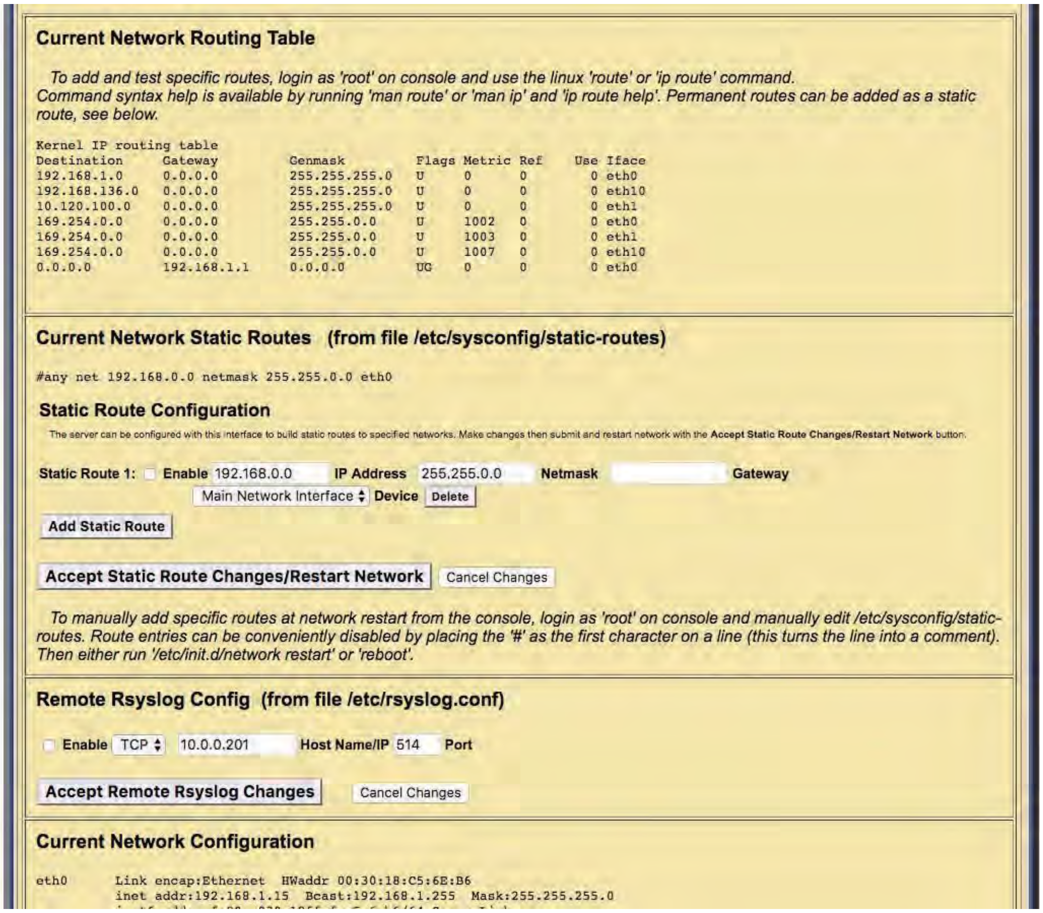
Network Status Information

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

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

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

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



Current Network Routing Table

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

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

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

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

Static Route Configuration

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

Static Route 1: □ Enable 192.168.0.0 IP Address 255.255.0.0 Netmask Gateway
Main Network Interface Device

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

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

□ Enable TCP 10.0.0.201 Host Name/IP 514 Port

Current Network Configuration

```
eth0      Link encap:Ethernet  HWaddr 00:30:18:C5:6E:B6
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
```

Server Network Configuration Screen (Network Status Information)

Static Route Configuration

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

To configure a static route:

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

Note
A conflicting route can block network connectivity.

To disable a static route:

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

Remote Rsyslog Configuration

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

To enable the Remote Rsyslog feature:

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

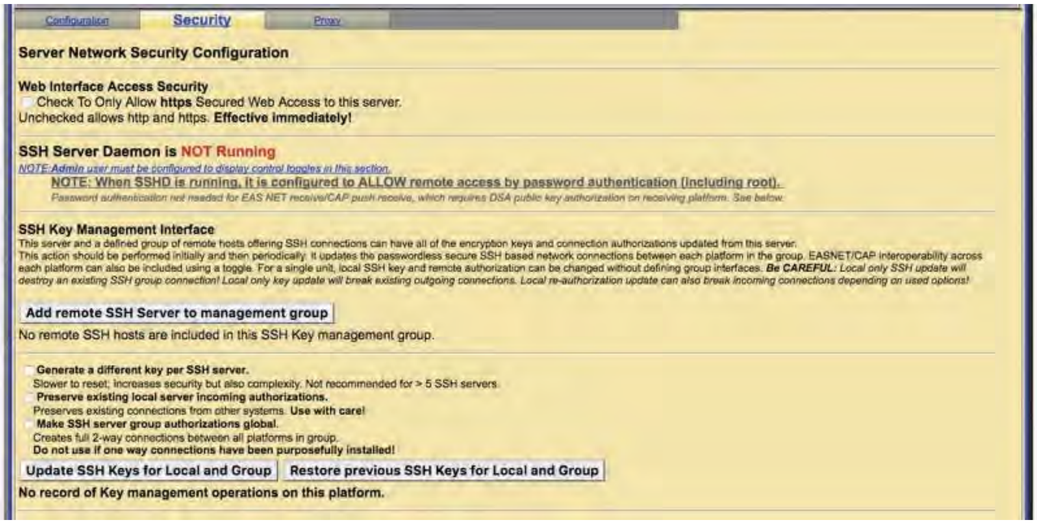
To disable the Remote Rsyslog feature:

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

Security: Server Network Security Configuration

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

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



Server Network Security Configuration

Web Interface Access Security
□ Check To Only Allow **https** Secured Web Access to this server.
Unchecked allows http and https. **Effective immediately!**

SSH Server Daemon is NOT Running
NOTE:Admin user must be configured to display control toggles in this section.
NOTE: When SSHD is running, it is configured to ALLOW remote access by password authentication (including root).
Password authentication not needed for EAS NET receive/CAP push receive, which requires DSA public key authorization on receiving platform. See below.

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

No remote SSH hosts are included in this SSH Key management group.

□ **Generate a different key per SSH server.**
Slower to reset; increases security but also complexity. Not recommended for > 5 SSH servers.
□ **Preserve existing local server incoming authorizations.**
Preserves existing connections from other systems. **Use with care!**
□ **Make SSH server group authorizations global.**
Creates full 2-way connections between all platforms in group.
Do not use if one way connections have been purposefully installed!

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

No record of Key management operations on this platform.

Server Network Security Configuration Screen

Web Interface Access Security

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

If the box is checked:

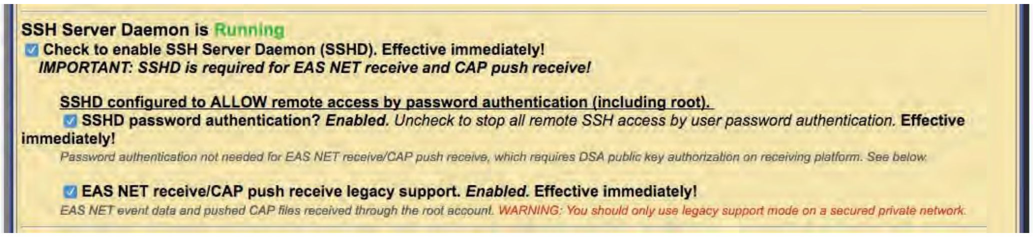
- Browser access is forced to be via HTTPS. The change is immediate.
- All communications to the server will be encrypted.

SSH Server Daemon (Status)

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

To enable the SSH Server Daemon:

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



SSH Server Daemon is Running
☑ **Check to enable SSH Server Daemon (SSHD). Effective immediately!**
IMPORTANT: SSHD is required for EAS NET receive and CAP push receive!

SSHD configured to ALLOW remote access by password authentication (including root).
☑ **SSHD password authentication? *Enabled.*** *Uncheck to stop all remote SSH access by user password authentication.* **Effective immediately!**
Password authentication not needed for EAS NET receive/CAP push receive, which requires DSA public key authorization on receiving platform. See below.

☑ **EAS NET receive/CAP push receive legacy support. *Enabled.* Effective immediately!**
EAS NET event data and pushed CAP files received through the root account. WARNING: You should only use legacy support mode on a secured private network.

Server Network Security Configuration Screen (SSH Server Daemon Section)

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

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

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

SSH Key Management Interface

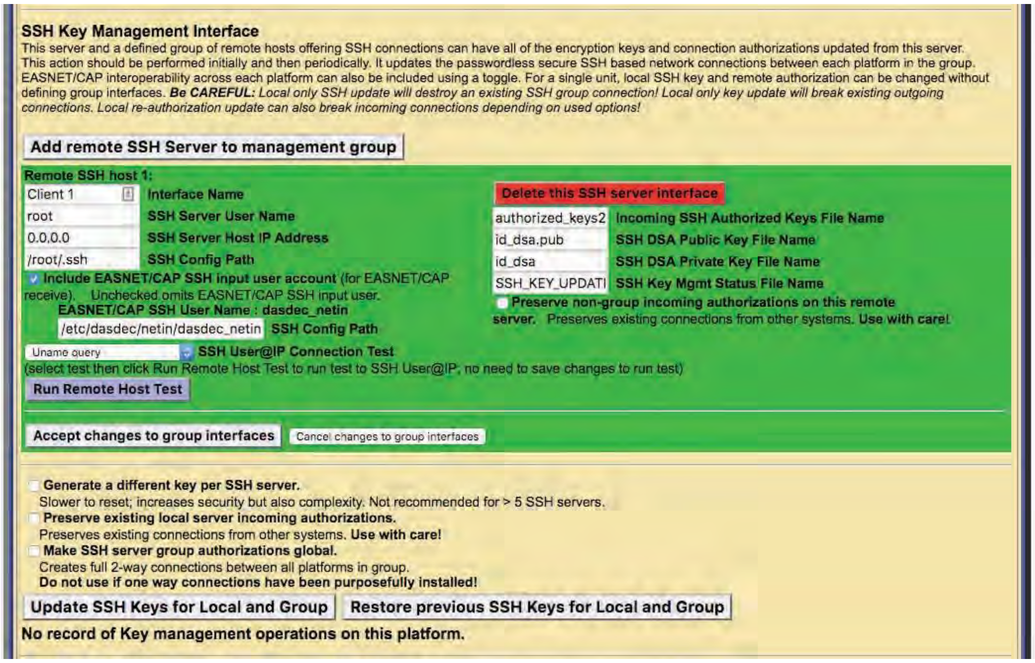
Secure Shell is used for EAS-Net network communication/control between an EAS device and other EAS-Net compatible platforms (including other EAS devices). SSH is a secure communications method that relies on public/private key encryption. To communicate with another platform via SSH, the public key from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

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

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

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

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



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

Remote SSH host 1:
Client 1 **Interface Name**
root **SSH Server User Name**
0.0.0.0 **SSH Server Host IP Address**
/root/.ssh **SSH Config Path**
☑ **Include EASNET/CAP SSH input user account** (for EASNET/CAP receive). Unchecked omits EASNET/CAP SSH input user.
EASNET/CAP SSH User Name : dasdec_netin
/etc/dasdec/netin/dasdec_netin **SSH Config Path**
Uname query **SSH User@IP Connection Test**
(select test then click Run Remote Host Test to run test to SSH User@IP, no need to save changes to run test)

authorized_keys2 **Incoming SSH Authorized Keys File Name**
id_dsa.pub **SSH DSA Public Key File Name**
id_dsa **SSH DSA Private Key File Name**
SSH_KEY_UPDATI **SSH Key Mgmt Status File Name**
☐ **Preserve non-group incoming authorizations on this remote server.** Preserves existing connections from other systems. **Use with care!**

Run Remote Host Test
Accept changes to group interfaces
Cancel changes to group interfaces

☐ **Generate a different key per SSH server.**
Slower to reset; increases security but also complexity. Not recommended for > 5 SSH servers.
☐ **Preserve existing local server incoming authorizations.**
Preserves existing connections from other systems. **Use with care!**
☐ **Make SSH server group authorizations global.**
Creates full 2-way connections between all platforms in group.
Do not use if one way connections have been purposefully installed!

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

No record of Key management operations on this platform.

SSH Key Management Interface Screen

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

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

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

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

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

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

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

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

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

The section below the SSH Management interface displays the following:

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

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

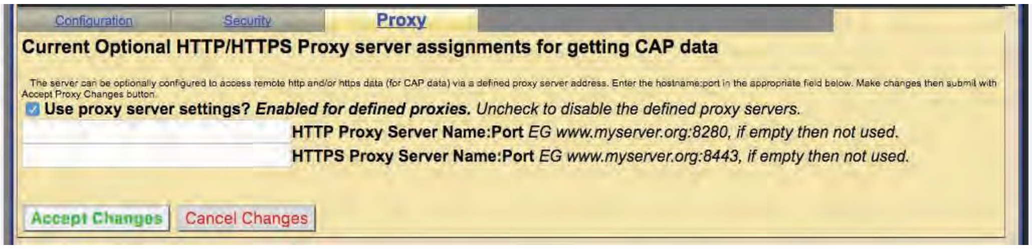
The **Enable** check box is normally checked, which enables this key for use. By unchecking this check box, that key will not be used, and communication with that device or group of devices will be discontinued. Only enabled keys are utilized.

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

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

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

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



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

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

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

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

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

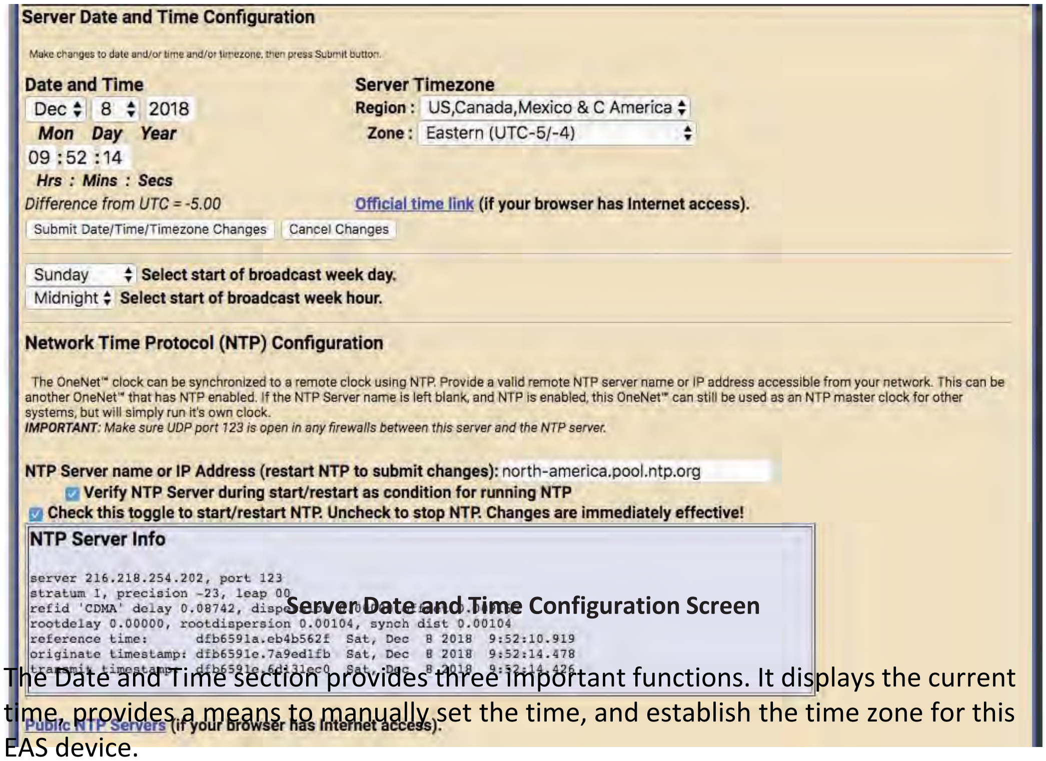
Proxy Screen

To configure a proxy server with the EAS device:

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

TIME SETUP

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



Server Date and Time Configuration

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

Date and Time

Dec 8 2018
Mon Day Year
09 :52 :14
Hrs : Mins : Secs
Difference from UTC = -5.00

Server Timezone

Region : US,Canada,Mexico & C America
Zone : Eastern (UTC-5/-4)

Official time link (if your browser has Internet access).

Sunday Select start of broadcast week day.
Midnight Select start of broadcast week hour.

Network Time Protocol (NTP) Configuration

The OneNet™ clock can be synchronized to a remote clock using NTP. Provide a valid remote NTP server name or IP address accessible from your network. This can be another OneNet™ that has NTP enabled. If the NTP Server name is left blank, and NTP is enabled, this OneNet™ can still be used as an NTP master clock for other systems, but will simply run it's own clock.
IMPORTANT: Make sure UDP port 123 is open in any firewalls between this server and the NTP server.

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

☑ Verify NTP Server during start/restart as condition for running NTP
☑ Check this toggle to start/restart NTP. Uncheck to stop NTP. Changes are immediately effective!

NTP Server Info

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

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

Server Date and Time Configuration Screen

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

To manually set the time:

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

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

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

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

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

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

To enable the NTP feature:

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

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

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

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

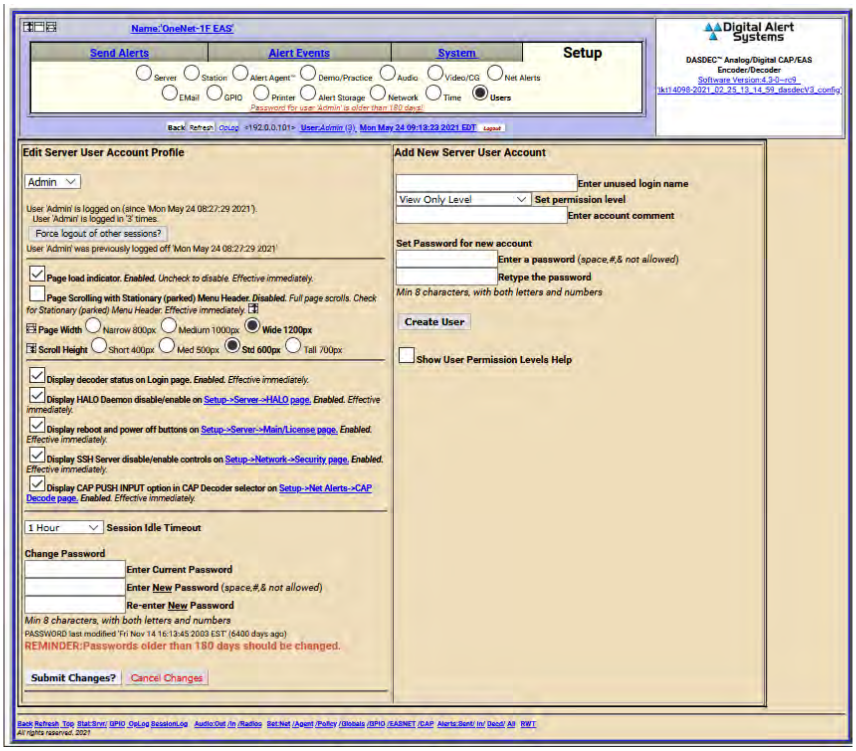
NTP Server Info is located in a gray shaded area below the NTP settings. This is an informational display area that provides status about the NTP connection. Use this information to verify the time offset between the EAS device and the remote NTP server.

