Digital Alert Systems

Application Note

Interfacing Digital Alert Systems DASDEC™ with Common Alerting Protocol (CAP) Servers

Brief guide for configuring the DASDEC EAS/CAP Encoder/Decoder to receive CAP events

TABLE OF CONTENTS

Introduction

The DASDEC flexible emergency message platform supports a variety of communication protocols for receiving alerts and transferring alert information to third party platforms. This document describes how to configure the DASDEC to receive Common Alerting Protocol (CAP) based EAS alerts and non-EAS messages from CAP servers over TCP/IP communication channels. CAP messages are received in two ways; by direct query of remote CAP server sources or by a Secure Shell based peer-to-peer push from a remote CAP sender.

In addition to handling legacy EAS messaging over audio, the DASDEC is capable of processing up to 10 simultaneous CAP input sources with multiple CAP message envelope formats. The DASDEC can process CAP messages directly from; a single XML CAP file, wrapped within EDXL-DE, as a list of CAP <alert> blocks within a container XML file, or from the ATOM XML format, with a separate interface for each CAP input source.

This documentation applies to DASDEC Software Version 2.0-0_a03 and above and supersedes all prior versions.[1] To verify the current DASDEC software version check the version number at the right side of the log in screen (See Figure 1. DASDEC log in screen below) or the "About" page under **Server >Help->About DASDEC-1EN**. (Please check our website at www.digitalalertsystems.com for information on downloading and installing the current software version)

[1] Due to the rapidly evolving development of CAP services some screens may differ from those shown.

Revision: 3.2 Publications: APNDAS-121

Digital Alert Systems
A division of **Monroe Electronics**
585-765-1155 | fax 585-765-9330
100 Housel Ave. | Lyndonville | NY | 14098
www.digitalalertsystems.com

CAP Input Configuration on DASDEC (Software Version 2.0+)

This application note assumes basic familiarity with the DASDEC web interface and describes setting up a sample CAP input. By default the DASDEC is licensed for ***CAP Standard*** to acquire CAP messages and decode into EAS alerts. Customers who purchased or received ***CAP Plus*** *or* ***CAP Premium*** will have an additional license keys activated.[2]

CAP Decode Setup

1. Log into your DASDEC as an administrator using your User Name and Password. (Defaults are User Name "**Admin"** with the password "**dasdec"**)

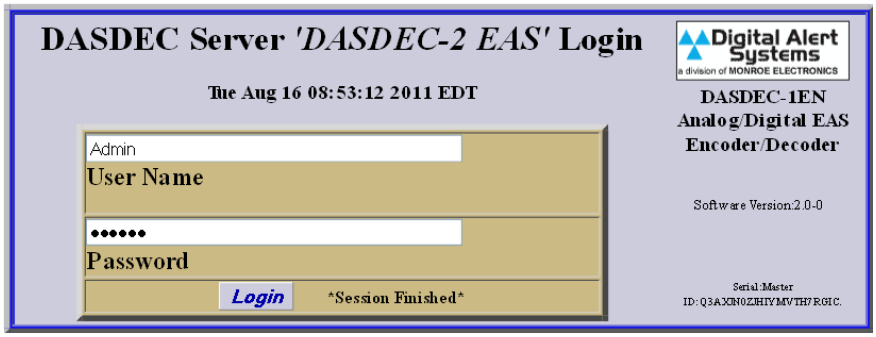


Figure 1. DASDEC log in screen

2. Go to **Setup> Net Alerts> CAP**, then place a check in the CAP decode box.

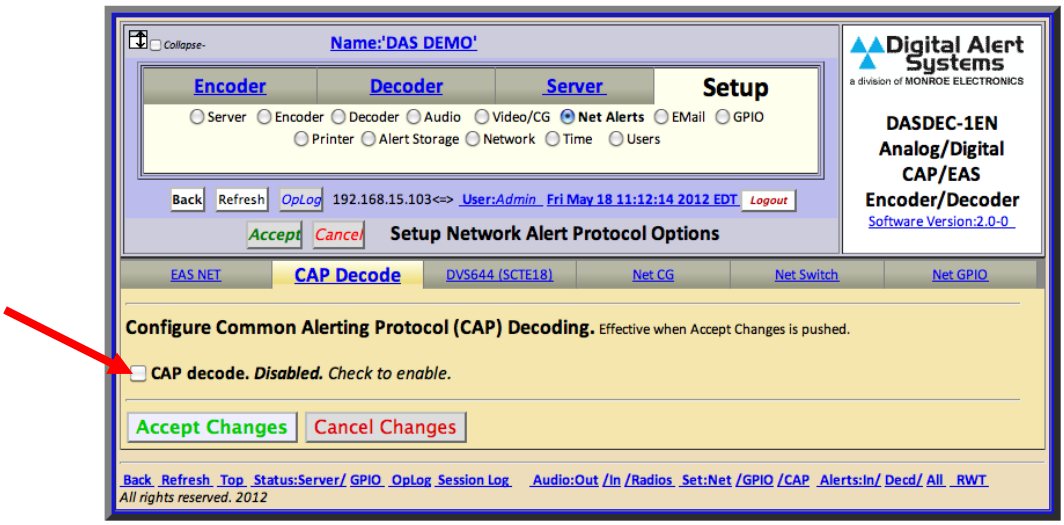


Figure 2 Enabling the CAP Decoder. Click the box

[2] Each license key is managed from the Setup->Server->Main/License setup page in the web interface.

