

Updating Certificate Authority Files For One-Net™/DASDEC™ EAS/CAP Devices

The One-Net and DASDEC EAS/CAP devices can use a special digital certificate provided by FEMA to validate the authenticity of IPAWS sourced CAP alerts. These certificates are designed to expire at a specific date and time, requiring the issuing authority to issue new certificates from time to time.

The current FEMA certificate will be expiring on June 24, 2018. FEMA recently issued a newer certificate which means IPAWS users should update their equipment before the June 24, 2018 expiration date. Not updating the certificate may result in the error message:

“Event Log:Digital Signature VERIFICATION ERROR : Signer UNTRUSTED! Check for correct CAP decoder CA file.;”

To update and change the Certificate Authority (CA) file within the EAS device (One-Net or DASDEC):

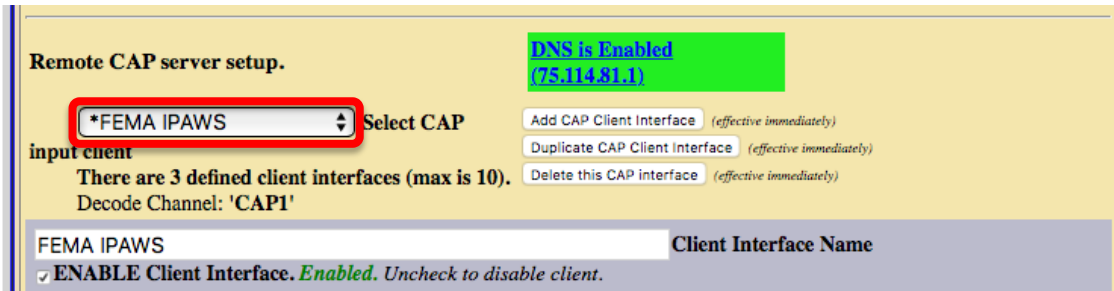
IMPORTANT NOTE for Firefox Users: The link in Step 1. below may not work correctly. Return to the page www.digitalalertsystems.com/resources_fsb.html to find the alternate CA file download link.

1. Download the current certificate authority file IPAWS_Valid-until-09-24-2018.crt from here:

www.digitalalertsystems.com/download/IPAWS_Valid-until-09-24-2018.crt

NOTE: This certificate will also be expiring in September of this year, however we must wait until FEMA issues the next certificate to replace this one.

2. Navigate to the **Setup > Net Alerts > CAP Decode** screen
3. Select the CAP configuration for IPAWS from the **Select CAP input client** pull-down menu.
(Note: The name may differ from the one shown below.)



Remote CAP server setup.

DNS is Enabled (75.114.81.1)

*FEMA IPAWS Select CAP input client

There are 3 defined client interfaces (max is 10).
Decode Channel: 'CAPI'

Add CAP Client Interface (effective immediately)
Duplicate CAP Client Interface (effective immediately)
Delete this CAP interface (effective immediately)

| Client Interface Name |
|---|
| FEMA IPAWS |
| <input checked="" type="checkbox"/> ENABLE Client Interface. <i>Enabled. Uncheck to disable client.</i> |

(continues on next page)

4. Scroll down and enable the **View Advanced Options** check box. The advanced options will appear.

Poll CAP from IPAWS Open 2.0 Server.
✓ Connected (up 1:01:56) Last alert info at 'Thu Jun 7 12:18:11 2018'
IPAWSOPEN provides access to national and localized CAP formatted EAS alerts. Enter the web host address (without https or http, eg. apps.fema.gov and you must have DNS enabled!). A default IPAWS URL path and internal manufacturer specific PIN is provided. Admin users can view and edit the URL path and other options under Advanced option setup.

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

View Advanced Options (unchecked to remove view).

Pin Type Preassigned IPAWS Pin User configurable Pin No Pin
 Use Secure connection. Enabled. Uncheck to use non-secured connection.
 Ignore SSL certificate checking. Presently SSL certificates must verify. Check to ignore certificate.

Optional Text to append to URL
 Require XML digital signatures. Reject alerts missing signatures or that fail signature verification. Enabled. Uncheck to disable.
XML Digital Signature Certificate Authority (CA) Name (upload below.) FCPCA-USTreasury-DHS-IGC-CA.crt

CA Information

5. Scroll to the bottom of the page to find the **Upload Certificate Authority file to DASDEC Server.** dialog box as shown below:

Upload Certificate Authority file to DASDEC Server.
Choose File no file selected
Upload Certificate Authority file

6. Click **Choose File** and select the recently downloaded file: **IPAWS_Valid-until-09-24-2018.crt**
7. Click **Open**. The screen should now appear as shown below

Upload Certificate Authority file to DASDEC Server.
Choose File IPAWS_Valid-until-09-24-2018.crt
Upload Certificate Authority file

8. Click **Upload Certificate Authority file** button. When the file is successfully installed the screen will show

Upload Certificate Authority file to DASDEC Server.
Choose File no file selected
CA File Upload Succeeded.
Upload Certificate Authority file

9. Scroll back up the page and in the **View Advanced Options** area locate the **XML Digital Signature Certificate Authority (CA) Name** then, using the pull-down menu, choose the **"IPAWS_Valid-until-09-24-2018.crt"** selection as shown below.

View Advanced Options (unchecked to remove view).

Pin Type Preassigned IPAWS Pin User configurable Pin No Pin
 Use Secure connection. Enabled. Uncheck to use non-secured connection.
 Ignore SSL certificate checking. Presently SSL certificates must verify. Check to ignore certificate.

Optional Text to append to URL
 Require XML digital signatures. Reject alerts missing signatures or that fail signature verification. Enabled. Uncheck to disable.
XML Digital Signature Certificate Authority (CA) Name (upload below.) IPAWS_Valid-until-09-24-2018.crt

CA Information

10. Click the **Accept Changes** button at the bottom of the screen.

Accept Changes Cancel Changes

END