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

USERS SETUP

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

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



Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
○ Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ● Users
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Back Refresh OpLog
Logout

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

Software Version:4.3-0~rc9
'lkt14098-2021_02_25_13_14_59_dasdecV3_config'

<192.0.0.101> User:Admin (3) Mon May 24 09:13:23 2021 EDT

Edit Server User Account Profile

Admin

User 'Admin' is logged on (since 'Mon May 24 08:27:29 2021').
User 'Admin' is logged in '3' times.

Force logout of other sessions?

User 'Admin' was previously logged off 'Mon May 24 08:27:29 2021'

☑ **Page load indicator. *Enabled.*** *Uncheck to disable. Effective immediately.*

☐ **Page Scrolling with Stationary (parked) Menu Header. *Disabled.*** *Full page scrolls. Check for Stationary (parked) Menu Header. Effective immediately.*

Page Width ○ Narrow 800px ○ Medium 1000px ● **Wide 1200px**

Scroll Height ○ Short 400px ○ Med 500px ● **Std 600px** ○ Tall 700px

☑ **Display decoder status on Login page. *Enabled.*** *Effective immediately.*

☑ **Display HALO Daemon disable/enable on** Setup->Server->HALO page. ***Enabled.*** *Effective immediately.*

☑ **Display reboot and power off buttons on** Setup->Server->Main/License page. ***Enabled.*** *Effective immediately.*

☑ **Display SSH Server disable/enable controls on** Setup->Network->Security page. ***Enabled.*** *Effective immediately.*

☑ **Display CAP PUSH INPUT option in CAP Decoder selector on** Setup->Net Alerts->CAP Decode page. ***Enabled.*** *Effective immediately.*

1 Hour **Session Idle Timeout**

Change Password

Enter Current Password

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

Re-enter New Password

Min 8 characters, with both letters and numbers

PASSWORD last modified 'Fri Nov 14 16:13:45 2003 EST' (6400 days ago)

REMINDER:Passwords older than 180 days should be changed.

Submit Changes? Cancel Changes

Add New Server User Account

Enter unused login name

View Only Level **Set permission level**

Enter account comment

Set Password for new account

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

Retype the password

Min 8 characters, with both letters and numbers

Create User

☐ **Show User Permission Levels Help**

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

All rights reserved. 2021

Users Setup Screen (Administration Level)

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

Permission Level	Description
Administration Level	Unlimited permissions
Operation/Control Level	Everything EXCEPT: • Upgrades • Software Licensing • Debug Log enable/disable • Web interface user setup/modification • Log deletion • Networked GPIO IP setup • Network setup • Network security setup • Configuration file deletion/rename
Operation Level	Everything Operation/Control can do EXCEPT: • Decoder channel enable/disable • Encoder required test setup • Configuration file interface • Time setup • Alert storage management setup • Networked GPIO setup
Basic Operation Level	• Can encode and forward alerts and run local access forwarding interface • Can terminate EAN with password re-entry • No Setup operations
EOC Operation Level	Special simplified level for Emergency Operation Centers • Can encode alerts • Can terminate EAN with password re-entry • No Setup operations
View Only Level	• Decoded, originated and forwarded alerts and status can be viewed • No Setup operations • No alerts can be originated. No manual forwarding. No cancellation

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

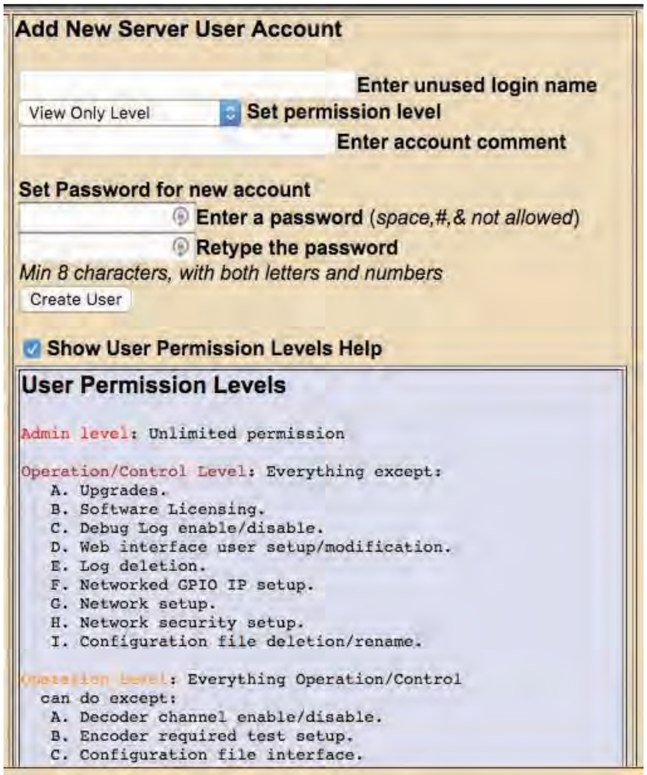
Password Policy

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

- Users are no longer permitted to continue using the default password (*dasdec*) after the initial login.
- Passwords must contain a minimum of 8 characters.
- Passwords must contain both letters and numbers.
- Commonly used (and blacklisted) passwords are not allowed.
- The following text strings are forbidden in any password. These are not case sensitive, and any combination of upper and lower case are disallowed.
    - *password*
    - *12345678*
    - *qwerty*
    - *dasdec*

- The EAS device will visually alert users with passwords older than 180 days.

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



Add New Server User Account

Enter unused login name

View Only Level | Set permission level

Enter account comment

Set Password for new account

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

Retype the password

Min 8 characters, with both letters and numbers

☑ Show User Permission Levels Help

User Permission Levels

```
Admin level: Unlimited permission

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

Operation Level: Everything Operation/Control
  can do except:
   A. Decoder channel enable/disable.
   B. Encoder required test setup.
   C. Configuration file interface.
```

Add New Server User Account Section

Enter unused login name

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

Set permission level

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

Enter account comment

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

Set Password for new account

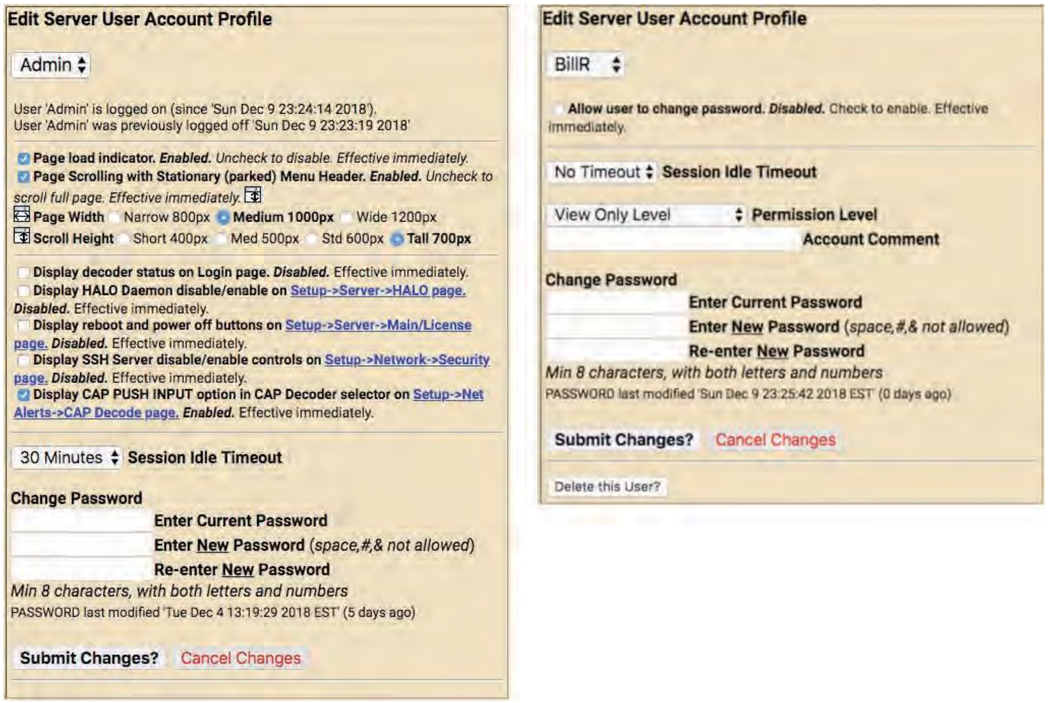
The password for any new account must be entered twice to insure accuracy. Please review the new password policy (above). Any proposed password not meeting this policy will be rejected (cancelling the creation of the new user account) and a brief description of the issue will be displayed just below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

Create User

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

Show User Permission Levels Help

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



Edit Server User Account Profile

Admin

User 'Admin' is logged on (since 'Sun Dec 9 23:24:14 2018').
User 'Admin' was previously logged off 'Sun Dec 9 23:23:19 2018'

☑ **Page load indicator.** ***Enabled.*** *Uncheck to disable. Effective immediately.*
☑ **Page Scrolling with Stationary (parked) Menu Header.** ***Enabled.*** *Uncheck to scroll full page. Effective immediately.*
Page Width ○ Narrow 800px ● **Medium 1000px** ○ Wide 1200px
Scroll Height ○ Short 400px ○ Med 500px ○ Std 600px ● **Tall 700px**

□ **Display decoder status on Login page.** ***Disabled.*** Effective immediately.
□ **Display HALO Daemon disable/enable on** Setup->Server->HALO page. ***Disabled.*** Effective immediately.
□ **Display reboot and power off buttons on** Setup->Server->Main/License page. ***Disabled.*** Effective immediately.
□ **Display SSH Server disable/enable controls on** Setup->Network->Security page. ***Disabled.*** Effective immediately.
☑ **Display CAP PUSH INPUT option in CAP Decoder selector on** Setup->Net Alerts->CAP Decode page. ***Enabled.*** Effective immediately.

30 Minutes **Session Idle Timeout**

Change Password
Enter Current Password
Enter New Password (*space,#,& not allowed*)
Re-enter New Password
Min 8 characters, with both letters and numbers
PASSWORD last modified 'Tue Dec 4 13:19:29 2018 EST' (5 days ago)

Submit Changes? Cancel Changes

Edit Server User Account Profile

BillR

□ **Allow user to change password.** ***Disabled.*** Check to enable. Effective immediately.

No Timeout **Session Idle Timeout**

View Only Level **Permission Level**
Account Comment

Change Password
Enter Current Password
Enter New Password (*space,#,& not allowed*)
Re-enter New Password
Min 8 characters, with both letters and numbers
PASSWORD last modified 'Sun Dec 9 23:25:42 2018 EST' (0 days ago)

Submit Changes? Cancel Changes

Delete this User?

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

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

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

User Account pull-down menu

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

Allow user to change password

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

Page load indicator

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

Page Scrolling with Stationary (parked) Menu Header

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

Page Width

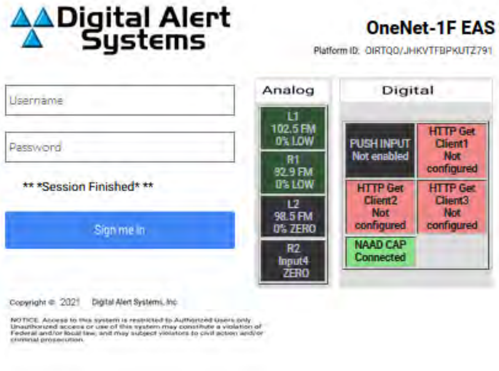
There are three page width settings for the web interface; Narrow 800 pixels, Medium 1000 pixels, and Wide 1200 pixels. Use the radio buttons to select the desired page width. Users may also make adjustments via the page width icon found in the header. This setting is available to all user levels.

Scroll Height

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

Display decoder status on Login page

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



Platform ID: OIRTQO/JHKVTFBPKUTZ791

** *Session Finished* **

Copyright © 2021 Digital Alert Systems, Inc

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

Login Screen with Decoder Status Display

Display HALO Daemon disable/enable

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

New Feature
Support for HALO is new in version 4.0.

Display reboot and power off buttons

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

Display SSH Server disable/enable controls

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

Display CAP PUSH INPUT Option

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

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

Session Idle Timeout

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

Change Password

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

Submit Changes?

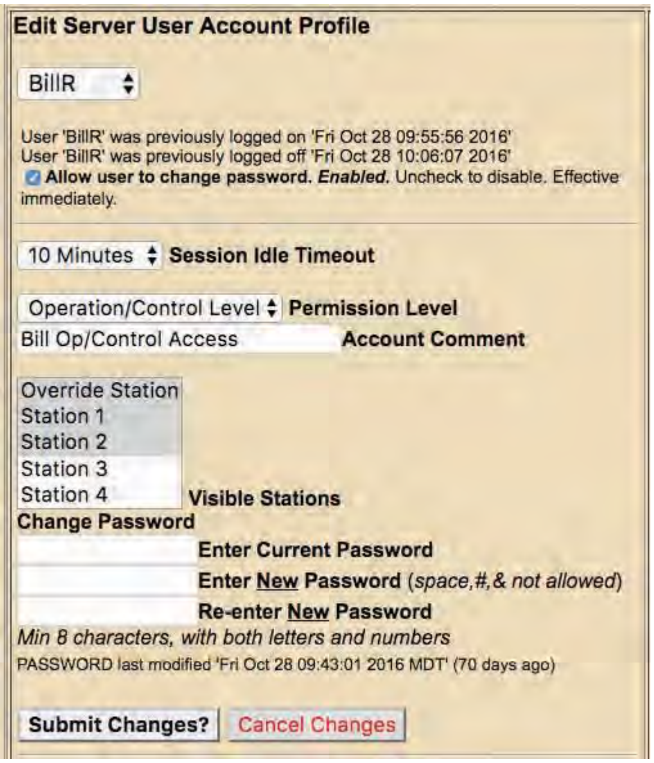
When clicked, this button will submit any changes. It is not necessary to use this button after selecting any of the above check boxes for their changes are immediate.

Cancel Changes

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

Delete this User?

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



Edit Server User Account Profile

BillR

User 'BillR' was previously logged on 'Fri Oct 28 09:55:56 2016'
User 'BillR' was previously logged off 'Fri Oct 28 10:06:07 2016'
☑ **Allow user to change password.** ***Enabled.*** Uncheck to disable. Effective immediately.

10 Minutes **Session Idle Timeout**

Operation/Control Level **Permission Level**

Bill Op/Control Access **Account Comment**

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

Change Password

Enter Current Password

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

Re-enter New Password

Min 8 characters, with both letters and numbers

PASSWORD last modified 'Fri Oct 28 09:43:01 2016 MDT' (70 days ago)

Edit Server User Account Profile - MultiStation Mode

MultiStation User Access

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

To create a new user account:

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

To modify a user account:

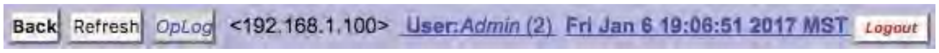
1. Select the desired user in the **User Account** pull-down menu.
2. Make changes to any of the following:
   - **Allow user to change password** check box
   - **Session Idle Timeout** pull-down
   - **Permission level** pull-down
   - **Account Comment** text field
   - **Visible Stations** (for MultiStation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

To delete a user account:

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

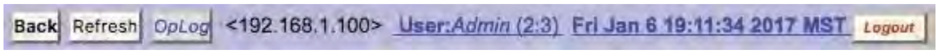
Notes about multiple active user sessions:

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



<192.168.1.100> User:Admin (2) Fri Jan 6 19:06:51 2017 MST

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



<192.168.1.100> User:Admin (2:3) Fri Jan 6 19:11:34 2017 MST

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

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

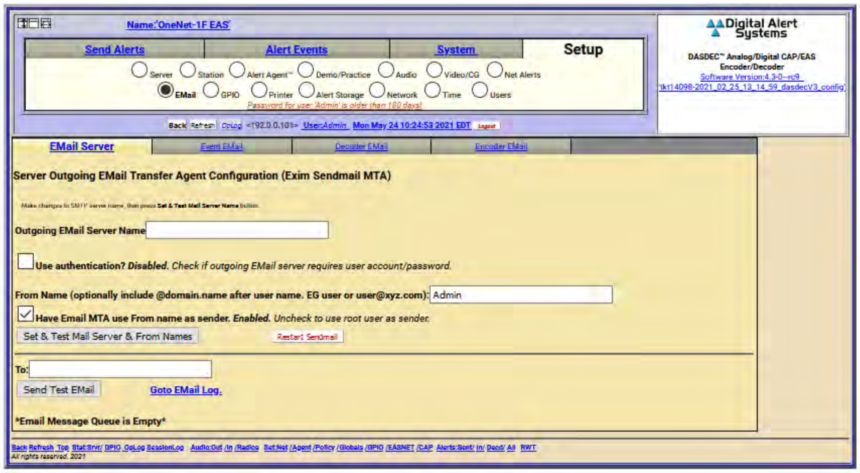
EMAIL SETUP

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

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

EMail Server

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


Name:'OneNet-1F EAS'
Send Alerts
Alert Events
System
Setup
Server
Station
Alert Agent™
Demo/Practice
Audio
Video/CG
Net Alerts
EMail
GPIO
Printer
Alert Storage
Network
Time
Users
Back
Refresh
OpLog
<192.0.0.101>
User:Admin
Mon May 24 10:24:53 2021 EDT
Logout
Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0--rc9
'tkt14098-2021_02_25_13_14_59_dasdecV3_config'
EMail Server
Event EMail
Decoder EMail
Encoder EMail
Set & Test Mail Server & From Names
Restart Sendmail
Send Test EMail
Goto EMail Log.
Back Refresh Top Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2021

○ Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
● EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users

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

Server Outgoing EMail Transfer Agent Configuration (Exim Sendmail MTA)

Make changes to SMTP server name, then press **Set & Test Mail Server Name** button.