3. The page will expand showing a number of CAP options

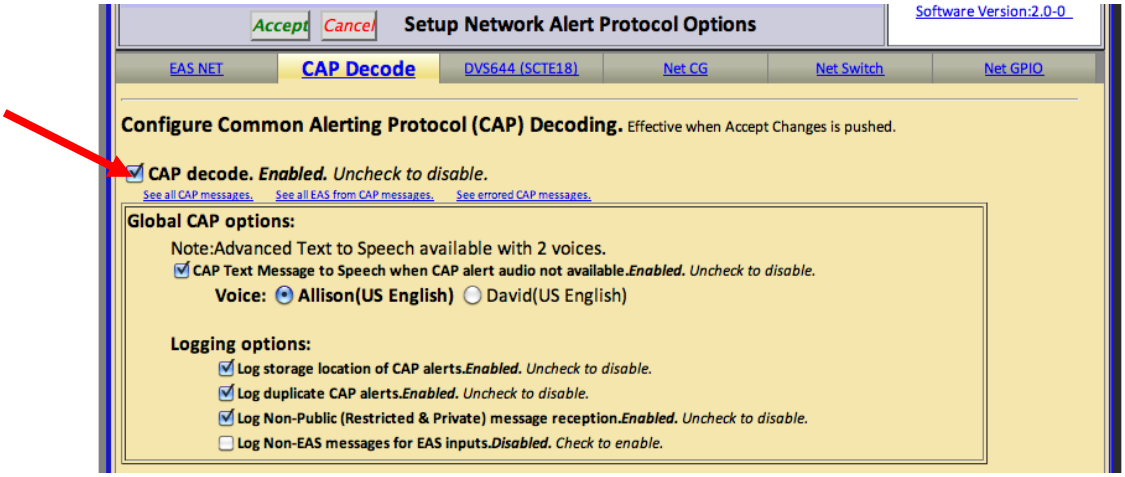


Figure 3 CAP Decode Enabled showing available TTS and logging options. (See text)

Check the box "CAP Text Message to Speech…" to enable automatic Text-To-Speech (TTS) conversion if the CAP message does not contain or redirect to an associated audio file.

If the DASDEC is licensed for the additional voices (CAP Premium) the additional voices are shown with a radio button to select the different options. If no option is shown or selected the DASDEC will use the standard TTS engine.

The Logging options are a series of check boxes toggling various logging functions:

Log storage location of CAP alerts. Check to enable recording the internal file system path for each CAP alert to the Operation Log. Remove check to disable.

Log duplicate CAP alerts. Check to enable a message when duplicate CAP alerts are received and discarded in the Operation Log. Remove check to disable.

Log Non-Public (Restricted & Private) message reception. Check to enable recording reception of non-public CAP messages to the Operation Log. Remove check to disable.

Log Non-EAS messages for EAS inputs. Check to enable a message when Non-EAS messages are received from sources that provide CAP EAS messages to the Operation Log. Remove check to disable.

4. Below the **Global CAP Options** in the **Remote CAP server setup** section a **CAP PUSH INPUT** client is already enabled as a default. It is recommended this be disabled by unchecking the box unless this type of interface is necessary. Disable this client by deselecting (unchecking) the box **ENABLE Client Interface** directly below the **CAP PUSH INPUT** field as shown in Figure 4

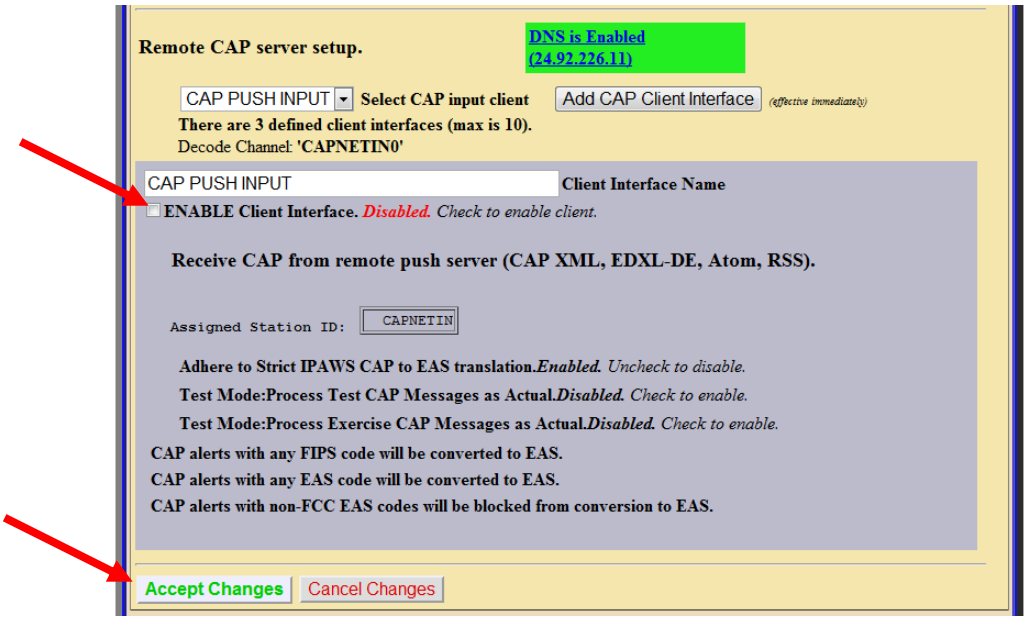


Figure 4 Disabling the default CAP PUSH INPUT client

5. Click **Accept Changes** to disable this default interface.
6. To continue add a CAP Interface by selecting the button **Add CAP Client Interface**

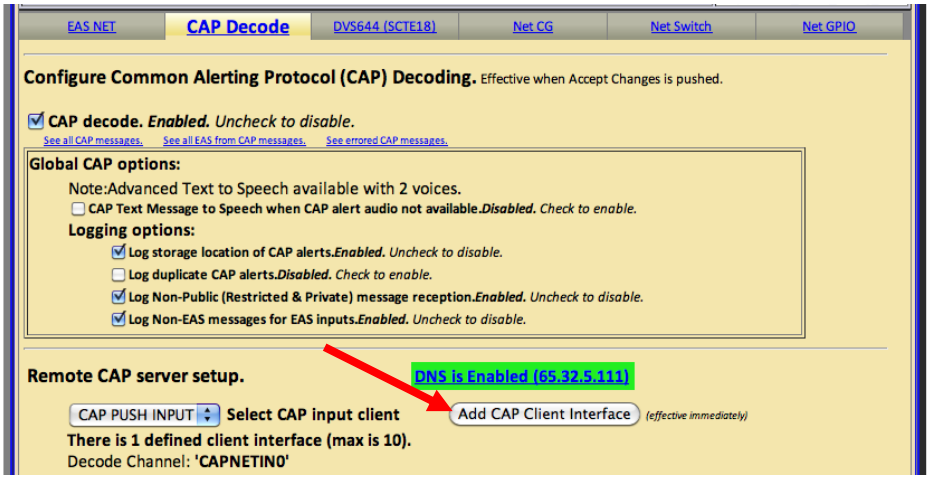


Figure 5 Adding a new CAP Client Interface

Interfacing with FEMA's Integrated Public Alert Warning System (IPAWS)

The DASDEC is designed and has received proper compliance certificates to allow a direct interface with the Federal Emergency Management Agency's IPAWS servers. Setting this interface is very straight-forward.

Follow steps 1 through 6 above.

7. The page expands to enter more information. It is a good idea to add a descriptive name identifying the CAP source In the **Client Interface Name** box as shown in the *example* below identifying the IPAWS CAP server as **"IPAWSOPEN".** Each client interface created is shown in the pull down menu to the left of **Select CAP input client** once it is saved.
8. Make sure the **ENABLE Client Interface** is selected turning on communications with this CAP Server. You can turn off the communications link to a CAP server by deselecting this box without losing the other parameters.
9. Using the drop down menu to the left of **CAP Poll Protocol** select ***IPAWS Open 2.0 Get***

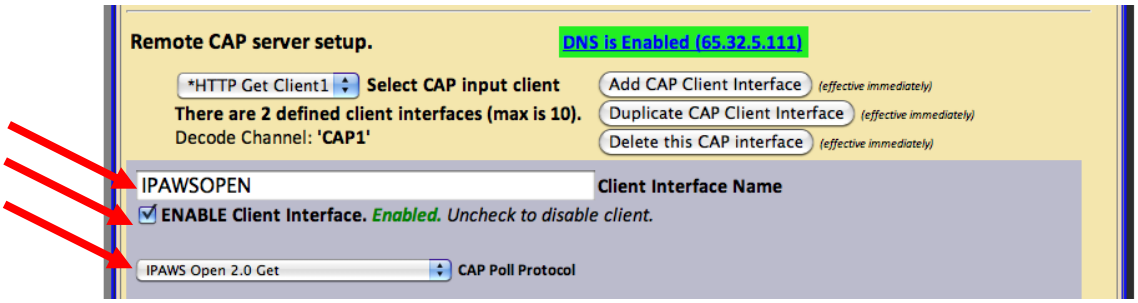


Figure 6 Selecting and naming the client interface for FEMA IPAWS

10. The page will change to accept configuration information based on the IPAWS Open CAP Poll Protocol selection above.
11. Enter **apps.fema.gov** in the **CAP server host address**. This is FEMA's IPAWS server's web address as such you must have DNS must be enabled to properly resolve the name. (A green box **"DNS is Enabled (xxx.xxx.xxx.xxx)"** is displayed at the top of the section verifying DNS is enabled. Refer to the manual for more information on setting DNS)

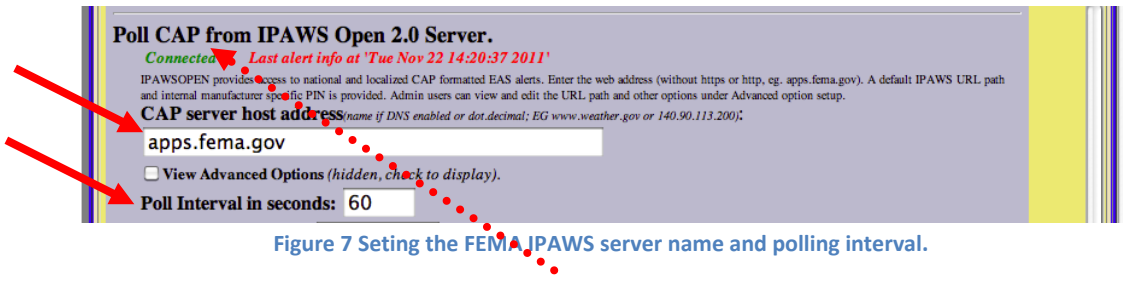


Figure 7 Seting the FEMA IPAWS server name and polling interval.