Outgoing EMail Server Name

□ Use authentication? ***Disabled.*** *Check if outgoing EMail server requires user account/password.*

From Name (optionally include @domain.name after user name. EG user or user@xyz.com): Admin

☑ Have Email MTA use From name as sender. ***Enabled.*** *Uncheck to use root user as sender.*

To:

Email Message Queue is Empty

EMail Server Tab

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

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

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

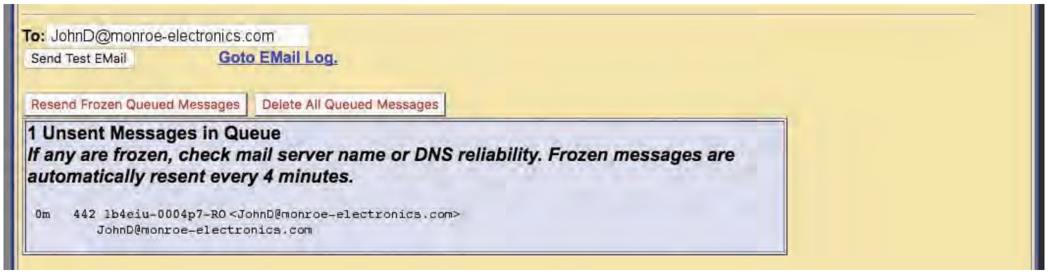
1. Go to **Setup > EMail > EMail Server.**
2. Enter the name of outgoing mail server in the **Outgoing Email Server** text field.
3. Check the **Use authentication?** check box – the **User Name** and **Password** text fields will appear.
4. Enter the appropriate user name in the **User Name** text field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

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

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

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

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



To: JohnD@monroe-electronics.com

1 Unsent Messages in Queue

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

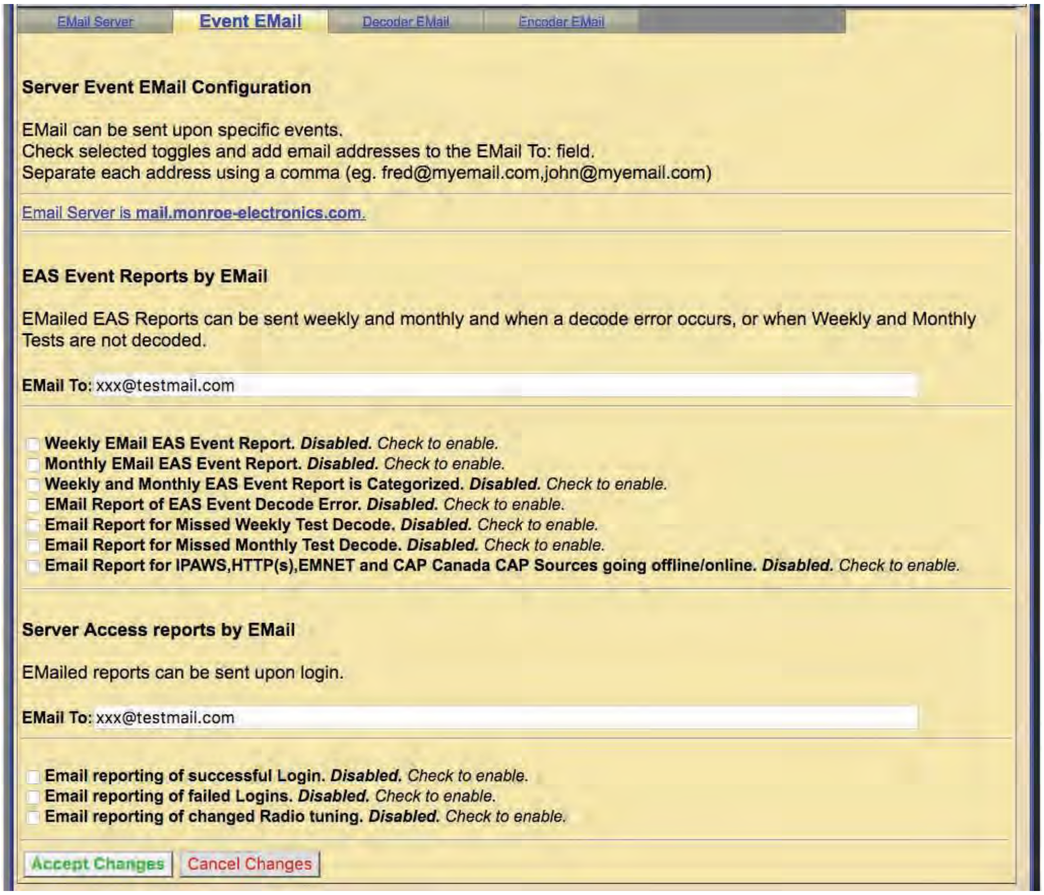
```
 0m   442 1b4eiu-0004p7-RO <JohnD@monroe-electronics.com>
         JohnD@monroe-electronics.com
```

Sent Test EMail Section

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

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

Event EMail



Server Event EMail Configuration

EMail can be sent upon specific events.
Check selected toggles and add email addresses to the EMail To: field.
Separate each address using a comma (eg. fred@myemail.com,john@myemail.com)

Email Server is **mail.monroe-electronics.com.**

EAS Event Reports by EMail

EMailed EAS Reports can be sent weekly and monthly and when a decode error occurs, or when Weekly and Monthly Tests are not decoded.

EMail To: xxx@testmail.com

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

Server Access reports by EMail

EMailed reports can be sent upon login.

EMail To: xxx@testmail.com

- □ **Email reporting of successful Login. *Disabled.*** *Check to enable.*
- □ **Email reporting of failed Logins. *Disabled.*** *Check to enable.*
- □ **Email reporting of changed Radio tuning. *Disabled.*** *Check to enable.*

Server Event EMail Configuration Screen

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

EAS Event Reports by EMail

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

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

Server Access Reports by EMail

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

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

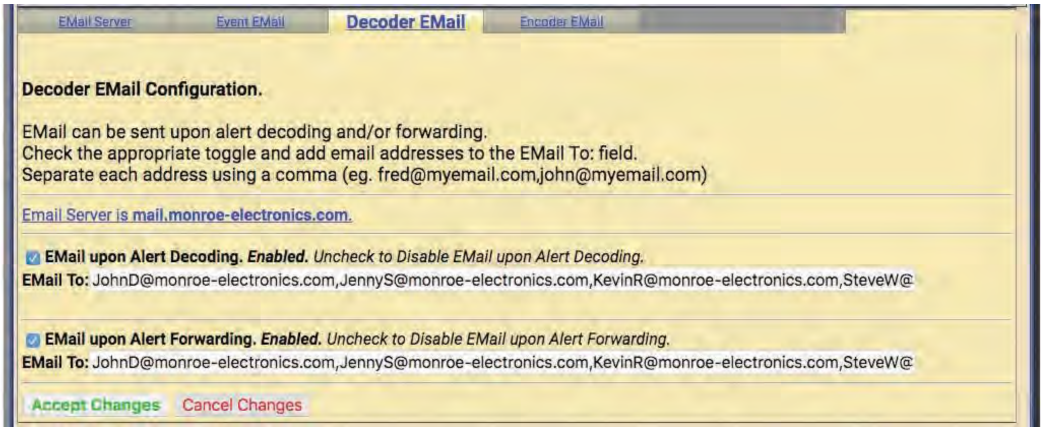
Once the desired updates have been made to the Event EMail screen, click the **Accept Changes** button to input these settings. The **Cancel Changes** button is used to cancel any updates and refresh the screen.

Decoder EMail

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

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

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



Decoder EMail Configuration.

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

Email Server is mail.monroe-electronics.com.

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

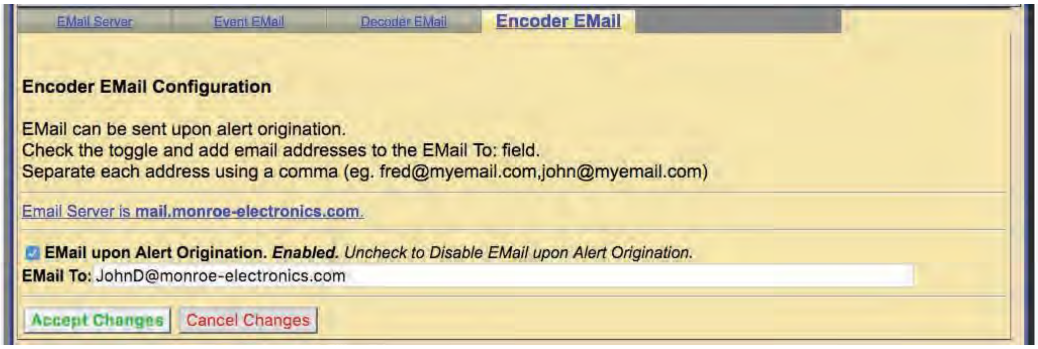
☑ **EMail upon Alert Forwarding. *Enabled.*** *Uncheck to Disable EMail upon Alert Forwarding.*
EMail To: JohnD@monroe-electronics.com,JennyS@monroe-electronics.com,KevinR@monroe-electronics.com,SteveW@

Decoder Email Configuration Screen

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

Encoder Email

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



Encoder EMail Configuration

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

Email Server is mail.monroe-electronics.com.

☑ **EMail upon Alert Origination.** ***Enabled.*** *Uncheck to Disable EMail upon Alert Origination.*
EMail To: JohnD@monroe-electronics.com

Encoder Email Configuration Screen

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

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

AUDIO SETUP

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

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

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

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

Audio Output Levels/Tests

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

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

All standard EAS devices come from the factory with:

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

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

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

Testing and Calibrating Levels

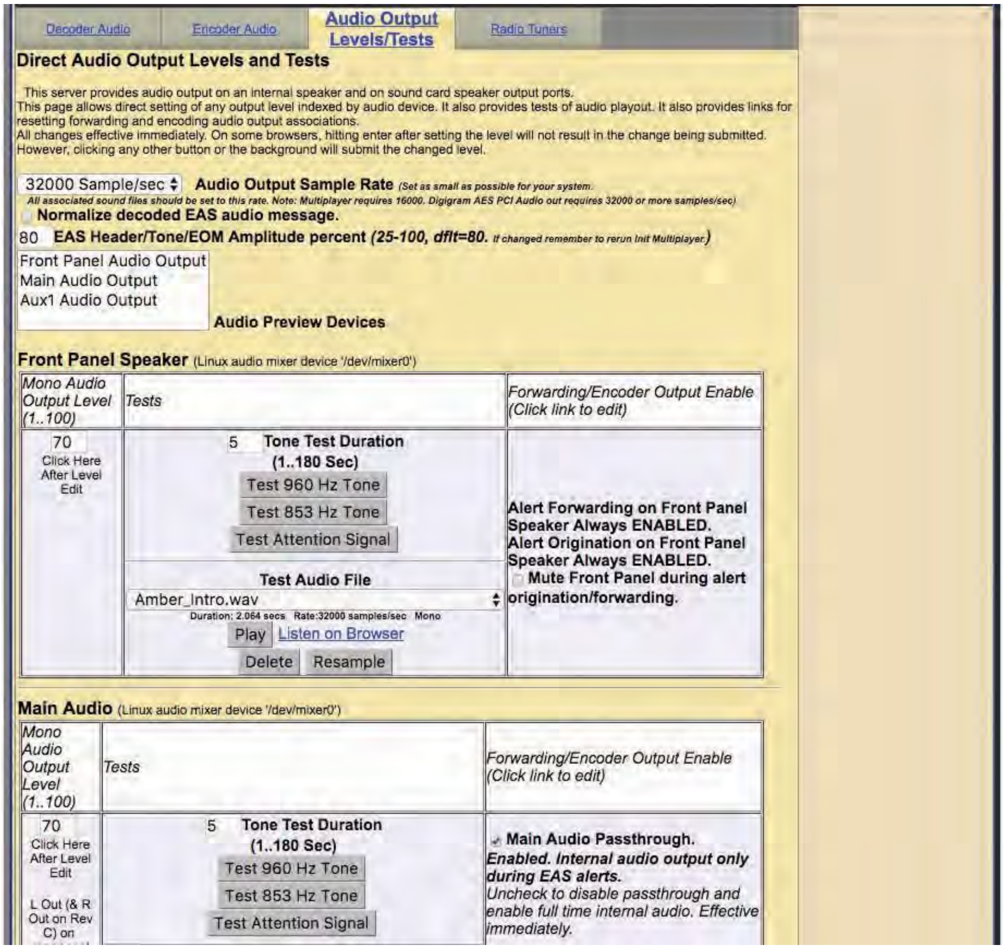
Audio tones can be played through each available audio output to test audio connections and calibrate levels using audio test equipment:

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

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

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

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



Direct Audio Output Levels and Tests

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

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

□ **Normalize decoded EAS audio message.**

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

Front Panel Audio Output
Main Audio Output
Aux1 Audio Output
Audio Preview Devices

Front Panel Speaker (Linux audio mixer device '/dev/mixer0')

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

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

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

Direct Audio Output Level and Tests Screen

Audio Output Sample Rate

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

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

Normalize decoded EAS audio message

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

EAS Header/Tone/EOM Amplitude percent

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

Audio Preview Devices

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

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

Front Panel Speaker

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

Mono Audio Output Level

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

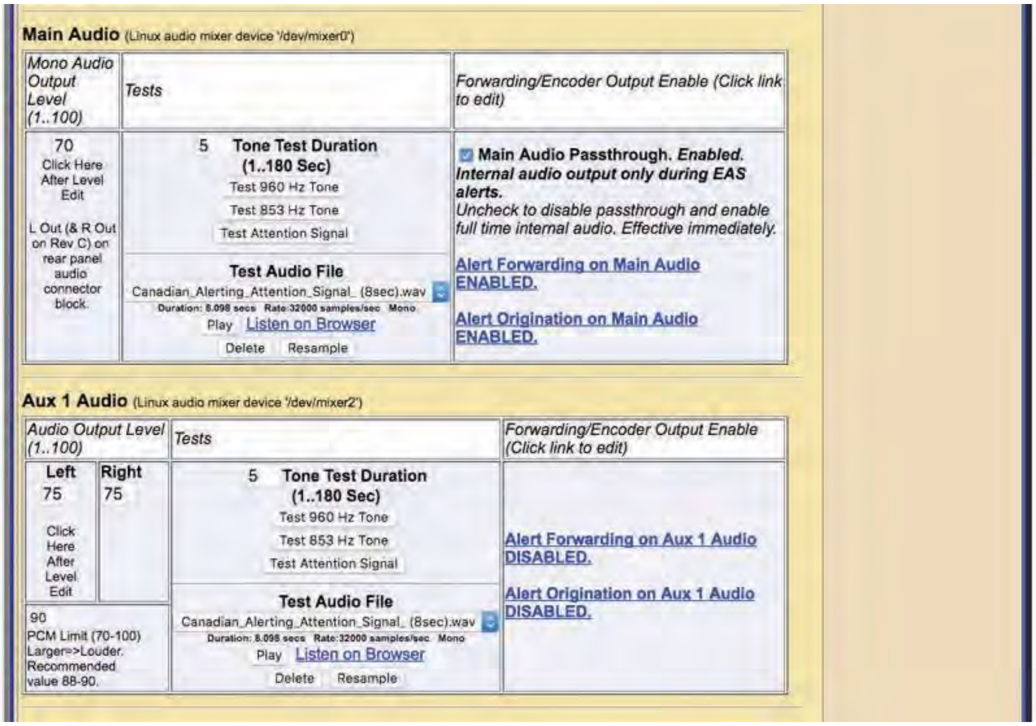
Audio Tests

There are several audio test options:

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

Forwarding/Encoder Output Enable

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



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

Mono Audio Output Level (1..100)	*Tests*	*Forwarding/Encoder Output Enable (Click link to edit)*
70 Click Here After Level Edit L Out (& R Out on Rev C) on rear panel audio connector block.	5 **Tone Test Duration (1..180 Sec)** Test 960 Hz Tone Test 853 Hz Tone Test Attention Signal **Test Audio File** Canadian_Alerting_Attention_Signal_ (8sec).wav Duration: 8.098 secs Rate:32000 samples/sec Mono Play Listen on Browser Delete Resample	☑ **Main Audio Passthrough.** ***Enabled. Internal audio output only during EAS alerts.*** *Uncheck to disable passthrough and enable full time internal audio. Effective immediately.* Alert Forwarding on Main Audio ENABLED. Alert Origination on Main Audio ENABLED.

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

Audio Output Level (1..100)		*Tests*	*Forwarding/Encoder Output Enable (Click link to edit)*
Left 75 Click Here After Level Edit	**Right** 75	5 **Tone Test Duration (1..180 Sec)** Test 960 Hz Tone Test 853 Hz Tone Test Attention Signal	Alert Forwarding on Aux 1 Audio DISABLED. Alert Origination on Aux 1 Audio DISABLED.
90 PCM Limit (70-100) Larger=>Louder. Recommended value 88-90.		**Test Audio File** Canadian_Alerting_Attention_Signal_ (8sec).wav Duration: 8.098 secs Rate:32000 samples/sec Mono Play Listen on Browser Delete Resample	

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

Main Audio and Aux Audio Tables

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

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

Forwarding / Encoder Output Enable & Main Audio / Passthrough Audio

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

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

Tests:

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

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

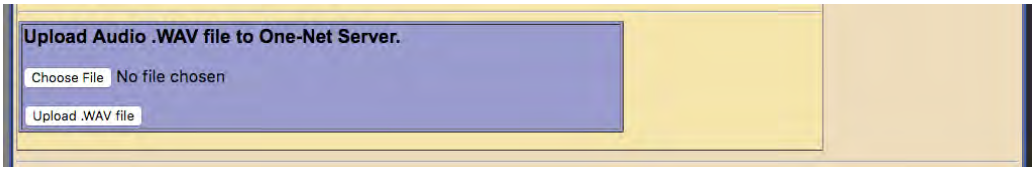
Note
The EAS Attention signal and WAV files can be played as described above for the front panel speaker interface table.

Alert Forwarding and Alert Origination

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

To make changes to these states:

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


Upload Audio .WAV file to One-Net Server.

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

Upload Audio .WAV file

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

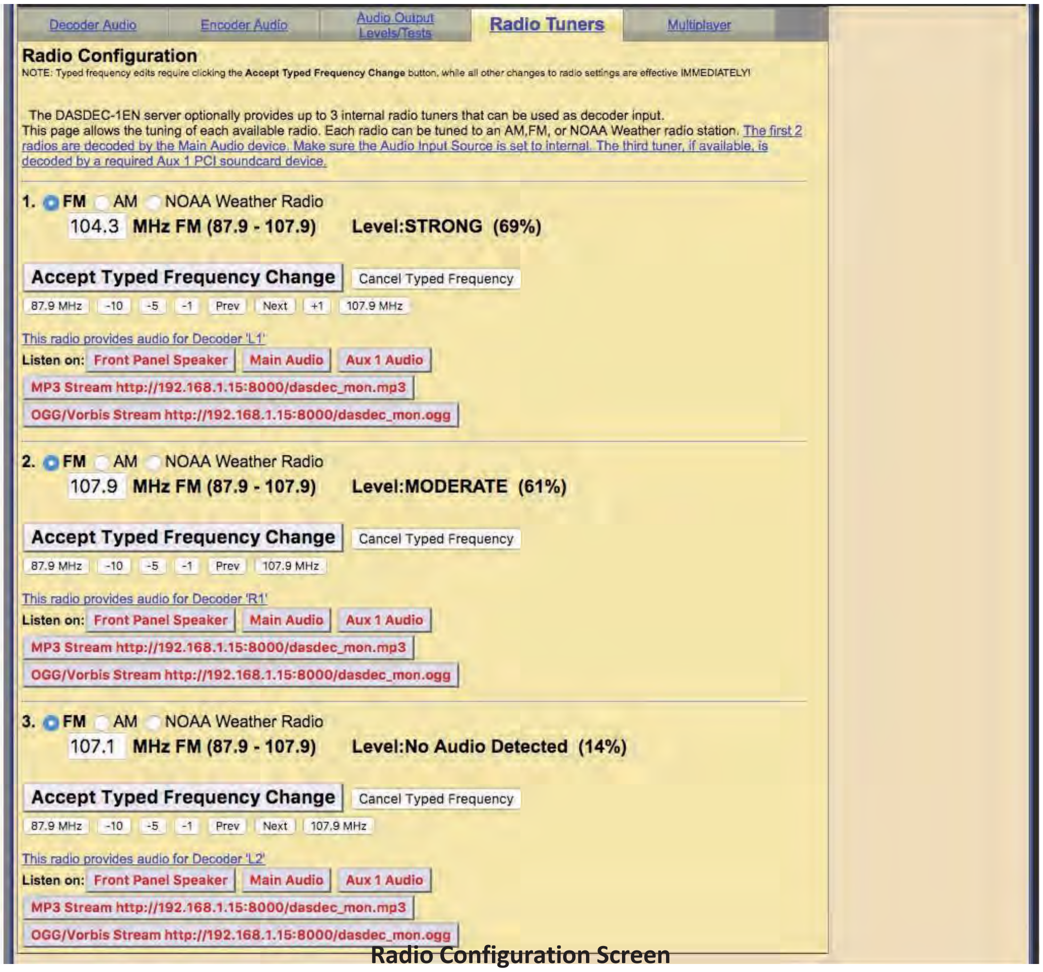
- Click the Browse button to locate the file on the computer
- Click the Upload .WAV file button. MP3 files are converted automatically into a WAV files.

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

Radio Tuners

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

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



Radio Configuration

NOTE: Typed frequency edits require clicking the **Accept Typed Frequency Change** button, while all other changes to radio settings are effective IMMEDIATELY!