12. When properly connected a green *Connected* message will be displayed directly under the Poll CAP from IPAWS Open 2.0 Server and the last time any alert information was received from the server. *(NOTE: You may need to refresh your browser to see the connected status)*
13. The number of seconds the DASDEC waits to check the CAP server for updates is entered in the **Poll Interval in seconds** box. (Default is 60 seconds).

14. Set the Assigned Station ID, which defines the default EAS station ID assigned to EAS alerts translated from this source. This name appears in the decoded log only if an EAS station ID cannot be derived from the CAP message. This field can be up to 8 printable characters and cannot include the dash '-' character.

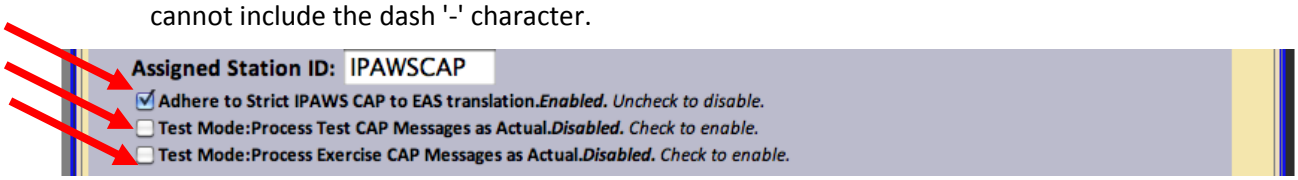


Figure 8 Assigning strict IPAWS compliance and test message handling.

15. The toggle **Adhere to Strict IPAWS CAP to EAS translation** is controls whether or not the incoming CAP messages must adhere to the IPAWS compliance specification. This should checked (Enabled) when processing CAP from IPAWS systems.

16. The toggles **Test Mode: Process Test CAP Messages as Actual** and **Test Mode: Process Exercise CAP Messages as Actual** allow some flexibility in testing CAP messages. These simply allow CAP messages with a status of Test and/or Exercise to be treated as actual events. Default is Disabled (unchecked).

IMPORTANT NOTE: The final sections provide more filter control of incoming CAP messages and are selected (checked) *Enabled* by default. Leaving these boxes checked means *ALL* events for *ALL* regions will be decoded and possibly acted on by the DASDEC. Users are strongly encouraged to uncheck and enter specific FIPS codes to process.

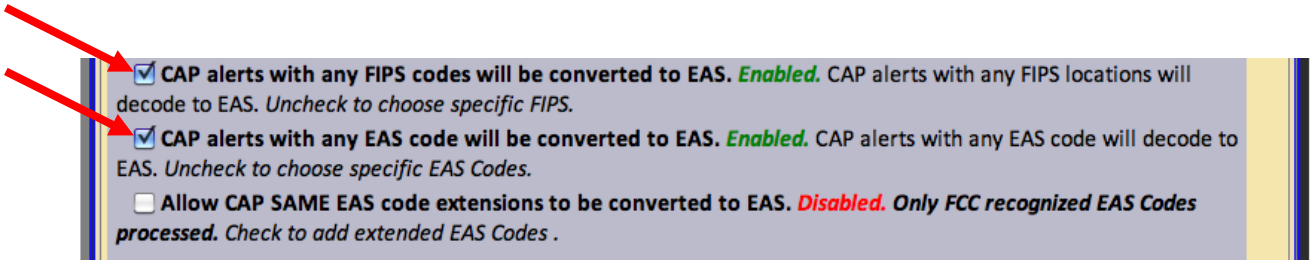


Figure 9 Default settings for FIPS and EAS results in ALL regions and All codes being enabled. (See important Note above)

17. The DASDEC supports the selection of specific FIPS location codes and EAS event codes in order to restrict the processing to specific EAS alert types and locations. Both FIPS and EAS codes have a toggle controlled interface to set specific filters for limiting CAP message processing which is selected as default. Deselect the **CAP alerts with any FIPS codes will be converted to EAS s**election in Figure 9 above to open the user interface for entering specific FIPS codes.