The DASDEC-1EN server optionally provides up to 3 internal radio tuners that can be used as decoder input.
This page allows the tuning of each available radio. Each radio can be tuned to an AM,FM, or NOAA Weather radio station. The first 2 radios are decoded by the Main Audio device. Make sure the Audio Input Source is set to internal. The third tuner, if available, is decoded by a required Aux 1 PCI soundcard device.

1. ● FM ○ AM ○ NOAA Weather Radio
104.3 **MHz FM (87.9 - 107.9)** **Level:STRONG (69%)**

Accept Typed Frequency Change | Cancel Typed Frequency
87.9 MHz | -10 | -5 | -1 | Prev | Next | +1 | 107.9 MHz

This radio provides audio for Decoder 'L1'
Listen on: Front Panel Speaker | Main Audio | Aux 1 Audio
MP3 Stream http://192.168.1.15:8000/dasdec_mon.mp3
OGG/Vorbis Stream http://192.168.1.15:8000/dasdec_mon.ogg

2. ● FM ○ AM ○ NOAA Weather Radio
107.9 **MHz FM (87.9 - 107.9)** **Level:MODERATE (61%)**

Accept Typed Frequency Change | Cancel Typed Frequency
87.9 MHz | -10 | -5 | -1 | Prev | 107.9 MHz

This radio provides audio for Decoder 'R1'
Listen on: Front Panel Speaker | Main Audio | Aux 1 Audio
MP3 Stream http://192.168.1.15:8000/dasdec_mon.mp3
OGG/Vorbis Stream http://192.168.1.15:8000/dasdec_mon.ogg

3. ● FM ○ AM ○ NOAA Weather Radio
107.1 **MHz FM (87.9 - 107.9)** **Level:No Audio Detected (14%)**

Accept Typed Frequency Change | Cancel Typed Frequency
87.9 MHz | -10 | -5 | -1 | Prev | Next | 107.9 MHz

This radio provides audio for Decoder 'L2'
Listen on: Front Panel Speaker | Main Audio | Aux 1 Audio
MP3 Stream http://192.168.1.15:8000/dasdec_mon.mp3
OGG/Vorbis Stream http://192.168.1.15:8000/dasdec_mon.ogg

Radio Configuration Screen

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

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

A numeric level indicator displays the strength of reception:

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

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

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

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

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

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

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

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

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

Decoder Audio

The Decoder Audio page has three areas to configure:

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

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

Main and Auxiliary Audio Decoder Configuration

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

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

Soundcard name and associated Linux mixer device

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

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

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

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

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

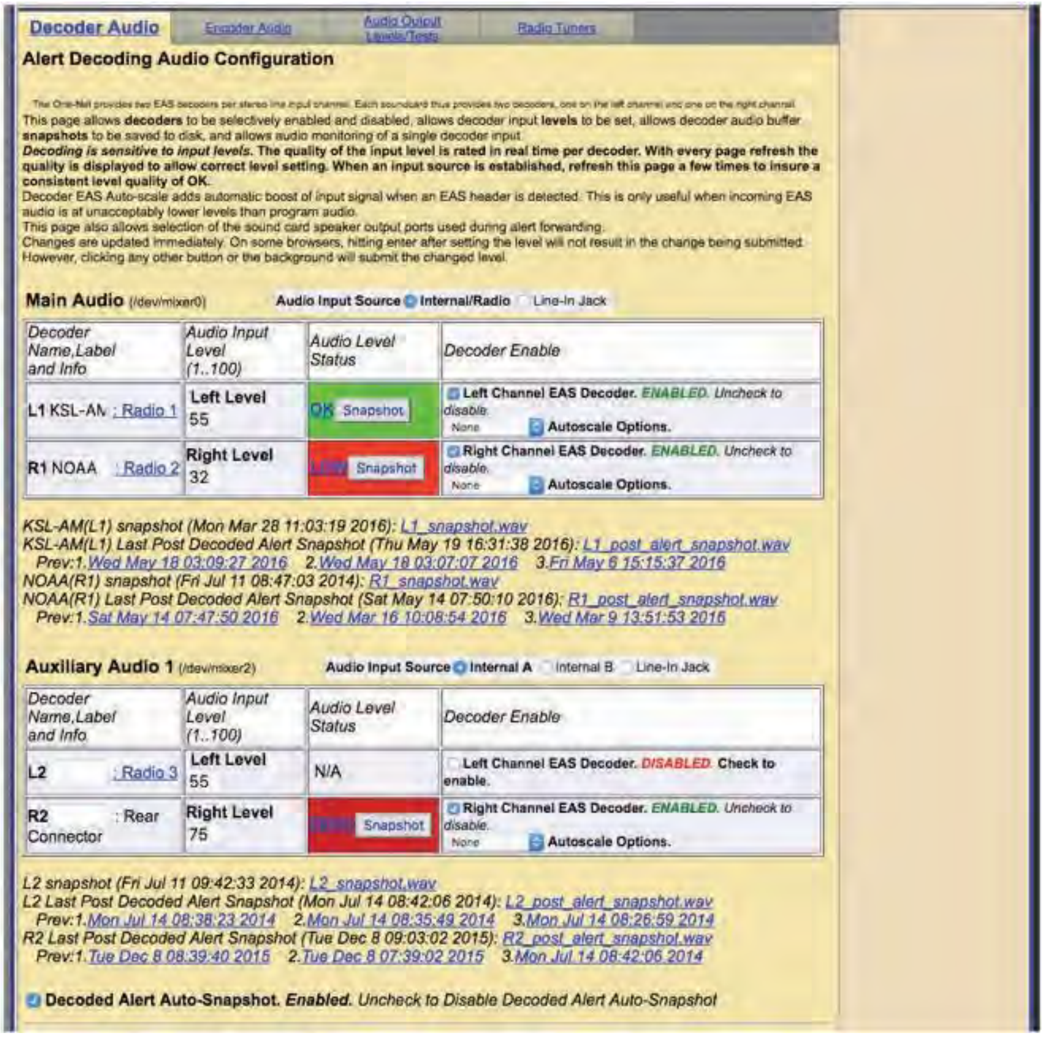
- Two are connected to the main audio device
- The third is connected through the Audio Input Source “Internal A” connection
- A fourth audio source, from the back panel screw connector terminal, is also routed through this input channel

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

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

Soundcard decoder pair display table

Each table provides names and controls for two decoders to be selectively enabled and disabled and for decoder input levels to be set. Typically, all decoders can be enabled. The EAS device supports two EAS decoders per stereo line input channel. This results in each sound card device providing two decoders, one on the left channel and one on the right channel (L1 and R1). Each decoder is displayed in a separate row in the sound card status table. Each row has four columns to review and configure.



Alert Decoding Audio Configuration

The One-Net provides two EAS decoders per stereo line input channel. Each soundcard thus provides two decoders, one on the left channel and one on the right channel.

This page allows **decoders** to be selectively enabled and disabled, allows decoder input **levels** to be set, allows decoder audio buffer **snapshots** to be saved to disk, and allows audio monitoring of a single decoder input.

Decoding is sensitive to input levels. **The quality of the input level is rated in real time per decoder. With every page refresh the quality is displayed to allow correct level setting. When an input source is established, refresh this page a few times to insure a consistent level quality of OK.**

Decoder EAS Auto-scale adds automatic boost of input signal when an EAS header is detected. This is only useful when incoming EAS audio is at unacceptably lower levels than program audio.

This page also allows selection of the sound card speaker output ports used during alert forwarding.

Changes are updated immediately. On some browsers, hitting enter after setting the level will not result in the change being submitted. However, clicking any other button or the background will submit the changed level.

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

Decoder Name,Label and Info	*Audio Input Level (1..100)*	*Audio Level Status*	*Decoder Enable*
L1 KSL-AM : Radio 1	**Left Level** 55	OK Snapshot	☑ **Left Channel EAS Decoder.** *ENABLED. Uncheck to disable.* None **Autoscale Options.**
R1 NOAA : Radio 2	**Right Level** 32	LOW Snapshot	☑ **Right Channel EAS Decoder.** *ENABLED. Uncheck to disable.* None **Autoscale Options.**

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

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

Decoder Name,Label and Info	*Audio Input Level (1..100)*	*Audio Level Status*	*Decoder Enable*
L2 : Radio 3	**Left Level** 55	N/A	☐ **Left Channel EAS Decoder.** *DISABLED.* **Check to enable.**
R2 : Rear Connector	**Right Level** 75	[illegible] Snapshot	☑ **Right Channel EAS Decoder.** *ENABLED. Uncheck to disable.* None **Autoscale Options.**

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

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

Alert Decoding Audio Configuration Screen

The audio soundcard table columns are:

Decoder Name, Label and Info

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

Audio Input Level (1..100)

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

Audio Level Status

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

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

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

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

In the screen shot, four snapshot files are shown:

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

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

Decoder Enable

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

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

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

- None
- FFT Filter
- Amplification

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

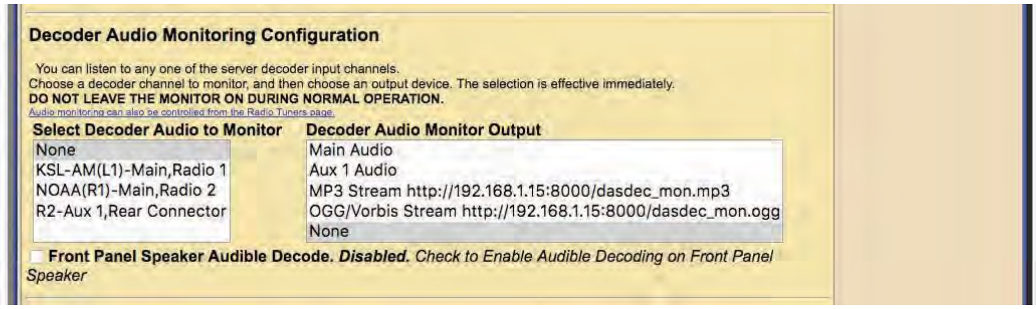
- A snapshot WAV file being generated after an alert is decoded or after a decode error is detected
- Detailed troubleshooting in the case where an incoming EAS audio has resulted in decoder errors.

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

Decoder Audio Monitoring Configuration

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

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



Decoder Audio Monitoring Configuration

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

Select Decoder Audio to Monitor
None
KSL-AM(L1)-Main,Radio 1
NOAA(R1)-Main,Radio 2
R2-Aux 1,Rear Connector

Decoder Audio Monitor Output
Main Audio
Aux 1 Audio
MP3 Stream http://192.168.1.15:8000/dasdec_mon.mp3
OGG/Vorbis Stream http://192.168.1.15:8000/dasdec_mon.ogg
None

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

Decoder Audio Monitoring Configuration Section

To operate:

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

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

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

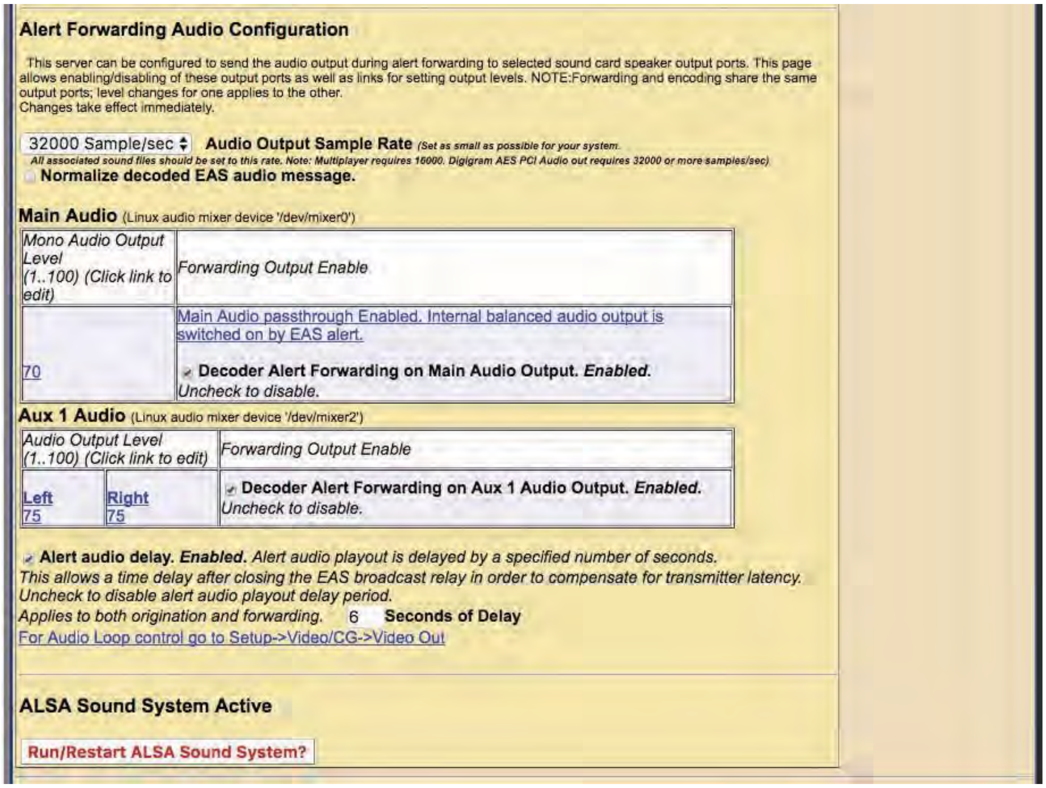
Front Panel Speaker Audible Decode

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

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

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

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



Alert Forwarding Audio Configuration

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

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

□ **Normalize decoded EAS audio message.**

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

Mono Audio Output Level (1..100) (Click link to edit)	*Forwarding Output Enable*
70	Main Audio passthrough Enabled. Internal balanced audio output is switched on by EAS alert. ☑ **Decoder Alert Forwarding on Main Audio Output.** ***Enabled.*** *Uncheck to disable.*

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

Audio Output Level (1..100) (Click link to edit)		*Forwarding Output Enable*
Left 75	Right 75	☑ **Decoder Alert Forwarding on Aux 1 Audio Output.** ***Enabled.*** *Uncheck to disable.*

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

ALSA Sound System Active

Alert Forwarding Audio Configuration Section

Alert Forwarding Audio Configuration

Audio Output Sample Rate

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

Normalize decoded EAS audio message

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

Audio Forwarding Tables

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

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

Audio Output Level

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

Forwarding Output Enable

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

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

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

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

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

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

ALSA Sound System Active

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

Encoder Audio

There are two main configuration options for encoder audio:

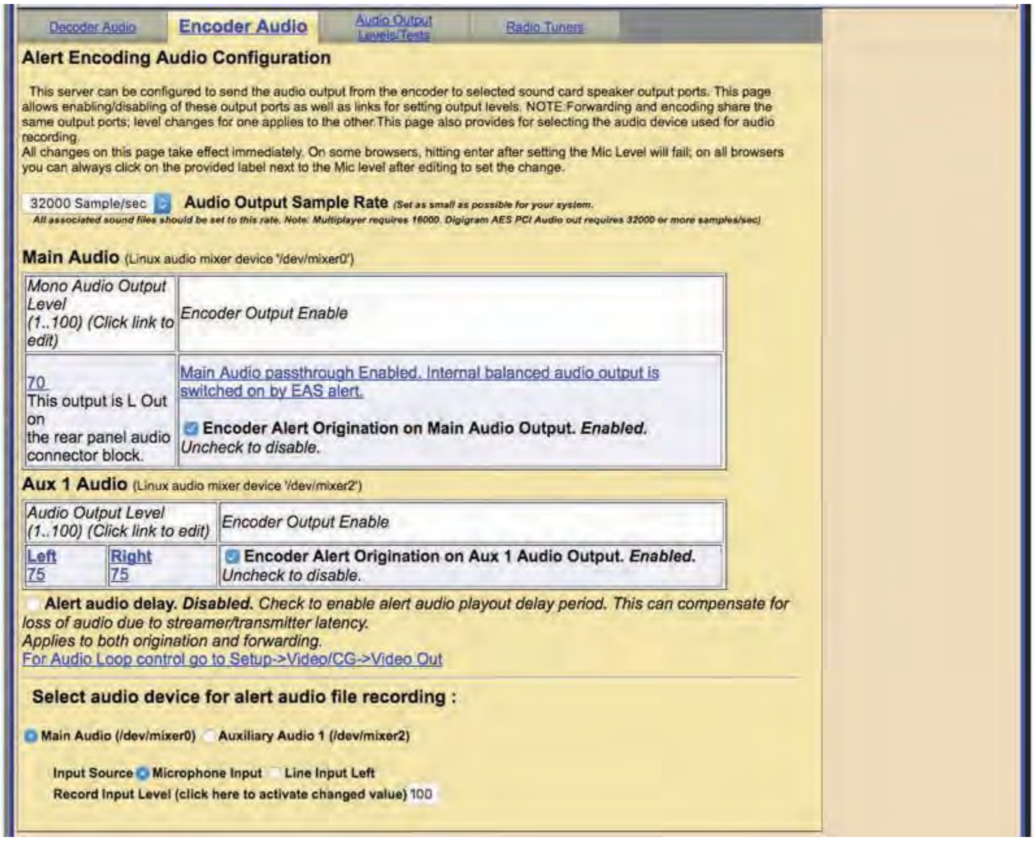
- Alert Encoding Audio Configuration
- Alert Audio File Recording.

Alert Encoding Audio Configuration

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

This interface allows for:

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



Alert Encoding Audio Configuration

This server can be configured to send the audio output from the encoder to selected sound card speaker output ports. This page allows enabling/disabling of these output ports as well as links for setting output levels. NOTE:Forwarding and encoding share the same output ports; level changes for one applies to the other.This page also provides for selecting the audio device used for audio recording.
All changes on this page take effect immediately. On some browsers, hitting enter after setting the Mic Level will fail; on all browsers you can always click on the provided label next to the Mic level after editing to set the change.

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

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

Mono Audio Output Level (1..100) (Click link to edit)	*Encoder Output Enable*
70 This output is L Out on the rear panel audio connector block.	Main Audio passthrough Enabled. Internal balanced audio output is switched on by EAS alert. ☑ **Encoder Alert Origination on Main Audio Output.** ***Enabled.*** *Uncheck to disable.*

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

Audio Output Level (1..100) (Click link to edit)		*Encoder Output Enable*
Left 75	Right 75	☑ **Encoder Alert Origination on Aux 1 Audio Output.** ***Enabled.*** *Uncheck to disable.*

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

Select audio device for alert audio file recording :

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

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

Alert Encoding Audio Configuration Screen

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

Audio Output Sample Rate

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

Main Audio and Auxiliary Audio Tables

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

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

The table has two columns:

- Audio Output Level
- Encoder Output Enable

Audio Output Level

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

Encoder Output Enable

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

Alert Audio Delay

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

Select audio device for alert audio file recording

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

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

Sound card source

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

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

Input Source

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

- Microphone Input
- Line Input Left

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

Record Input Level

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

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

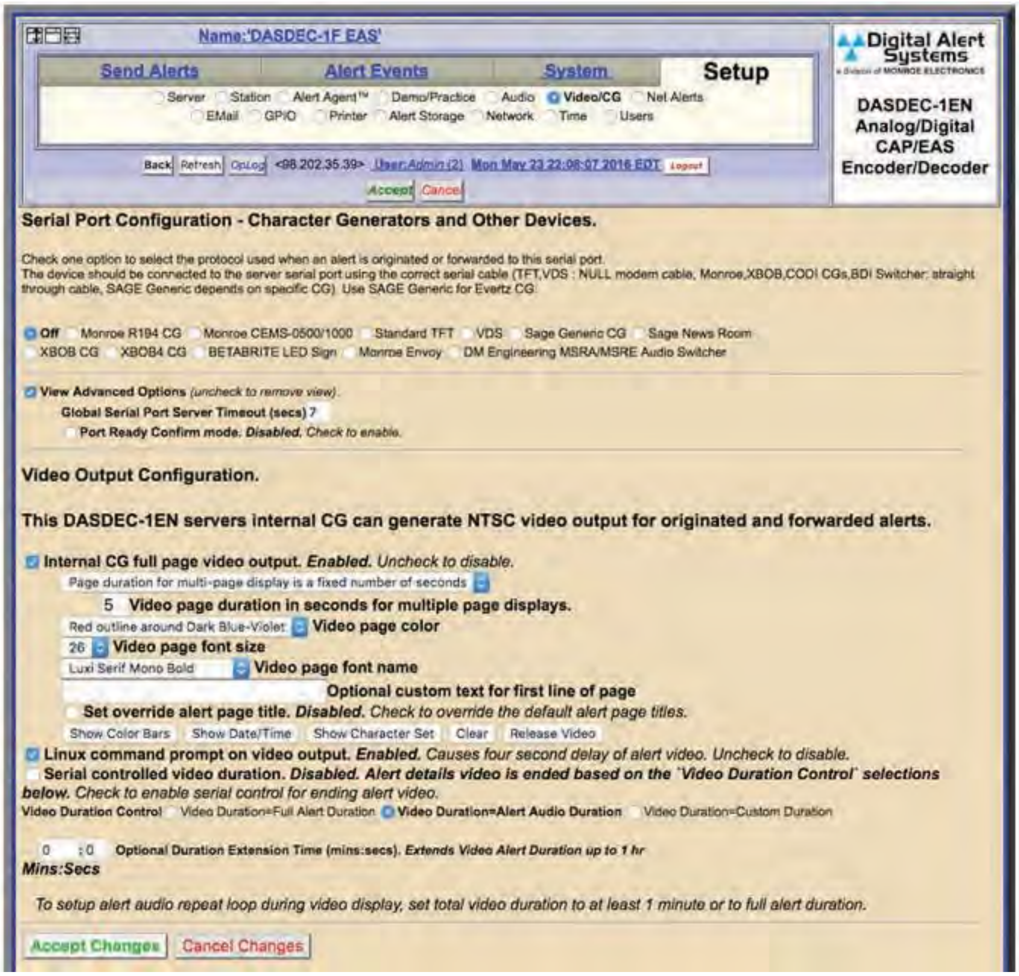
Note
When the EAS devices' MultiStation Mode is enabled, the audio forwarding configuration for each **station** overrides the settings on these tables! Configure station alert audio forwarding on the proper station interface configuration page under **Setup > Station**.

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

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

VIDEO/CG SETUP

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


Name:'DASDEC-1F EAS'
Send Alerts
Alert Events
System
Setup
Digital Alert Systems
a Division of MONROE ELECTRONICS
DASDEC-1EN Analog/Digital CAP/EAS Encoder/Decoder
○ Server ○ Station ○ Alert Agent™ ○ Demo/Practice ○ Audio ● Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users
Back
Refresh
OpLog
<98.202.35.39>
User:Admin (2)
Mon May 23 22:08:07 2016 EDT
Logout
Accept
Cancel

Serial Port Configuration - Character Generators and Other Devices.

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

● Off ○ Monroe R194 CG ○ Monroe CEMS-0500/1000 ○ Standard TFT ○ VDS ○ Sage Generic CG ○ Sage News Room
○ XBOB CG ○ XBOB4 CG ○ BETABRITE LED Sign ○ Monroe Envoy ○ DM Engineering MSRA/MSRE Audio Switcher

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

Video Output Configuration.

This DASDEC-1EN servers internal CG can generate NTSC video output for originated and forwarded alerts.

☑ **Internal CG full page video output.** ***Enabled.*** *Uncheck to disable.*
Page duration for multi-page display is a fixed number of seconds
5 **Video page duration in seconds for multiple page displays.**
Red outline around Dark Blue-Violet **Video page color**
26 **Video page font size**
Luxi Serif Mono Bold **Video page font name**
Optional custom text for first line of page
□ **Set override alert page title.** ***Disabled.*** *Check to override the default alert page titles.*

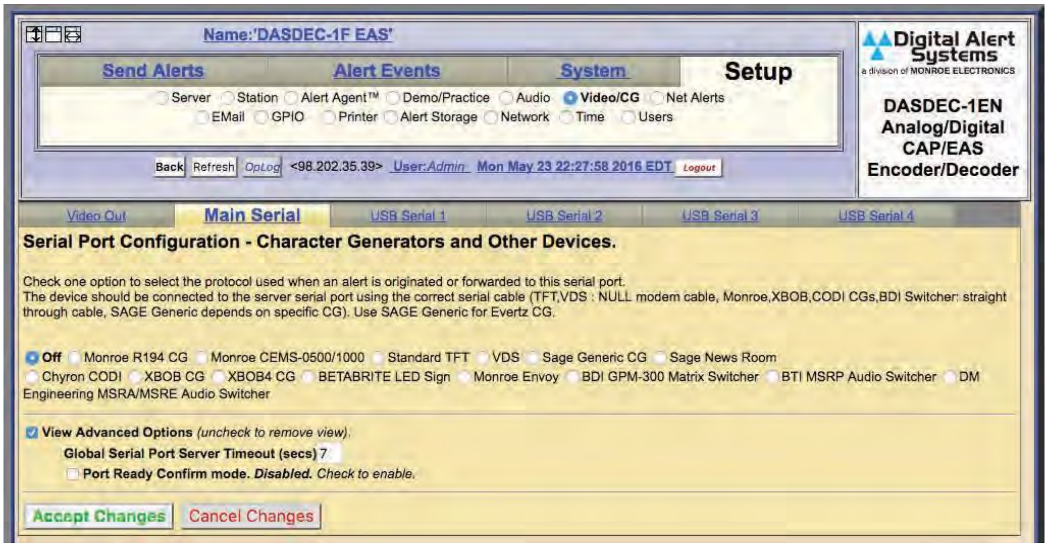
☑ **Linux command prompt on video output.** ***Enabled.*** *Causes four second delay of alert video. Uncheck to disable.*
□ **Serial controlled video duration.** ***Disabled. Alert details video is ended based on the 'Video Duration Control' selections below.*** *Check to enable serial control for ending alert video.*
Video Duration Control ○ Video Duration=Full Alert Duration ● **Video Duration=Alert Audio Duration** ○ Video Duration=Custom Duration

0 :0 **Optional Duration Extension Time (mins:secs).** ***Extends Video Alert Duration up to 1 hr***
Mins:Secs

To setup alert audio repeat loop during video display, set total video duration to at least 1 minute or to full alert duration.

Video/CG Configuration Screen

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



Serial Port Configuration - Character Generators and Other Devices.

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

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

☑ **View Advanced Options** *(uncheck to remove view).*

Global Serial Port Server Timeout (secs) 7

□ **Port Ready Confirm mode.** ***Disabled.*** *Check to enable.*

Video/CG Configuration Screen (Broadcast Mode)

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

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

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

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

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

Main Serial

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

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

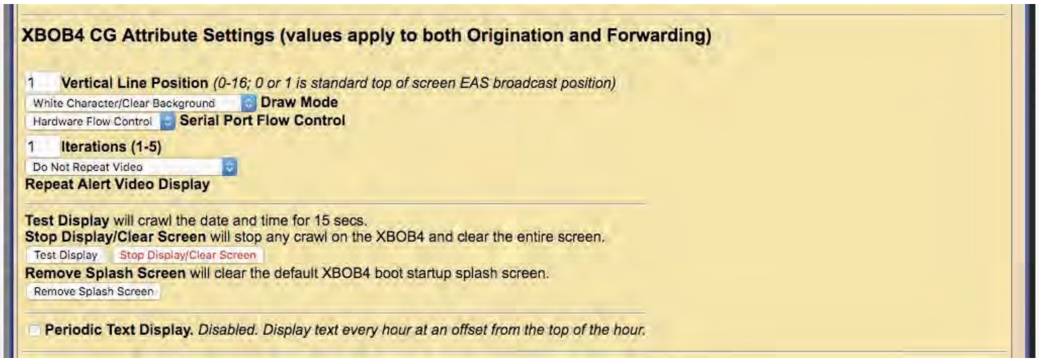
Serial Port Character Generator Configuration

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

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

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

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



XBOB4 CG Attribute Settings (values apply to both Origination and Forwarding)

1 **Vertical Line Position** *(0-16; 0 or 1 is standard top of screen EAS broadcast position)*
White Character/Clear Background **Draw Mode**
Hardware Flow Control **Serial Port Flow Control**
1 **Iterations (1-5)**
Do Not Repeat Video
Repeat Alert Video Display

Test Display will crawl the date and time for 15 secs.
Stop Display/Clear Screen will stop any crawl on the XBOB4 and clear the entire screen.

Remove Splash Screen will clear the default XBOB4 boot startup splash screen.

□ **Periodic Text Display.** *Disabled. Display text every hour at an offset from the top of the hour.*

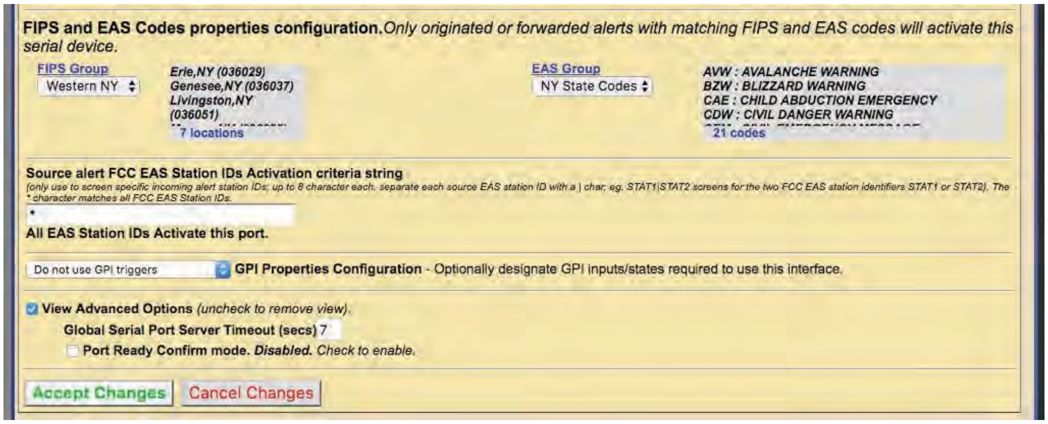
XBOB-4 CG Attribute Settings Section

CG Attribute Settings

The options displayed here depends on the selected CG protocol.

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

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



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

FIPS Group: Western NY

Erie,NY (036029)
Genesee,NY (036037)
Livingston,NY (036051)
7 locations

EAS Group: NY State Codes

AVW : AVALANCHE WARNING
BZW : BLIZZARD WARNING
CAE : CHILD ABDUCTION EMERGENCY
CDW : CIVIL DANGER WARNING
21 codes

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

*

All EAS Station IDs Activate this port.

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

☑ **View Advanced Options** *(uncheck to remove view).*

Global Serial Port Server Timeout (secs) 7

□ **Port Ready Confirm mode.** ***Disabled.*** *Check to enable.*

FIPS and EAS Codes Properties Configuration Section

FIPS and EAS Codes filter configuration

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

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

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

Source alert FCC EAS Station IDs

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

GPI Properties Configuration

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

View Advanced Options

This check box exposes two additional settings:

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

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

USB Serial 1 through 4

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

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

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

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

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

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

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

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

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

Serial port protocols

The supported protocols and their options are listed below:

1. DAS Model R194 CG Attribute Settings

The following attributes are available:

Iterations (1-5)
This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

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

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

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

Stop Display
Click this button to stop the Test Display.

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

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

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

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

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

2. DAS Model CEMS 500/1000 CG Attribute Settings

Repeat Alert Video Display – *Defaults to Do Not Repeat*

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

3. Standard TFT Attribute Settings

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

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

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

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

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

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

Pre/Post Alert Audio extension – *Defaults to disabled*
When enabled, TFT client audio play commands will use pre and post alert audio if they are defined.

In No-Audio mode, hold EOM for audio duration – *Defaults to disabled*
Option is typically used when using a MultiPlayer or another TFT interface is the master. When enabled, TFT client audio play commands will use pre and post alert audio if they are defined.

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

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

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

4. Sage Generic CG Attribute Settings

Serial Port Baud Rate – *Defaults to 9600*
Select 9600 or 19200 baud depending on the remote device requirements.

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

Max text length - *Defaults to 2000*
Maximum number of characters sent to the connected CG. Evertz has a maximum number of 2,047 characters.

Throttle down serial port write speed – *Defaults to disabled*
When Enabled, data is written with pauses between 128 byte blocks. This can be helpful when sending this to devices that cannot do flow control.

Iterations – *Defaults to one. Crawl is done once*
This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

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

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

5. Sage News Room Attribute Settings

Check to run immediate upon matching decoded alert – *Defaults to disabled*
When enabled, data for matching FIPS and EAS filtered alerts is sent to the remote device using the Sage News Room protocol.

Serial Port Baud Rate – *Defaults to 9600.*
Select 9600 or 19200 baud depending on the remote device requirements.

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

Max text length - *Defaults to 4000*
Maximum number of characters sent to the connected device.

Throttle down serial port write speed – *Defaults to disabled*
When Enabled, data is written with pauses between 128 byte blocks. This can be helpful when sending this to devices that cannot do flow control.

6. Chyron CODI CG Attribute Settings

Vertical Position
Set from video scanline 10 (top most) to 440 (bottom).

Font - *Defaults to one*
Set from 1 to 8.

Color – *Defaults to white*

- White
- Blue
- Yellow
- Red
- Magenta
- Cyan
- Green
- Black

Crawl Background - *Defaults to no background banner*

- No background banner
- On (method 1:def banner only)
- On (method 2:vid, banner, vid)

Speed

- 120 Pix/Sec NTSC
- 240 Pix/Sec NTSC
- 360 Pix/Sec NTSC
- 480 Pix/Sec NTSC
- 600 Pix/Sec NTSC
- 720 Pix/Sec NTSC
- 840 Pix/Sec NTSC
- 900 Pix/Sec NTSC
- 1080 Pix/Sec NTSC
- 1200 Pix/Sec NTSC

CODI Serial Port Baud Rate – *Defaults to 9600*
Select 9600 or 19200 baud depending on the remote device requirements.

Text over Video Antialiased – *default enabled*
When enabled, the text is anti-aliases over the video background.

Video Blanking control
May be required for backgrounds on Analog CODI.

When Checked, clears CODI screen prior to message crawl
When enabled, the screen is fully cleared of graphics prior to the EAS text crawl.

When checked, delays CODI message crawl until after EAS audio header & attention
When enabled, the crawl is delayed until after the EAS audio header and attention two-tone signal is played.

Iterations – *Defaults to one. Crawl is done once*

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

Repeat Alert Video Display pull-down

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

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

CODI Test Patterns, Screen Clear, and Reset

Set Test Pattern

Select a test pattern by entering a numeric value between 1 and 22

Display Selected Test Pattern
Click the **Display Selected Test Pattern** button to display the (above) selected test pattern.

Clear CODI Display
Clicking the **Clear CODI Display** button will clear the CODI video output. This is useful after displaying a test pattern.

Reset CODI
Clicking this button will reset the CODI CG.

7. XBOB CG Attribute Settings

Vertical position – *Defaults to one*
Sets the vertical location of the crawl on the screen from 0 (topmost) to 16 (bottom)

Solid black background – *Defaults to enabled*
When Enabled, the crawl text is set to display on top of a black banner.

Iterations – *Defaults to one. Crawl is done once*
This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

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

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

8. XBOB4 CG

Vertical Line position – *Defaults to one*
Sets the vertical location of the crawl on the screen from 0 (topmost) to 16 (bottom)

Draw Mode
Controls the appearance of the crawl displayed on the screen. Choose between the following:

- White Character/Clear Background
- White Character / Black Background
- White Character / Half-tone Background
- Black Character / White background.

Serial Point Flow Control
Select Hardware or Software or None depending upon the hardware support on the remote device.

Iterations – *Defaults to one. Crawl is done once*
This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display – *Defaults to Do Not Repeat*
Select from a set of options for repeating the data write to the remote device after a pause period set from the **Set Alert Video Repetition Period** field. The repeat period has to be at least 2 minutes.

Test Display
Click this button to test the interface with the XBOB4 CG.

Stop Display/Clear Screen
Click this button to stop the Test Display and clear the video output.

Remove Splash Screen
Will clear the default XBOB4 boot startup splash screen.

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

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

Draw Mode
Controls the appearance of the crawl displayed on the screen. Choose one of the four available modes. (see Draw Mode above)

Display Mode
Choose between **Crawl** or **Do Not Crawl**

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

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

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

9. VDS CG Attribute Settings

Select VDS Mode

- Standard VDS840
- StarMU/Star 8
- Sage VDS840 Emulation
- Sage VDS830 Emulation
- VDS830

Serial Port Bit Config

- 8 data, 1 stop bit
- 8 data, 2 stop bit
- 7 data, StarMU/Star 8

Serial Port Flow

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

VDS Serial Port Baud Rate – *Defaults to 9600*
Select 9600 or 19200 baud depending on the remote device requirements.

Vertical position – *Defaults to video 20*
Set from 20 (top most) to 208 (bottom).

Speed – *Defaults to Med*

- Slow
- Medium
- Fast

Crawl Font – *Defaults to one*
Set from 1 to 4.

Char Color – *Defaults to white*

- Clear, key over video
- Yellow
- Bright Green
- Bright Red
- Gray
- Cyan
- Magenta
- Blue
- White
- Bright Cyan
- Bright Magenta
- Bright Blue
- Dull Yellow
- Green
- Red
- Black

Set Color Background by EAS Severity? – *Defaults to disabled.*
When enabled, the text color is determined based on a color selection set for the EAS severity category. Select the desired color for each severity level.

Delay VDS message crawl – *Defaults to disabled*
When enabled, the crawl is delayed until after the EAS audio header and attention two-tone signal is played.

Iterations – *Defaults to one. Crawl is done once*
This value sets the number of times the video alert will display back-to-back. This is not the same as Repeat (below).

Repeat Alert Video Display pull-down

- Do Not Repeat Video
- Repeat Video For Duration of Alert
- Repeat Once

- Repeat Twice
- Repeat 3 Times
- Repeat 4 Times
- Repeat 5 Times
- Repeat 10 Times

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

10. BetaBrite LED Sign Attribute Settings

Check to display immediately upon matching decoded alert
When enabled, matching FIPS and EAS filtered alerts are crawled on the BetaBrite LED display upon decoding. When disabled, matching FIPS and EAS filtered alerts are displayed upon origination and forwarding play-out. Use this feature as a way to post a visual notification that an alert has been decoded.

Stop decoded alert display upon Acknowledgement event
Becomes visible when the **Check to display immediately matching decoded alert** check box is enabled. Clicking this check box will cause the BetaBrite display to clear after the pending alert message is acknowledged.

Max text length – *Default to 4000*
Controls the maximum number of characters sent to the BetaBright LED Sign.

Display Duration Control
The duration of the BetaBrite crawl is set by selecting one of three Display Duration Control radio button options. The duration can be set to the full alert duration, to the alert audio duration, or to a custom duration. The first two options apply to Originated and Forwarded alerts while the third (Custom Duration) option applies to Decoded alerts.