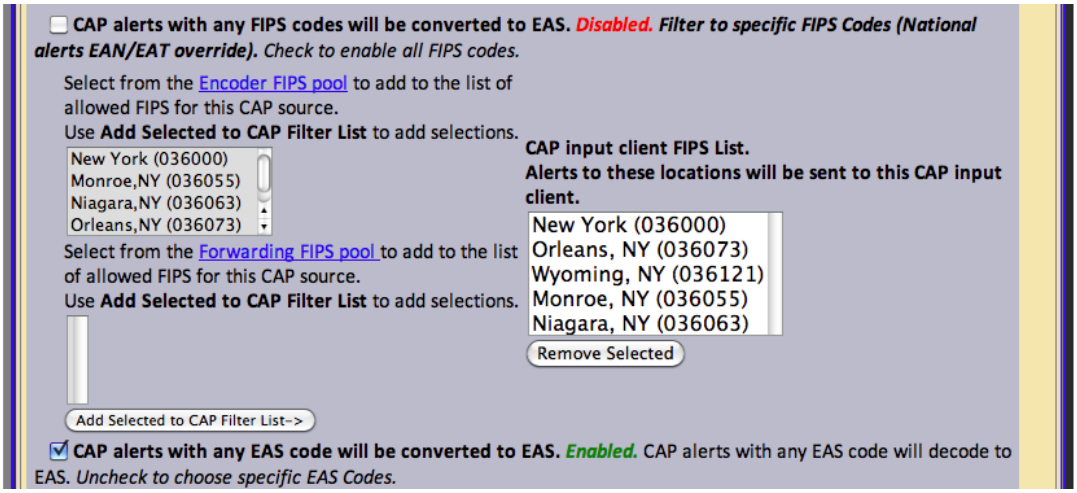


Figure 10 Adding specific FIPS codes for CAP Decoding narrows activation response areas

18. To speed selection the box on the left matches the list of Encoder FIPS pool – those FIPS codes already configured for standard EAS activation. To quickly add these to the **CAP Input client FIPS List** simply click the first item in the list, then holding the SHIFT key scroll to the bottom of the list and click the last item. This will select the entire list. Click **Add Selected to CAP Filter List** and all the selected FIPS codes will be added to the list. You can add or remove items from the list by selecting the specific item and Add or Remove as desired.

19. There maybe occasion to alter the specific EAS events codes to active. Deselect the **CAP alerts with any FIPS codes will be converted to EAS s**election in Figure 10 above to open the user interface for entering specific EAS codes.

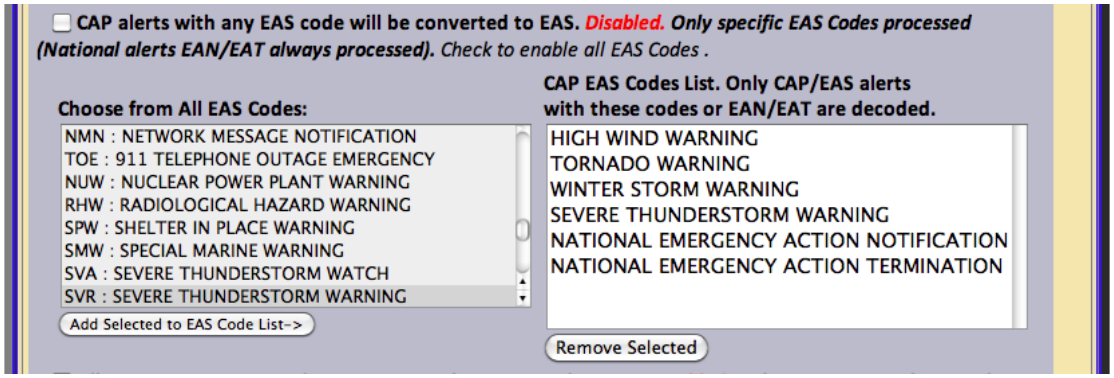


Figure 11 Adding specific EAS codes to narrow activation response type.

20. The box on the left of Figure 11 shows all EAS event codes. Select any item on the left list then click **Add Selected to EAS Code List** and the item will be added to the **CAP EAS Codes List**. The *EAN – National Emergency Action Notification* and *EAT – National Emergency Action Termination*[3] are automatically added as part of the list. You can add or remove items from the list by selecting the specific item and Add or Remove as desired..

[3] While the EAT was dropped as an event code in the FCC's Fifth Report & Order governing EAS. We include it here for backward compatibility.

NOTE: Any CAP message with the special parameter *EAS-Must-Carry* set to *TRUE*, will ignore EAS code filtering. FIPS filters however will still be applied to CAP messages with EAS-Must-Carry. National Alerts – EAN and EAT – ignore both filters.

21. CAP messages can carry non-standard FCC (3-letter) EAS Event codes. Toggling the **Allow CAP SAME EAS code extensions to be converted to EAS** provides a method to enter these other event code definitions as shown in the example in Figure 12. This interface must be used with care, and only for areas that allow non-FCC EAS code extensions, otherwise leave this section Disabled (unchecked).

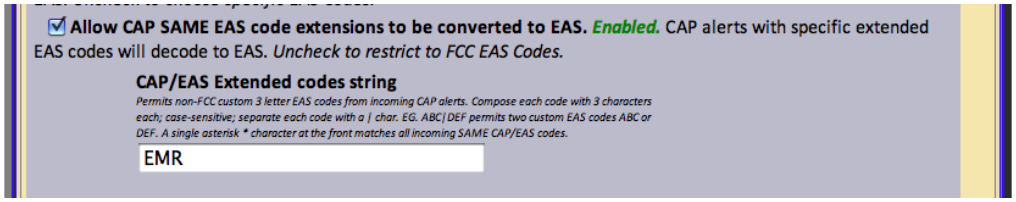


Figure 12 Adding optional extended EAS event codes. (See text for more details)

22. Each code is 3 characters and case-sensitive. You can place multiple codes on the line by separating them with a "pipe" character (no space). For example using the fictional codes "ABC" and "DEF" and placing them as ABC|DEF permits two custom EAS codes. More information is provided on the screen.