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

Test Display
Click this button to test the interface with the BetaBright. The test consists of crawling the date and time for about 30 seconds.

Stop Display
Click this button to stop any crawl on the BetaBright.

11. BDI GPM-300 Matrix Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

12. BTI MSRP Audio Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

13. DM Engineering MSRA/MSRE Audio Switcher Attribute Settings

Audio Channel Selections – switch these GPM300 channels to EAS during alert audio. Click the desired numbered channels. Use either the Shift or ALT modifier keys when selecting more than one channel.

FIPS and EAS Codes properties configuration

Each of the Serial interface screens contain filtering for both FIPS and EAS codes along with Station ID filtering. Functionally, this means these serial devices can be selectively configured to activate during specific EAS alert, locations and/or origination Station ID's. When selecting "All Locations" from the FIPS Group or "All" from the EAS Group pull-down menus, no filtering will take place.

FIPS and EAS Codes filter configuration

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

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

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

Source alert FCC EAS Station IDs

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

GPI Properties Configuration

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

View Advanced Options

This check box exposes two additional settings:

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

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

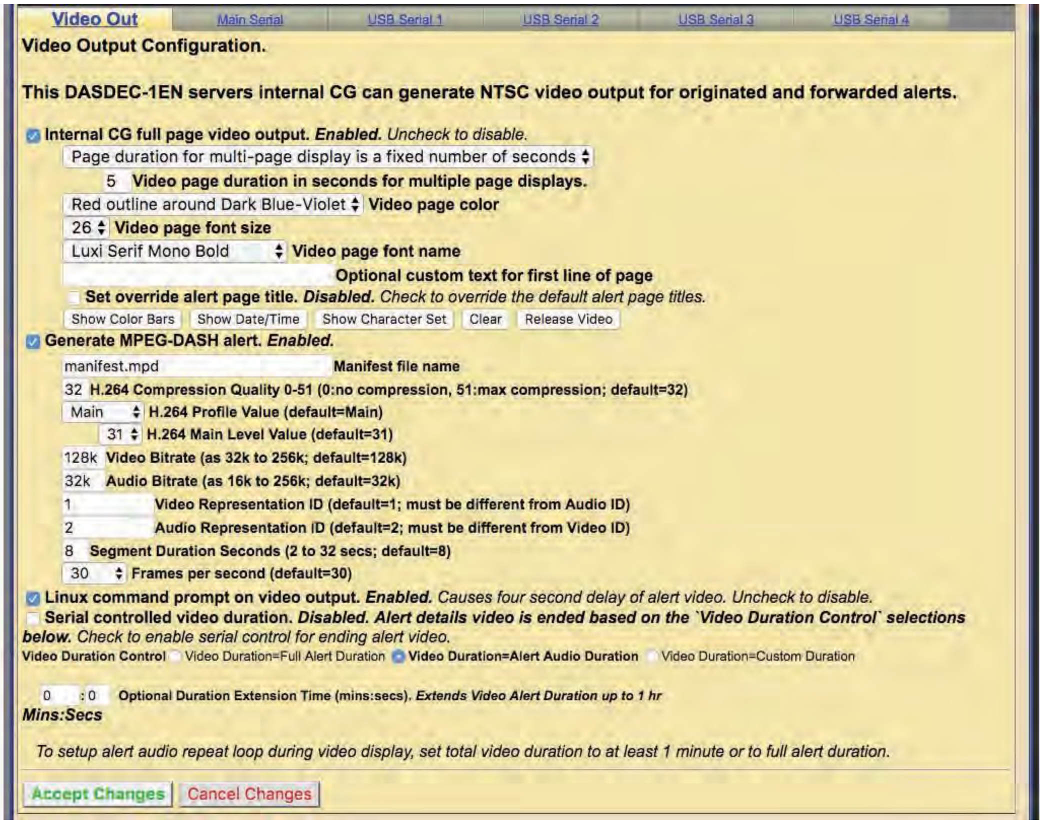
Video Out

The Video Output Configuration sub-tab has three check boxes:

- Internal CG full page video output
- Linux command prompt on video output
- Serial controlled video duration

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

Click **Accept Changes** to apply changes to this page.



Video Output Configuration.

This DASDEC-1EN servers internal CG can generate NTSC video output for originated and forwarded alerts.

☑ **Internal CG full page video output.** ***Enabled.*** *Uncheck to disable.*

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

5 **Video page duration in seconds for multiple page displays.**

Red outline around Dark Blue-Violet **Video page color**

26 **Video page font size**

Luxi Serif Mono Bold **Video page font name**

Optional custom text for first line of page

☐ **Set override alert page title.** ***Disabled.*** *Check to override the default alert page titles.*

☑ **Generate MPEG-DASH alert.** ***Enabled.***

manifest.mpd **Manifest file name**

32 **H.264 Compression Quality 0-51 (0:no compression, 51:max compression; default=32)**

Main **H.264 Profile Value (default=Main)**

31 **H.264 Main Level Value (default=31)**

128k **Video Bitrate (as 32k to 256k; default=128k)**

32k **Audio Bitrate (as 16k to 256k; default=32k)**

1 **Video Representation ID (default=1; must be different from Audio ID)**

2 **Audio Representation ID (default=2; must be different from Video ID)**

8 **Segment Duration Seconds (2 to 32 secs; default=8)**

30 **Frames per second (default=30)**

☑ **Linux command prompt on video output.** ***Enabled.*** *Causes four second delay of alert video. Uncheck to disable.*

☐ **Serial controlled video duration.** ***Disabled. Alert details video is ended based on the `Video Duration Control` selections below.*** *Check to enable serial control for ending alert video.*

Video Duration Control ○ Video Duration=Full Alert Duration ● **Video Duration=Alert Audio Duration** ○ Video Duration=Custom Duration

0 : 0 **Optional Duration Extension Time (mins:secs).** ***Extends Video Alert Duration up to 1 hr***

Mins:Secs

To setup alert audio repeat loop during video display, set total video duration to at least 1 minute or to full alert duration.

Video Out Screen

Note

In current software, running the NTSC video details generator will slow down the start of every alert by a few seconds as the video system is initialized from a VGA console state to a video output state. Depending on the required timing of your on-air system, this can be objectionable. Only enable NTSC video details output if it is needed.

Internal CG full page video output

Use the check box to enable or disable the **Main station** Video Output if licensed and the hardware support is enabled. The EAS device can provide a full screen NTSC analog video display of the current originated or forwarded alert.

Page Duration pull-down
The **Page Duration** has two settings available in this pull-down menu:

- Page duration for multi-page display is a fixed number of second
- Page duration is Video Duration/Number of Pages

Note

When MultiStation mode is enabled, the Video Output toggle for each **station** overrides this **Main station** setting check box! Configure per station alert Video Output on the proper station interface configuration page under **Setup > Decoder > Forwarding**.

Video Page Color pull-down

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

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

Video page font size pull-down

This pull-down menu sets the font size for the video page output. Available sizes range from 16 to 34.

Video page font name pull-down

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

Optional custom text for first line of page

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

Set override alert page title

Video Display Buttons:

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

Show Color Bars – Displays NTSC color bars

Show Date/Time – Displays the current date and time

Show Character Set – Displays a set of characters based on the configured font, size and color.

Clear – Clears the current video output screen to black. Useful when clearing the screen from the previous test buttons.

Release Video – Releases the VGA output from displaying video and returns the VGA screen to the Linux command prompt.

Video Duration Control

Full Alert Duration

Optional Duration Extension

Generate MPEG-DASH alert

A valid MPEG-DASH license key is required for this feature. When enabled, this feature will create MPEG-DASH content of EAS alerts. The following settings are made visible when this feature is enabled:

Manifest file name

Enter the desired name of the manifest (.mpd) file. Make sure to include the .mpd file extension in the file name.

H.264 Compression Quality – Default to 32

This value determines the amount of compression within the H.264 stream. The value of ‘0’ is no compression and the value of 51 is max compression.

H.264 Profile Value – Default to Main

Choose between **Baseline**, **Main** and **High** profiles from this pull-down menu.

H.264 Main Level Value – Default to 31

Choose between the value of 31 or 40 from this pull-down menu.

Video Bitrate – Default to 128k
Enter a Video Bitrate value between 32k to 256k.

Audio Bitrate – Default to 32k
Enter a Video Bitrate value between 16k to 256k.

Video Representation ID – Default to 1
Enter the Representation ID for the video. Must be different from the Audio Representation ID.

Audio Representation ID – Default to 2
Enter the Representation ID for the audio. Must be different from the Video Representation ID.

Segment Duration Seconds – Default to 8
Input the Segment Duration Seconds in the provide text box. Value should be between 2 and 32.

Frames per Second – Default to 30
Choose between **24**, **29.97** and **30** frames per second from this pull-down menu.

Linux command prompt on video output

Forces the video output to display the command line prompt. Enabling this option will cause a four second delay in the alert video.

Serial controlled video duration

This setting is either enabled or disabled by checking/unchecking the check box.

- When enabled, the screen states, **'Alert details video is ended when serial protocol controlled EOM audio finishes. Uncheck for other video control options.'**
- When disabled, as shown in the above screen shot, the message changes to 'Alert details video is ended based on the **`Video Duration Control` selections below.'** and displays the following settings:

Video Duration Control: Select which of the three radio buttons is needed for Video Duration Control:

- Video Duration=Full Alert Duration
- Video Duration=Alert Audio Duration
- Video Duration=Custom Duration

Custom Duration allows for setting the exact video duration in minutes and seconds, up to one extra hour. One use for this option is to provide for a minimum video duration on short Weekly Test alerts.

Optional Duration Extension Time
These text fields allow users to extend the video alert duration up to 1 hour.

ALERT AGENT™ SETUP

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

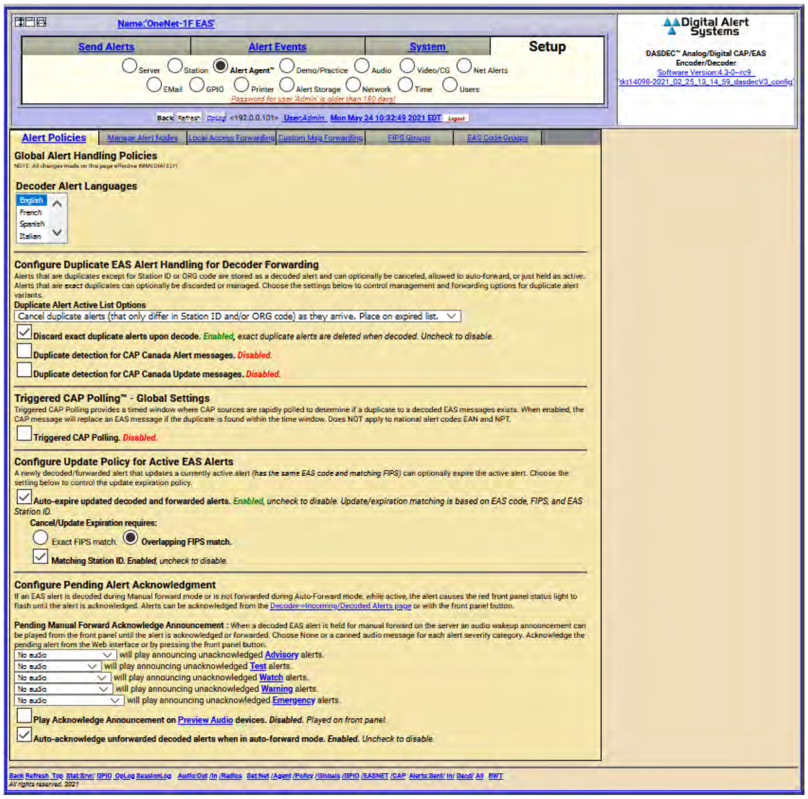
Sub-Tab	Description
Alert Policies	Configure the decoder alert language, duplicate EAS handling, update policy for active EAS alerts and pending alert acknowledgment.
Manage Alert Nodes	Create, edit, test and delete Alert Nodes.
Local Access Forwarding	Create custom text for Civil Emergency Messages.
Custom Msg Forwarding	Configure custom message forwarding
FIPS Groups	Create, edit, manage, and delete FIPS Location Groups along with encoder FIPS locations.
EAS Code Groups	Create, edit, manage, and delete EAS Code Groups along with encoder EAS codes.

Alert Policies

The Alert Policies sub-tab is broken into four sections; Decoder Alert Language, Configure Duplicate EAS Alert Handling for Decoder Forwarding, Configure Update Policy for Active EAS Alerts, and Configure Pending Alert Acknowledgment (this sub-tab requires a Plus Package License Key). All changes to settings in this screen are immediate.

Attention
All changes to configuration settings on the Alerts Policies screen take effect immediately.

Alert Policies Screen



Name:'OneNet-1F EAS'

Send Alerts | Alert Events | System | Setup

○ Server ○ Station ● Alert Agent™ ○ Demo/Practice ○ Audio ○ Video/CG ○ Net Alerts
○ EMail ○ GPIO ○ Printer ○ Alert Storage ○ Network ○ Time ○ Users

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

Back Refresh OpLog <192.0.0.101> User:Admin Mon May 24 10:32:49 2021 EDT Logout

Digital Alert Systems
DASDEC™ Analog/Digital CAP/EAS Encoder/Decoder
Software Version:4.3-0--rc9
'tkt14098-2021_02_25_13_14_59_dasdecV3_config'

Alert Policies | Manage Alert Nodes | Local Access Forwarding | Custom Msg Forwarding | FIPS Groups | EAS Code Groups

Global Alert Handling Policies
NOTE: All changes made on this page effective IMMEDIATELY!

Decoder Alert Languages
English
French
Spanish
Italian

Configure Duplicate EAS Alert Handling for Decoder Forwarding
Alerts that are duplicates except for Station ID or ORG code are stored as a decoded alert and can optionally be canceled, allowed to auto-forward, or just held as active. Alerts that are exact duplicates can optionally be discarded or managed. Choose the settings below to control management and forwarding options for duplicate alert variants.

Duplicate Alert Active List Options
Cancel duplicate alerts (that only differ in Station ID and/or ORG code) as they arrive. Place on expired list.

☑ **Discard exact duplicate alerts upon decode.** *Enabled, exact duplicate alerts are deleted when decoded. Uncheck to disable.*
☐ **Duplicate detection for CAP Canada Alert messages.** *Disabled.*
☐ **Duplicate detection for CAP Canada Update messages.** *Disabled.*

Triggered CAP Polling™ - Global Settings
Triggered CAP Polling provides a timed window where CAP sources are rapidly polled to determine if a duplicate to a decoded EAS messages exists. When enabled, the CAP message will replace an EAS message if the duplicate is found within the time window. Does NOT apply to national alert codes EAN and NPT.

☐ **Triggered CAP Polling.** *Disabled.*

Configure Update Policy for Active EAS Alerts
A newly decoded/forwarded alert that updates a currently active alert *(has the same EAS code and matching FIPS)* can optionally expire the active alert. Choose the setting below to control the update expiration policy.

☑ **Auto-expire updated decoded and forwarded alerts.** *Enabled, uncheck to disable. Update/expiration matching is based on EAS code, FIPS, and EAS Station ID.*

Cancel/Update Expiration requires:
○ Exact FIPS match. ● **Overlapping FIPS match.**
☑ **Matching Station ID.** ***Enabled**, uncheck to disable.*

Configure Pending Alert Acknowledgment
If an EAS alert is decoded during Manual forward mode or is not forwarded during Auto-Forward mode, while active, the alert causes the red front panel status light to flash until the alert is acknowledged. Alerts can be acknowledged from the Decoder->Incoming/Decoded Alerts page or with the front panel button.

Pending Manual Forward Acknowledge Announcement : When a decoded EAS alert is held for manual forward on the server an audio wakeup announcement can be played from the front panel until the alert is acknowledged or forwarded. Choose None or a canned audio message for each alert severity category. Acknowledge the pending alert from the Web interface or by pressing the front panel button.

No audio will play announcing unacknowledged Advisory alerts.
No audio will play announcing unacknowledged Test alerts.
No audio will play announcing unacknowledged Watch alerts.
No audio will play announcing unacknowledged Warning alerts.
No audio will play announcing unacknowledged Emergency alerts.

☐ **Play Acknowledge Announcement on Preview Audio devices.** ***Disabled.** Played on front panel.*
☑ **Auto-acknowledge unforwarded decoded alerts when in auto-forward mode.** ***Enabled.** Uncheck to disable.*

Back Refresh Top Stat:Srvr/ GPIO OpLog SessionLog Audio:Out /In /Radios Set:Net /Agent /Policy /Globals /GPIO /EASNET /CAP Alerts:Sent/ In/ Decd/ All RWT
All rights reserved. 2021

Decoder Alert Languages

This setting enables users to select the languages used within the EAS device. The default is English. Multiple languages may be selected using the SHIFT or CTRL keys.

Configure Duplicate EAS Alert Handling for Decoder Auto-Forwarding

An incoming EAS alert that is an exact duplicate of a previously decoded alert, is completely discarded and a message is logged in the operation log. EAS alerts that are duplicates except for Station ID or ORG code are stored as a decoded alert and can be optionally auto-forwarded or held. Use the selector to choose the setting to control manual or auto-forwarding for these alerts.

Triggered CAP Polling ™ - Global Settings

When enabled, Triggered CAP Polling provides a timed window where CAP sources are rapidly polled to determine if a duplicate to a decoded EAS message exists. To enable, check the **Triggered CAP Polling** check box. Uncheck to disable. The **Global Window** time defines the amount of time after an EAS message is decoded the EAS device will rapidly poll the CAP server for a duplicate EAS message. If a duplicate CAP message is found within the configured time window, the initial EAS message will be dequeued and replaced with the more detailed CAP message. This feature does not apply to the EAN and NPT national codes. Additional Triggered CAP Polling controls can be found for individual Alert Nodes.

NEW **New Feature**
Version 4.0 software introduces Triggered CAP Polling.

Configure Update Policy for Active EAS Alerts

This option allows you to expire an active alert when a new alert is decoded and updates the previous alert. When enabled, you can choose what requirements the new alert must have to expire the previous active alert.

The following is an example of this situation: Two local radio stations are being monitored. Both send out a monthly test for the same FIPS codes, with the same start time and duration, but the stations have changed the station ID. The alerts arrive several minutes apart. The EAS device has been set to auto-forward monthly tests to the given FIPS codes. The first decoded monthly test is forwarded automatically. The user has configured the duplicate alert handling to NOT auto-forward duplicate alerts that differ in Station ID or ORG code. The second alert is decoded, but is held for manual forward.

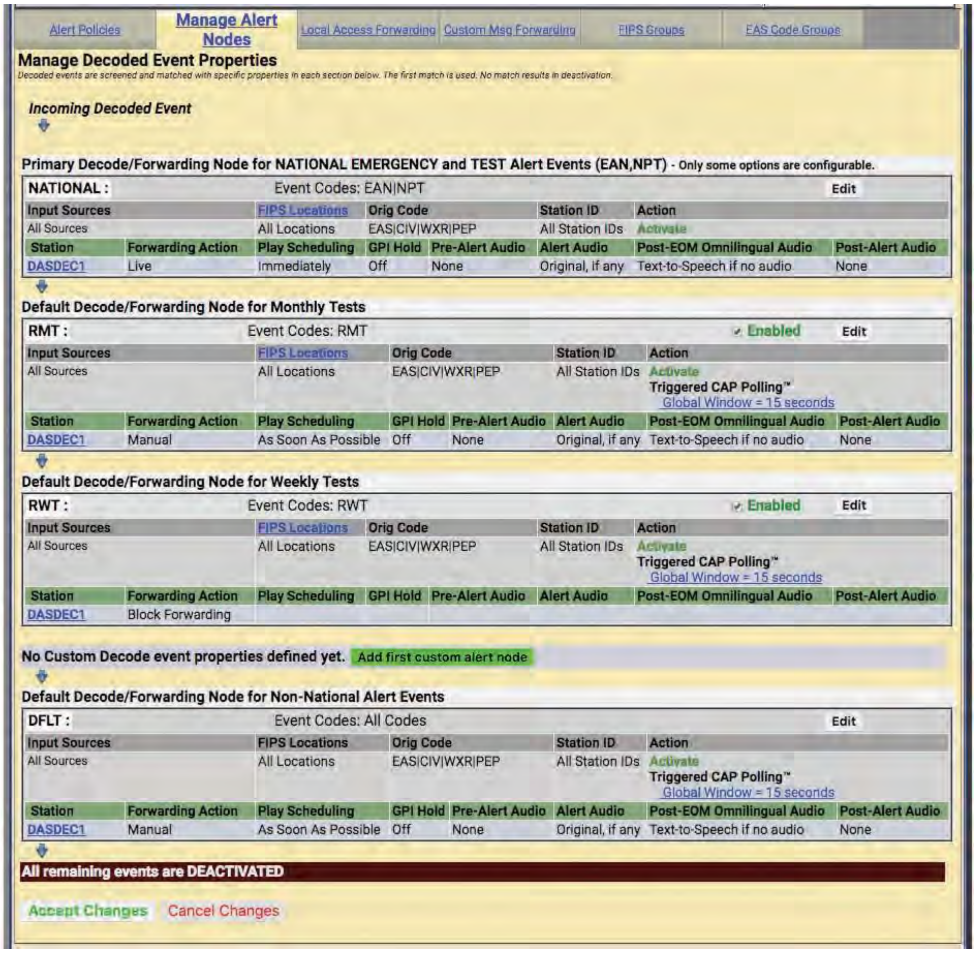
Configure Pending Alert Acknowledgment *(Requires a Plus Package License Key)*

When an EAS alert is decoded during Manual forward mode, while active, it causes the red front panel status light to flash until the alert is *acknowledged*. Alerts can be *acknowledged* from the **Alert Events > Incoming/Decoded Alerts** screen or by pressing the front panel button. In addition, some configuration options are associated with alert acknowledgment.

> **Pending Manual Forward Acknowledge Announcement**
> Each type of alert category can be configured to play-out an audio announcement on the front panel speaker during the time the alert is manually pending forward and before it has been acknowledged. Use the provided selectors to control audio announcement for each alert severity category.
>
> **Play Acknowledge Announcement on Preview Audio devices**
> The Audio Preview Devices are configured in the **Setup > Audio > Audio Output Levels/Test** screen. By checking this box, the Acknowledgment Announcement plays out the selected Audio Preview Devices. A Preview Audio hyperlink is provided to navigate to the Audio Preview Devices settings.
>
> **Auto-acknowledge unforwarded decoded alerts when in auto-forward mode**
> Checking this box automatically acknowledges any unforwarded decoded alerts while the EAS device is in auto-forward mode. The Auto-Forward Mode setting is located at **Setup > Station > Global Options** screen in the Global Forwarding Settings section.
>
> **Alert audio, if any, will play on the front panel speaker when the front panel button is pressed to acknowledge an unforwarded decoded alert**
> All EAS device versions provide a check box to select whether the alert voice audio message is played during Front Panel button acknowledgment of a current, active non-forwarded alert.

Manage Alert Nodes

Alert Nodes is a new concept in managing incoming EAS messages. The Alert Agent continuously monitors all incoming sources; analog – audio/radios, and digital - EAS-Net™ / CAP/ etc. then takes action if the input meets the specified criteria. To set the various properties, the Alert Agent uses Alert Nodes. An Alert Node allows the simple selection of alerting properties and defines an action based on the incoming criteria.



Manage Decoded Event Properties

Decoded events are screened and matched with specific properties in each section below. The first match is used. No match results in deactivation.

Incoming Decoded Event

Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN,NPT) - Only some options are configurable.

NATIONAL : Event Codes: EAN|NPT — Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action
All Sources	All Locations	EAS|CIV|WXR|PEP	All Station IDs	Activate

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Live	Immediately	Off	None	Original, if any	Text-to-Speech if no audio	None

Default Decode/Forwarding Node for Monthly Tests

RMT : Event Codes: RMT — ☑ Enabled — Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action
All Sources	All Locations	EAS|CIV|WXR|PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Manual	As Soon As Possible	Off	None	Original, if any	Text-to-Speech if no audio	None

Default Decode/Forwarding Node for Weekly Tests

RWT : Event Codes: RWT — ☑ Enabled — Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action
All Sources	All Locations	EAS|CIV|WXR|PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Block Forwarding						

No Custom Decode event properties defined yet. Add first custom alert node

Default Decode/Forwarding Node for Non-National Alert Events

DFLT : Event Codes: All Codes — Edit

Input Sources	FIPS Locations	Orig Code	Station ID	Action
All Sources	All Locations	EAS|CIV|WXR|PEP	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Manual	As Soon As Possible	Off	None	Original, if any	Text-to-Speech if no audio	None

All remaining events are DEACTIVATED

Manage Alert Nodes Screen

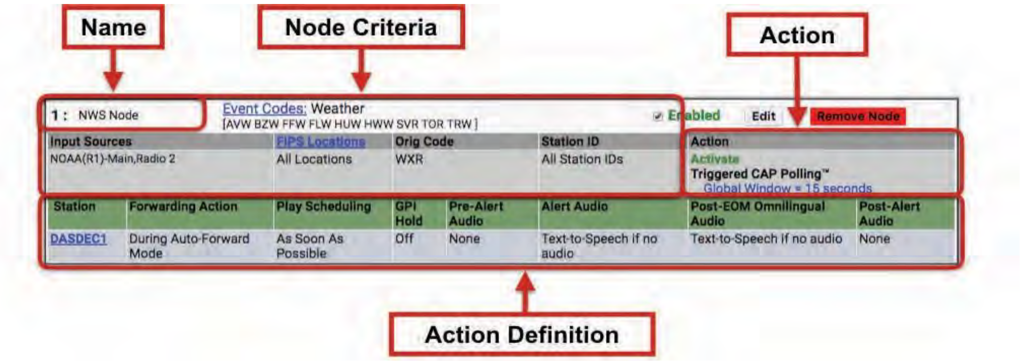
The Manage Alert Nodes screen is divided into two sections: an Alert Node test (top of screen) and a list of Alert Nodes in order of priority (from top to bottom). Incoming decoded events will be evaluated by the top Alert Node and will continue down the list. The EAS device is pre-configured with four Alert Nodes – three are based on required alert events/tests: **National** (EAN & NPT), **Required Monthly Test** (RMT), and **Required Weekly Test** (RWT). These three required Alert Nodes cannot be deleted. The fourth Alert Node is named DFLT (or Default).

An example of the power and flexibility of Alert Nodes:

> An EAS device is configured to monitor three radio sources; LP-1, LP-2, and the National Weather Service (NWS). The NWS source covers your service area as well as areas outside your service area, along with providing Required Weekly Tests. The RWT's broadcast by this NWS source duplicate RWT's received on LP-1. The NWS source is providing weather alerts for your service area and others while also providing duplicate RWT's. An Alert Node can be configured to only forward weather-related EAS alerts for your service area that are received on the NWS source. The Alert Node will ignore all other EAS alerts received from this source.

Before demonstrating how to configure an Alert Node for this example, below are some basic elements related to Alert Nodes.

Note
The Alert Node sub-tab requires the use of the Accept Changes button for any changes to take effect. There are Accept Changes and Cancel Change buttons at both the top and bottom of this screen.



1 : NWS Node

Event Codes: Weather
[AVW BZW FFW FLW HUW HWW SVR TOR TRW]

Input Sources	FIPS Locations	Orig Code	Station ID	Action
NOAA(R1)-Main,Radio 2	All Locations	WXR	All Station IDs	Activate Triggered CAP Polling™ Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	During Auto-Forward Mode	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

Alert Nodes are simple to configure and have four basic components:

- Name
- Node Criteria
- Action
- Action Definition

Name

When adding a new Alert Node, the EAS device creates an Alert Node name (a combination of letters and numbers). Edit this name to be more descriptive of the Node's purpose. To the left of the name is a number that represents the order of the Alert Node. Changing the order of the Alert Node changes the Alert Nodes' number.

Node Criteria

At the core of each Alert Node is the Node Criteria where the decoded EAS information is processed and matched against the criteria settings established in the following five areas:

- Input Sources
- FIPS Location Codes
- EAS Event Codes
- Originator Codes
- Station ID

Input Sources

Any combination of input sources can be selected – a single radio source or a combination (radios, CAP/IPAWS, and/or EAS-NET™ sources). Select the desired input sources from the pull-down menu by clicking each item. Pressing the CTRL key while clicking input sources will allow the user to select multiple sources.

FIPS Location Codes

Clicking on the FIPS Locations pull-down menu will reveal all available FIPS Location Groups configured in the EAS device. Select the desired FIPS Location Group by clicking on it. The pull-down menu includes an **All Locations** selection as the default setting for cases when no specific FIPS Location Code Group is needed. FIPS Location Groups are configured within the **Setup > Alert Agent™ > FIPS Groups** sub-tab and can quickly be accessed by clicking the **FIPS Locations** hyperlink. Only one selection may be made from this pull-down menu.

EAS Event Codes

At the top of each Alert Node is an **Event Codes** pull-down menu where available EAS Code Groups are selected. The pull-down menu includes an **All** selection as the default setting when no specific EAS Event Code Group is needed. EAS Event Code Groups are configured within the **Setup > Alert Agent™ > EAS Code Groups** sub-tab and can quickly be accessed by clicking the **Event Codes** hyperlink. Only one selection may be made from this pull-down menu.

Orig (Originator) Codes

This is a three character ASCII code found in an EAS header which denotes the source of an EAS alert. Select one or a combination of Originator Codes from the list. Pressing the CTRL key while clicking input sources will allow the user to select multiple sources. The current FCC rules define four available ORG Codes:

- EAS – Broadcast Station/Cable System
- CIV – Civil Authority
- WXR – National Weather Service
- PEP – Primary Entry Point

Station ID

Found in the EAS header is the identification of the specific station that originated the EAS alert. Entering the desired station ID into this text field will allow EAS alerts that originate from this station ID to activate this Alert Node. Using an asterisk (*) will allow all station IDs.

Action

There are two available Action options found in this pull-down menu:

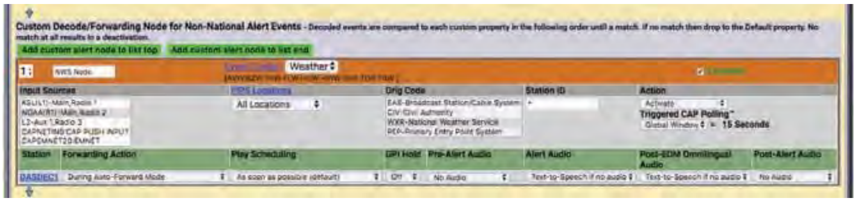
- Deactivate/Log Only
- Activate

The **Deactivate/Log Only** option will log the incoming EAS alert and perform no further actions. The Action Definition interface will not be visible and no actions may be configured.

Selecting **Activate** will make the Action Definition interface visible and configurable.

Triggered CAP Polling™ pull-down menu provides three options for node-specific configuration settings:

- Off *(will not initiate this feature for the given node criteria)*
- Global Window *(uses global time window settings)*
- Node Window *(enables use of custom time window settings)*



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

Add custom alert node to list top
Add custom alert node to list end
1
NWS Node
Event Codes
Weather

Input Sources	FIPS Locations	Orig Code	Station ID	Action
ASU(L1)-Main Radio 1 NOAA(R1)-Main Radio 2 L2-Aux 1 Radio 3 CAPNETIMS CAP PUSH INPUT CAPDMNET20 DMNET	All Locations	EAS-Broadcast Station/Cable System CIV-Civil Authority WXR-National Weather Service PEP-Primary Entry Point System	*	Activate Triggered CAP Polling™ Global Window = 15 Seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	During Auto-Forward Mode	As soon as possible (default)	Off	No Audio	Text-to-Speech if no audio	Text-to-Speech if no audio	No Audio

Editing a Custom Alert Node

Action Definition

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

- Forwarding Action
- GPI Hold
- Pre-Alert Audio
- Alert Audio
- Post EOM Omnilingual Audio
- Post-Alert Audio

Forwarding Action

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

- **Block Forwarding** – will NOT forward the EAS alert defined in this Alert Node.
- **Manual** – requires manual forwarding of the EAS alert defined in this Alert Node (GPI or manual forwarding)
- **During Auto-Forward Mode** – will automatically forward the EAS alert defined in this Alert Node when the station is in Auto-Forward Mode. When in Manual Forward Mode, users will need to manually forward the EAS alert via a GPI or web interface.
- **Force Immediately** – forces an immediate forward of the EAS alert defined in this Alert Node.
- **Force by offset time and before expiration** – displays offset settings (in minutes & seconds). Delays the forwarding of the EAS alert defined in this Alert Node by the entered offset time. If the offset pushes the EAS alert past its expiration time, the offset time will be reduced so as to forward the EAS alert within the expiration time. This alert may be forced by manual means (GPI or manual means).

Play Scheduling

When selecting any of the above **Forwarding Actions** besides Block Forwarding, the **Play Scheduling** pull-down menu becomes available.

- **As soon as possible** (default) – after the incoming alert message is decoded, it is played - beginning at the start time of the alert message.
- **As late as possible** – after the incoming alert message is decoded, it is held and then played just before the end of the valid alert time period.
- **Next minute interval** (MM:00) – the alert playout is delayed until the top of the next 60 second interval.
- **Next 30 sec. interval** (MM:00, 30) – the alert playout is delayed until the next 30 second interval.
- **Next 20 sec. interval** (MM:00, 20, 40) – the alert playout is delayed until the next 20 second interval.
- **Next 15 sec. interval** (MM:00, 15, 30, 45) – the alert playout is delayed until the next 15 second interval.
- **Next 10 sec. interval** – the alert playout is delayed until the next 10 second interval.
- **Immediately** – after the incoming alert message is decoded, it is played immediately - ignoring the start time of the alert message.

GPI Hold

In certain situations, it is desirable and acceptable to delay the forwarding of EAS alerts so as to not interfere with certain programming (i.e. commercial content). GPI closures can be employed to hold off EAS alerts through automatic or manual means. Go to the **Setup > GPIO** screen for GPI settings.

Pre-Alert Audio

Audio WAV files can be uploaded to the EAS device and played prior to the EAS alert audio. This pull-down menu displays all the available audio WAV files stored on the EAS device. Select the desired audio WAV file by clicking it within the list. The selected file will play prior to the EAS alert defined within this Alert Node. Audio WAV files can be uploaded from the **Setup > Audio > Audio Output Levels/Test** screen.

Alert Audio

Enables multiple options for alert audio.

- **Original Audio** – plays the original alert audio contained within the EAS alert
- **Text-to-Speech if no audio** – creates and plays a text-to-speech audio file (based on the EAS alert text) if no audio file is available to play. A premium voice(s) is recommended when using this feature.
- **Text-to-Speech only** – ignores any original alert audio and forces the creation and playout of text-to-speech audio
- **Uploaded Audio WAV files** – a list of uploaded audio WAV files is available from the pull-down menu to be used during the Alert Audio section of the EAS message.

Note
In most situations, the original alert audio or text-to-speech audio are preferred. However, uploaded audio WAV files are frequently used for regular EAS tests such as the RMT. In this way the FCC EAS rules can be satisfied along with providing better quality and branded audio to the viewers.

Post EOM Omnilingual Audio

This setting is only available with a valid OmniLingual™ Enable Key.

- **Original Audio** – plays the secondary language audio file contained within the EAS alert (CAP only)
- **Text-to-Speech if no audio** – creates and plays a text-to-speech audio file (based on the EAS alert text) if no secondary audio file is available to play. A premium voice(s) is recommended when using this feature.
- **Text-to-Speech only** – ignores any secondary audio files and forces the creation and playout of text-to-speech audio. This selection will provide a translation of the English text to the configured Extended Alert Languages found in the **Setup > Station > Main** sub-tab.

Post-Alert Audio

Audio WAV files can be uploaded to the EAS device and played after the EAS alert audio. This pull-down menu displays all the available audio WAV files stored on the EAS device. Select the desired file by clicking it in the list. The selected file will play after the EAS alert defined within this Alert Node. Audio WAV files can be uploaded from the **Setup > Audio > Audio Output Levels/Test** screen.

Enabled

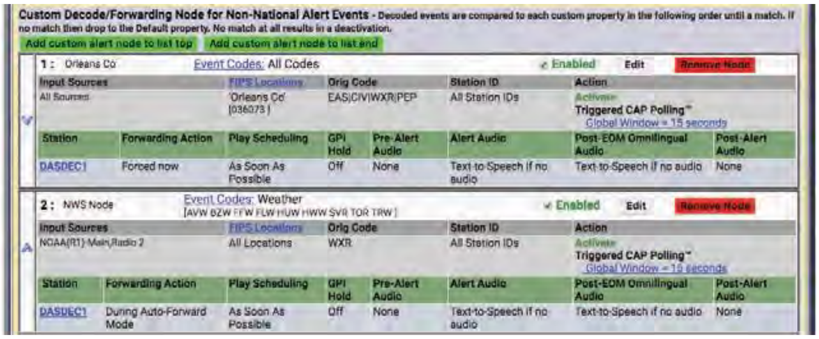
All Alert Nodes (except for the National and DFLT) have an **Enabled** check box that allows users to enable/disable that Alert Node.

Edit

Clicking the **Edit** button on any Alert Node will allow the user to modify the settings for that particular node.

Remove Node

Each Custom Alert Node has a red **Remove Node** button. This button will delete the corresponding Alert Node. After clicking the **Remove Node** button, the selected Alert Node will be removed from the web interface. Click the **Accept Changes** button to finalize the deletion. This deletion cannot be undone after the **Accept Changes** button has been used. Selecting the **Cancel Changes** button before clicking the **Accept Changes** button will restore the removed node.


Add custom alert node to list top
Add custom alert node to list end
Edit
Remove Node
Edit
Remove Node

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

1 : Orleans Co   Event Codes: All Codes   ✓ Enabled

Input Sources	FIPS Locations	Orig Code	Station ID	Action
All Sources	'Orleans Co' [036073]	EAS|CIV|WXR|PEP	All Station IDs	Activate Triggered CAP Polling* Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Forced now	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

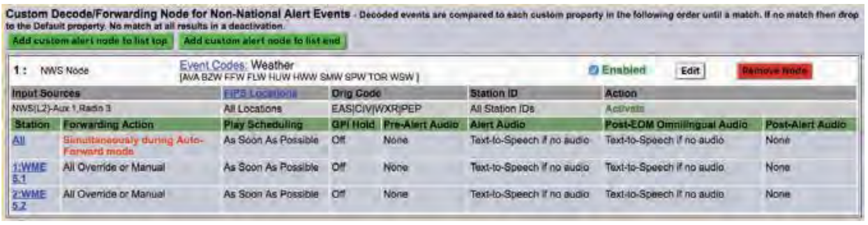
2 : NWS Node   Event Codes: Weather [AVW BZW FFW FLW HUW HWW SVR TOR TRW]   ✓ Enabled

Input Sources	FIPS Locations	Orig Code	Station ID	Action
NOAA(R1)-Main,Radio 2	All Locations	WXR	All Station IDs	Activate Triggered CAP Polling* Global Window = 15 seconds

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	During Auto-Forward Mode	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

Priority of Alert Nodes

Alert Nodes are placed in order of priority (from top to bottom). The Alert Node at the top of the list is processed first, followed by the next node down until each EAS alert reaches the DFLT Alert Node at the bottom of the screen. This is important to understand because an incoming EAS alert might meet the Node Criteria for multiple Alert Nodes. When this happens, only the first node in the priority list will perform the Action Definition of that node. Subsequent Alert Nodes with matching Node Criteria will not be processed. To make sure the Alert Nodes are in the correct order, test them with the Test Node Interface (see below). The required Alert Nodes are found at the top (National, RMT, & RWT) and bottom (DFLT) with the Custom Alert Nodes in between them. These are required nodes, but can be disabled. Changes to the order of Custom Alert Nodes are performed by clicking the up and down arrows located at the far left of each node. The order of required Alert Nodes cannot be modified.