23. Press **Accept Changes** to store all the settings

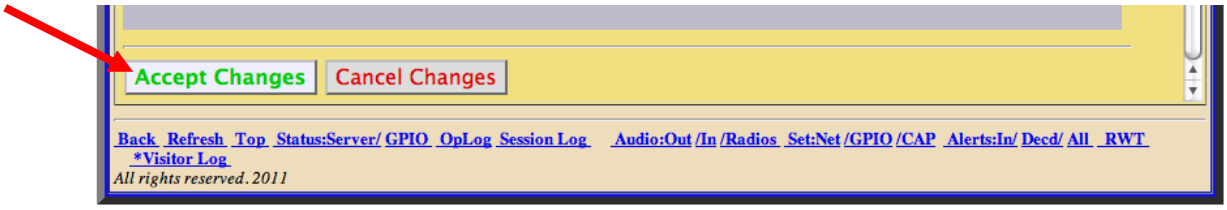


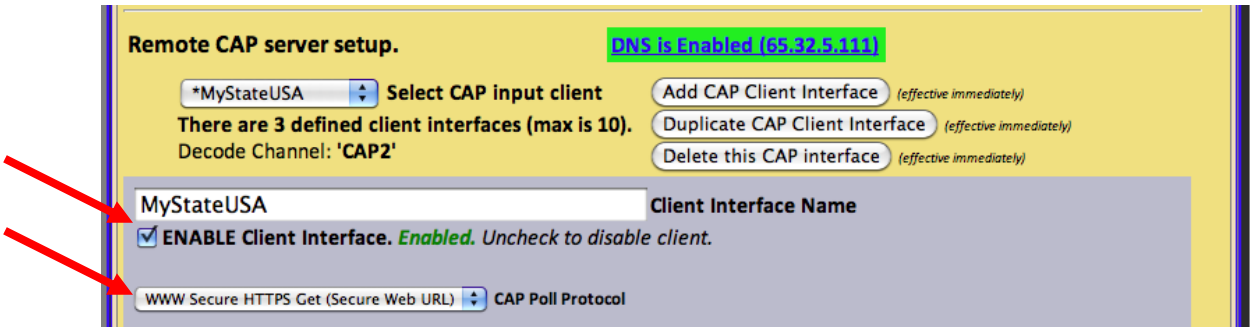
Figure 13 Accept Changes when done to store all settings.

Interfacing with MyStateUSA

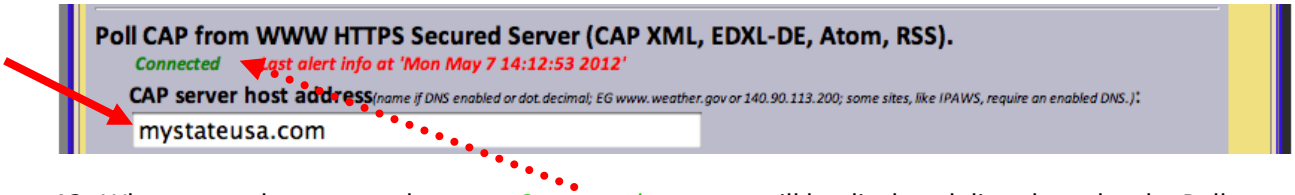
The DASDEC is designed to support a number of CAP Servers – even those with dynamic data exchange for updates. The following is an example using a MyStateUSA configuration.

Follow steps 1 through 6 above.

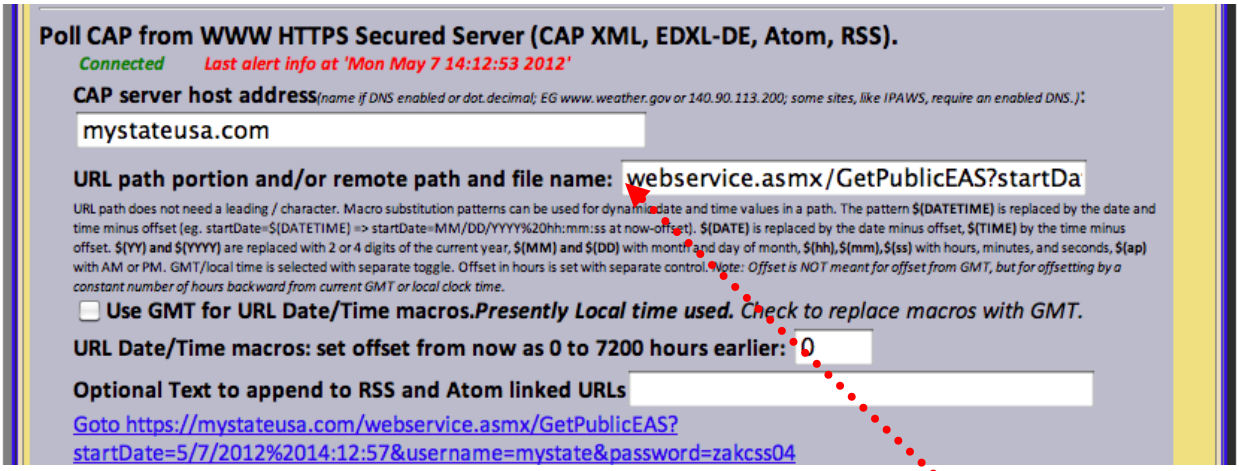
7. The page expands to enter more information. It is a good idea to add a descriptive name identifying the CAP source In the **Client Interface Name** box as shown in the *example* below identifying the CAP server as **"MyStateUSA".** Each client interface created is shown in the pull down menu to the left of **Select CAP input client** once it is saved.
8. Select **ENABLE Client Interface** to turn on communications with this CAP Server. You can turn off the communications link to a CAP server by deselecting this box without losing the other parameters.
9. Using the drop down menu to the left of **CAP Poll Protocol** select ***WWW Secure HTTPS Get (Secure Web URL)***



10. The page will change to accept configuration information based on the WWW Secure HTTPS Get protocol selection above.
11. Enter **mystateusa.com** in the **CAP server host address**. This is MyStateUSA server's web address therefore you must have DNS must be enabled to properly resolve the name. (A green box **"DNS is Enabled (xxx.xxx.xxx.xxx)"** is displayed at the top of the section verifying DNS is enabled. Refer to the manual for more information on setting DNS)



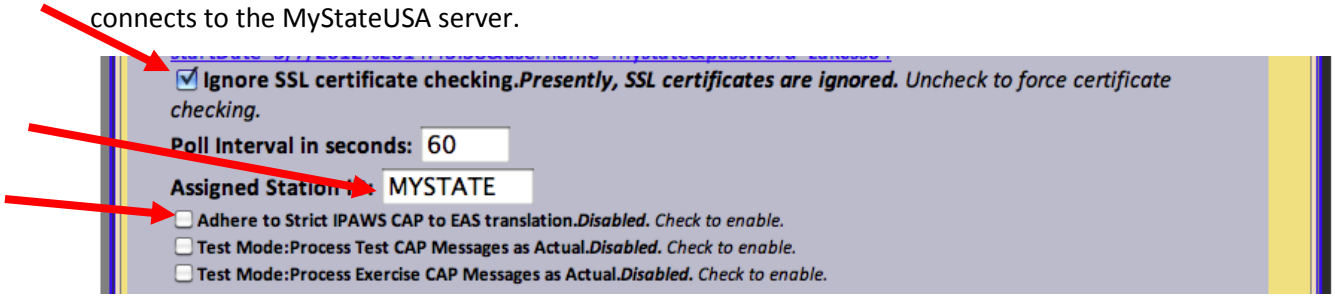
12. When properly connected a green *Connected* message will be displayed directly under the Poll CAP from IPAWS Open 2.0 Server and the last time any alert information was received from the server. (NOTE: You may need to refresh your browser to see the connected status)



13. The MyStateUSA's server works by comparing the time of the last connection and the current connection to see determine if any new alerts need to be pushed to the DASDEC. In order for this to work correctly in the box **URL path portion and/or remote path and file name:** box enter the following macro:

webservice.asmx/GetPublicEAS?startDate=$(DATETIME)&username=mystate&password=zakcss04

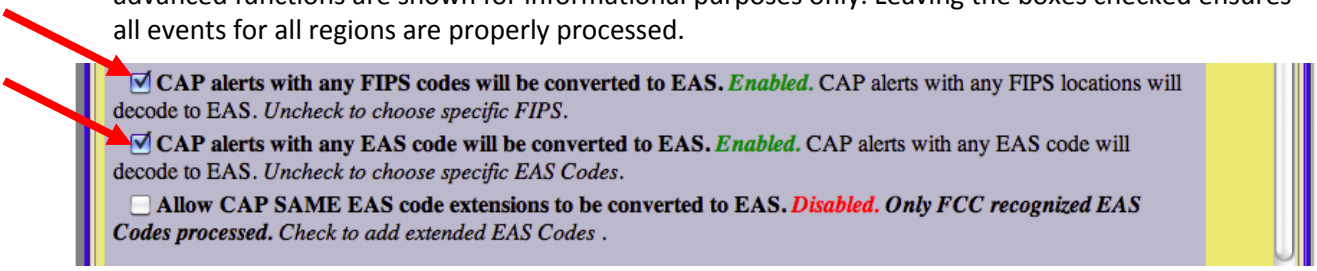
This macro dynamically updates the current connection time in the $(DATETIME) field whenever it connects to the MyStateUSA server.



14. Select the checkbox **Ignore SSL certificate checking.** When enabled the line will read: **Ignore SSL certificate checking *Presently, SSL certificates are ignored.*** *Uncheck to force certificate checking*
15. The number of seconds the DASDEC waits to check the CAP server for updates is entered in the **Poll Interval in seconds** box. (Default is 60 seconds).
16. Set the Assigned Station ID, which defines the default EAS station ID assigned to EAS alerts translated from this source. This name appears in the decoded log only if an EAS station ID cannot be derived from the CAP message. This field can be up to 8 printable characters and cannot include the dash '-' character. It's preferable to use something easily identifiable such as **MYSTATE** as shown in the example.