Add custom alert node to list top
Add custom alert node to list end
Edit
Remove Node

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

1 : NWS Node   Event Codes: Weather [AVA BZW FFW FLW HUW HWW SMW SPW TOR WSW]   ☑ Enabled

Input Sources	FIPS Locations	Orig Code	Station ID	Action
NWS(L2)-Aux 1,Radio 3	All Locations	EAS|CIV|WXR|PEP	All Station IDs	Activate

Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
All	Simultaneously during Auto-Forward mode	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None
1:WME 5.1	All Override or Manual	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None
2:WME 5.2	All Override or Manual	As Soon As Possible	Off	None	Text-to-Speech if no audio	Text-to-Speech if no audio	None

MultiStation Mode

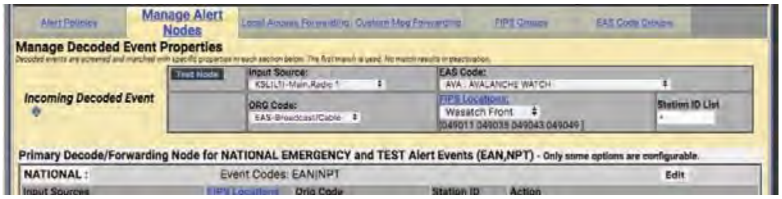
When utilizing MultiStation Mode, Alert Nodes will enable separate Alert Definition settings for each station. When a Node Criteria is matched with the incoming EAS alert, each stations' Alert Definition settings can be configured separately.

Forwarding Action, Play Scheduling, GPI Hold, Pre-Alert Audio, Alert Audio, Post-EOM Omnilingual Audio, and Post-Alert Audio settings can be defined for each station. This enables each station to customize how to handle the playout of the incoming alert and what audio is associated with that alert message.

To create a Custom Decode/Forwarding Alert Node:

- Click the green **Add custom alert node** button found below the RWT node. If this is the first custom node, there are three available button options:

  - Add first custom alert node
  - Add custom alert node to list top
  - Add custom alert node to list end
- Once a new Alert Node is added, modify it by clicking the **Edit** button for that node.
- Assign a descriptive name
- Configure the desired Node Criteria
- Select the appropriate Action (Deactivate/Log Only or Activate)
- Configure the Action Definition settings
- Click the **Accept Changes** button



Manage Decoded Event Properties

Decoded events are screened and matched with specific properties in each section below. The first match is used. No match results in deactivation.

Incoming Decoded Event

Input Source: KSL|LTI-Main,Radio 1

EAS Code: AVA : AVALANCHE WATCH

ORG Code: EAS-Broadcast/Cable

FIPS Locations: Wasatch Front [049011 049035 049043 049049]

Station ID List: *

Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN,NPT) - Only some options are configurable.

NATIONAL : Event Codes: EAN|NPT

Input Sources FIPS Locations Orig Code Station ID Action

Test Node Interface Section

Test Node Interface

After creating new Alert Nodes, it is a good idea to test if they are configured properly. The Test Node interface was created for this purpose. It is located at the top of the **Manage Alert Nodes** sub-tab and has five settings and an action button along with a results field. This test simulates the conditions of an incoming EAS alert against the list of configured Alert Nodes. The test starts at the top of the list (NATIONAL) – stopping when it finds the first Alert Node with a matching Node Criteria.

The first step in running an Alert Node test is to input the test settings. They are as follows:

Input Source

This pull-down menu contains all the available sources (radios, CAP/IPAWS, and EAS-NET™, etc.) where an alert might be received. Select a source by clicking on it. Only one source may be selected when testing an Alert Node.

EAS Code

Select the desired EAS Code from this pull-down menu. Only one EAS Code may be selected.

ORG Code

Click on the appropriate Originator (ORG) Code. Only one ORG Code may be selected.

FIPS Locations

This pull-down displays a list of available FIPS Groups. Select the desired FIPS Group by clicking on it. Only one FIPS Group may be selected.

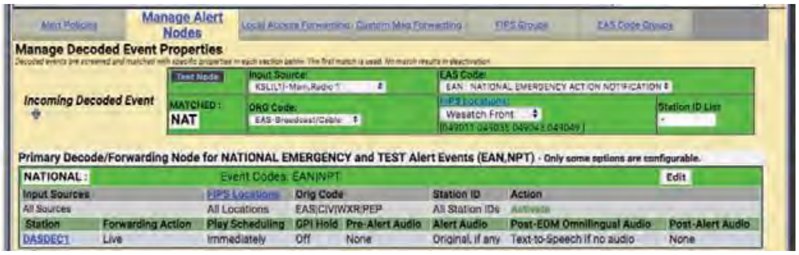
Station ID List

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

Test Node

The Test Node button is used when all the test criteria has been entered (above). Click it to start the test.

Results Field
Located in the lower left corner of the Test Node interface is a blank gray box (below the Test Node button). The results of each test will be displayed here. When a match is found, the Test Node interface and the matching Alert Node will turn green and the results field will contain the word 'MATCHED' along with the name of the matching Alert Node. (See example below)



Manage Decoded Event Properties
Decoded events are screened and matched with specific properties in each section below. The first match is used. No match results in deactivation.

Incoming Decoded Event

Test Node
MATCHED : NAT
Input Source: KSL(L1)-Main,Radio 1
ORG Code: EAS-Broadcast/Cable
EAS Code: EAN - NATIONAL EMERGENCY ACTION NOTIFICATION
FIPS Locations: Wasatch Front (049011 049035 049043 049049)
Station ID List: *

Primary Decode/Forwarding Node for NATIONAL EMERGENCY and TEST Alert Events (EAN,NPT) - Only some options are configurable.

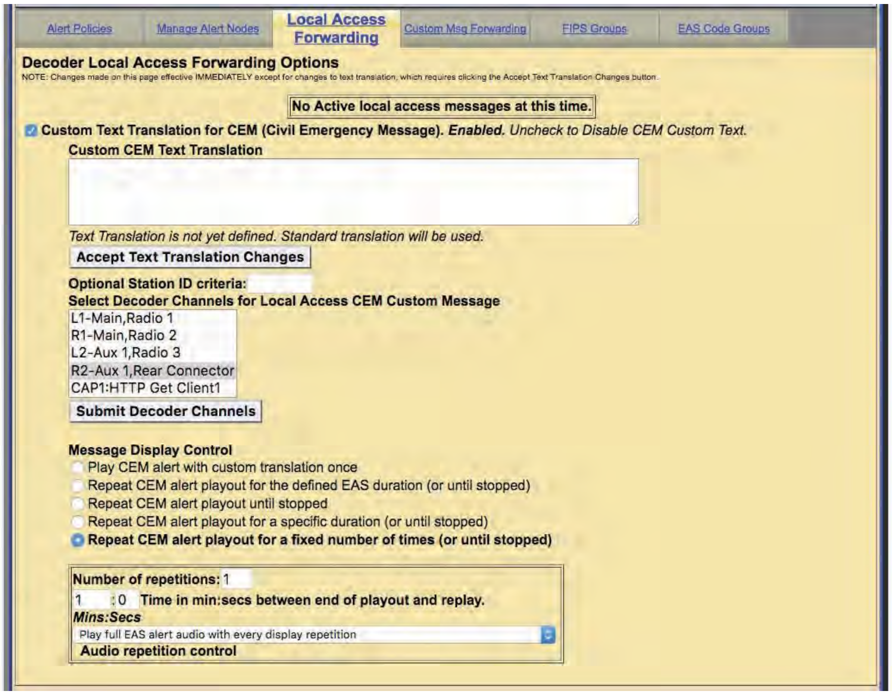
NATIONAL : Event Codes: EAN|NPT Edit

Input Sources		FIPS Locations	Orig Code		Station ID	Action	
All Sources		All Locations	EAS|CIV|WXR|PEP		All Station IDs	Activate	
Station	Forwarding Action	Play Scheduling	GPI Hold	Pre-Alert Audio	Alert Audio	Post-EOM Omnilingual Audio	Post-Alert Audio
DASDEC1	Live	Immediately	Off	None	Original, if any	Text-to-Speech if no audio	None

Test Node Interface Results

Local Access Forwarding

The **Decoder Local Access Forwarding** configuration sub-tab is used to configure customized forwarding play-out for decoded CEM (Civil Emergency Message) EAS alerts. This mode allows for custom alert translation text and repetition control when a CEM alert is auto-forwarded after being decoded from specific decoder channels and optionally, from a specific EAS source station (as based on decoded station ID). The mode is enabled using the check box **Custom Text Translation for CEM** (Civil Emergency Message).



Decoder Local Access Forwarding Options
NOTE: Changes made on this page effective IMMEDIATELY except for changes to text translation, which requires clicking the Accept Text Translation Changes button.

No Active local access messages at this time.

☑ Custom Text Translation for CEM (Civil Emergency Message). *Enabled.* *Uncheck to Disable CEM Custom Text.*

Custom CEM Text Translation

Text Translation is not yet defined. Standard translation will be used.

Accept Text Translation Changes

Optional Station ID criteria:

Select Decoder Channels for Local Access CEM Custom Message
L1-Main,Radio 1
R1-Main,Radio 2
L2-Aux 1,Radio 3
R2-Aux 1,Rear Connector
CAP1:HTTP Get Client1

Submit Decoder Channels

Message Display Control
○ Play CEM alert with custom translation once
○ Repeat CEM alert playout for the defined EAS duration (or until stopped)
○ Repeat CEM alert playout until stopped
○ Repeat CEM alert playout for a specific duration (or until stopped)
● Repeat CEM alert playout for a fixed number of times (or until stopped)

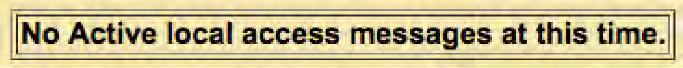
Number of repetitions: 1
1 :0 Time in min:secs between end of playout and replay.
Mins:Secs
Play full EAS alert audio with every display repetition
Audio repetition control

Local Access Forwarding Screen

Custom Text Translation for CEM (Civil Emergency Message)
This check box controls activation of the local access forwarding feature. When enabled, as shown in the above screen shot, local access forwarding is active and can be configured. **If a local access CEM alert is decoded, it will be automatically forwarded regardless of the decoder forwarding mode**.

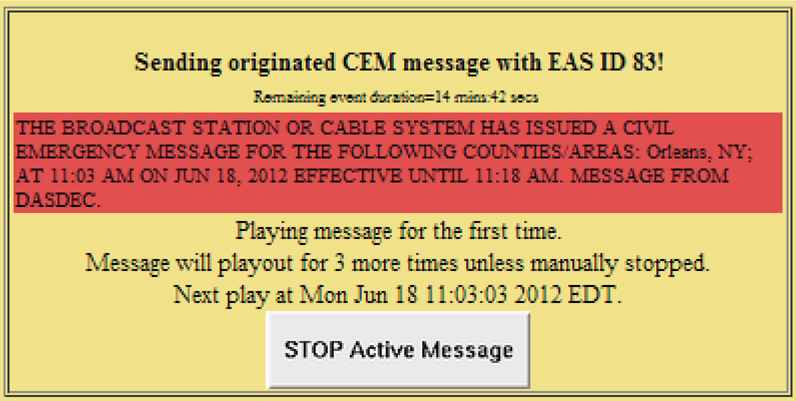
Local Access Message Play-out Status

The current status of Local Access Forwarding is displayed near the top of the page. When there are no active local access CEM messages being played, the status displays:



No Active local access messages at this time.

When a CEM alert is forwarded under control of Local Access Forwarding**,** the status window will display the: EAS devices' ID of the local access message, information about the repetition number of the play-out and when it will stop. There is a large flashing button for manually stopping the alert play-out at any time. While the message play-out is active, the **Setup > Alert Agent™ > Local Access Forwarding** screen will auto-refresh.



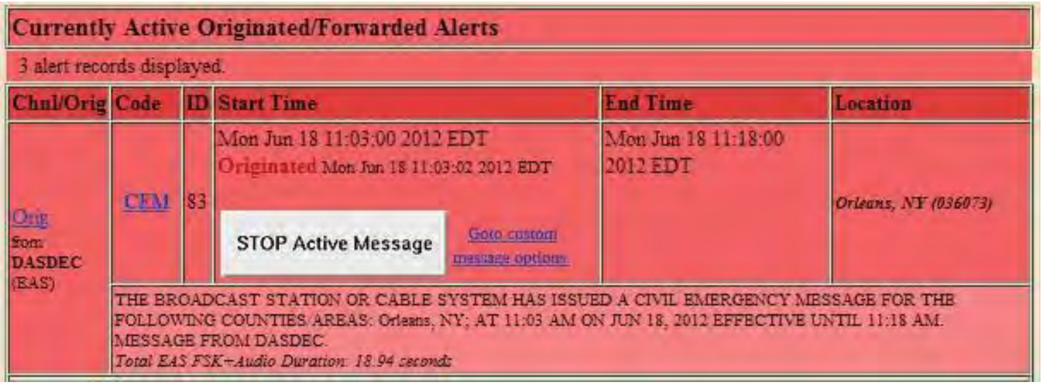
Sending originated CEM message with EAS ID 83!

Remaining event duration=14 mins:42 secs

THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A CIVIL EMERGENCY MESSAGE FOR THE FOLLOWING COUNTIES/AREAS: Orleans, NY; AT 11:03 AM ON JUN 18, 2012 EFFECTIVE UNTIL 11:18 AM. MESSAGE FROM DASDEC.

Playing message for the first time.
Message will playout for 3 more times unless manually stopped.
Next play at Mon Jun 18 11:03:03 2012 EDT.

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



Currently Active Originated/Forwarded Alerts

3 alert records displayed.

Chnl/Orig	Code	ID	Start Time	End Time	Location
Orig from DASDEC (EAS)	CEM	83	Mon Jun 18 11:03:00 2012 EDT Originated Mon Jun 18 11:03:02 2012 EDT STOP Active Message Goto custom message options	Mon Jun 18 11:18:00 2012 EDT	Orleans, NY (036073)
	THE BROADCAST STATION OR CABLE SYSTEM HAS ISSUED A CIVIL EMERGENCY MESSAGE FOR THE FOLLOWING COUNTIES/AREAS: Orleans, NY; AT 11:03 AM ON JUN 18, 2012 EFFECTIVE UNTIL 11:18 AM. MESSAGE FROM DASDEC. Total EAS FSK+Audio Duration: 18.94 seconds				

Incoming/Decoded Alerts

Custom CEM Text Translation

This text, if provided, will be displayed on the video details page and sent to CG's and to network protocols (like EAS NET, SCTE18, etc.) when the alert is forwarded

When a decoded CEM alert is forwarded, the text will be displayed on the EAS device video details page, and will be sent to any serially connected character generators and network protocols. If no custom text is entered, the standard translation of the decoded alert is used. After text is entered, click on the **Accept Text Translation Changes** button to submit the changed text.

Note
Any text entered during an active alert will not be used. Custom CEM Text Translation text must be entered and accepted prior to being used by an incoming alert.

Optional Station ID criteria

A station ID filter code can be entered in the field below the CEM text box. This will limit action of local access forwarding to those CEM alerts decoded from the Decoder Local Access Forwarding configuration sub-page. It is used to configure custom forwarding play-out for decoded CEM (Civil Emergency Message) EAS alerts specified source station.

Select Decoder Channels for Local Access CEM Custom Message

This selector interface displays all available decoders on the system. Select the set of decoders for the CEM custom local access forwarding response. CEM alerts decoded on the unselected decoder channels will not trigger local access forwarding and will be processed like any other incoming decoded alert.

Message Display Control

Select an alert play-out repetition action. Each option has one or more sub-options to refine the play-out repetition period and audio.

Number of repetitions

The Message Display Control option "**Repeat CEM alert play-out for a fixed number of times"** is for selecting the number of times the CEM alert is replayed.

Replay period

The repeat period interface for Message Display Control options that cause repetition for certain time durations, can set the replay period to the time in minutes/seconds between end of play-out and replay.

Audio control/ audio repetition control

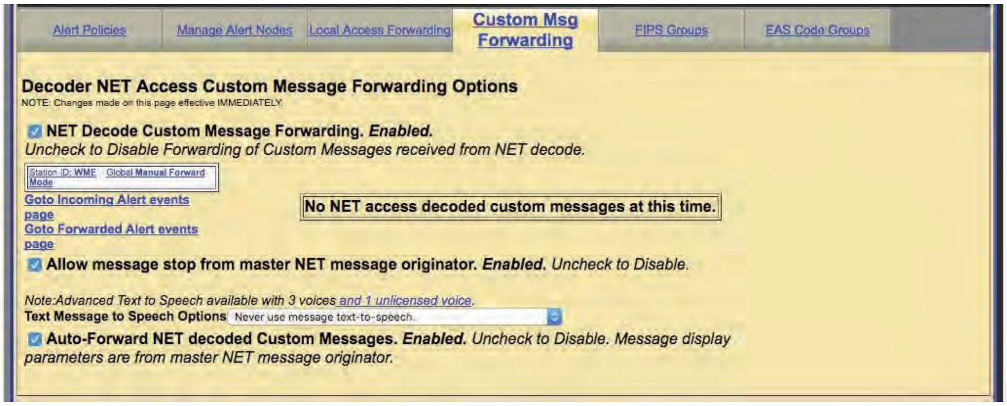
The pull-down menu allows selection of none, all, or part of the EAS audio message during the first and repeat play-outs.

Custom MSG Forwarding

The **Decoder NET Access Custom Message Forwarding Options** screen allows a user to enable EAS NET decode custom message forwarding and gives them control over how these messages are forwarded. Even in Manual Forwarding Mode, a user can auto-forward EAS NET decoded custom messages.

NET Decode Custom Message Forwarding

When enabled, it gives the operator the ability to forward decoded messages from EAS NET. If this option is disabled, custom messages that are decoded over EAS NET cannot be forwarded.



Decoder NET Access Custom Message Forwarding Options

NOTE: Changes made on this page effective IMMEDIATELY.

☑ **NET Decode Custom Message Forwarding.** ***Enabled.***
Uncheck to Disable Forwarding of Custom Messages received from NET decode.

Station ID: WME Global Manual Forward Mode

Goto Incoming Alert events page
Goto Forwarded Alert events page

No NET access decoded custom messages at this time.

☑ **Allow message stop from master NET message originator.** ***Enabled.*** *Uncheck to Disable.*

Note:Advanced Text to Speech available with 3 voices and 1 unlicensed voice.
Text Message to Speech Options Never use message text-to-speech.

☑ **Auto-Forward NET decoded Custom Messages.** ***Enabled.*** *Uncheck to Disable. Message display parameters are from master NET message originator.*

Custom Message Forwarding Screen

If the EAS device does not have any current active custom message alerts, there will be a message that says: **No NET access decoded custom messages at this time.**