17. As MyStateUSA typically has alerts that do not conform to the IPAWS CAP profile Do not check the **Adhere to Strict IPAWS CAP to EAS translation**. This must remain disabled (unchecked)
18. The toggles **Test Mode: Process Test CAP Messages as Actual** and **Test Mode: Process Exercise CAP Messages as Actual** allow some flexibility in testing CAP messages. These simply allow CAP messages with a status of Test and/or Exercise to be treated as actual events. Default is Disabled (unchecked).

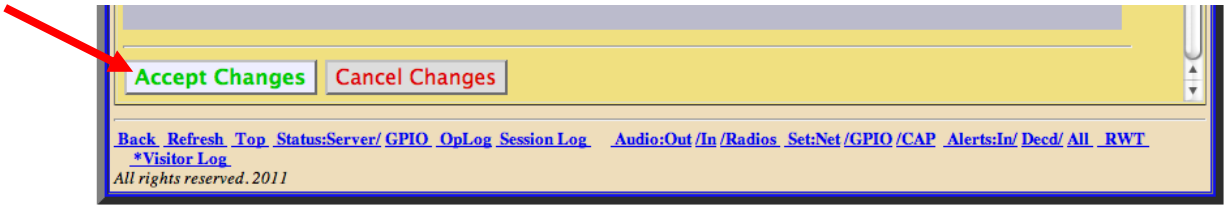
The final sections provide more esoteric CAP control and are defaulted as Enabled (checked). These advanced functions are shown for informational purposes only. Leaving the boxes checked ensures all events for all regions are properly processed.



19. *EAS event code and FIPS location code filters:* By default, CAP messages with any FIPS locations and any EAS code are processed and passed. The DASDEC supports the selection of specific EAS event code and FIPS location codes in order to restrict the processing to specific EAS alert types and locations. The example above shows the default values all FIPS codes and all EAS codes selected (checked).

    Note: Any CAP message with the special parameter EAS-Must-Carry set to TRUE, will ignore EAS code filtering. FIPS filters however will still be applied to CAP messages with EAS-Must-Carry. National Alerts EAN and EAT ignore both filters.

20. SEE **STEPS 17 – 22** beginning on **Page 6** for more information on restricting the CAP messages with FIPS and EAS event codes.
21. CAP messages can carry non-standard FCC (3-letter) EAS Event codes. By toggling the **Allow CAP SAME EAS code extensions to be converted to EAS** provides a method to enter these other event code definitions. This interface must be used with care, and only for areas that allow non-FCC EAS code extensions. More information is provided on the screen. See the figure above.
22. Press **Accept Changes** to store all the settings



Checking Decoded CAP/EAS alerts

When a CAP message is translated into an active EAS alert, the event will be displayed as an active decoded alert. Just like any other EAS alert, go to the **Decoder-> Incoming / Decoded Alerts** page to view all decoded and active alerts . Each active alert displays pertinent information about the alert, such as the source of the alert, the associated alert text, the location and time of the alert. CAP derived alerts will also display an active link to the original CAP file.

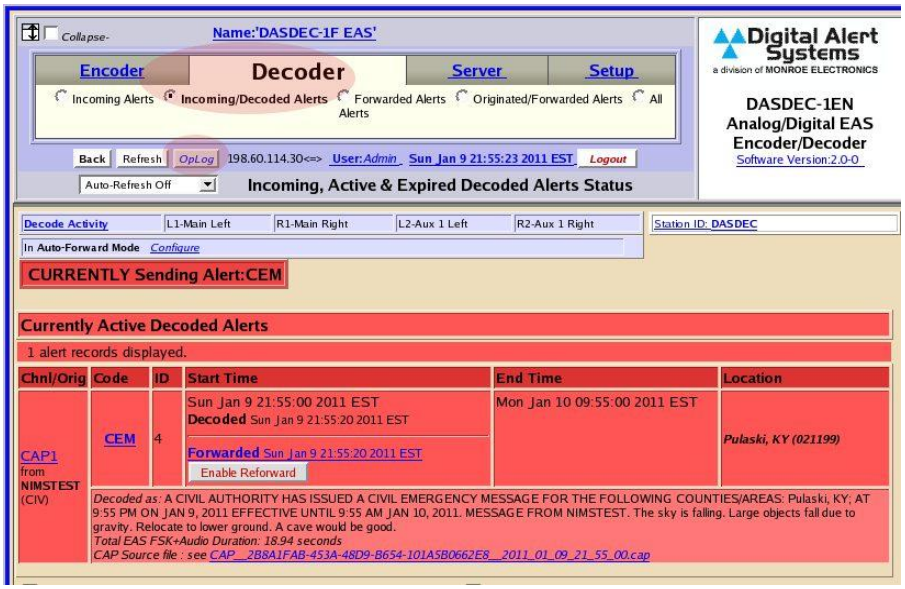


Figure 14. Example of CAP decoded and active (note red color) message