

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

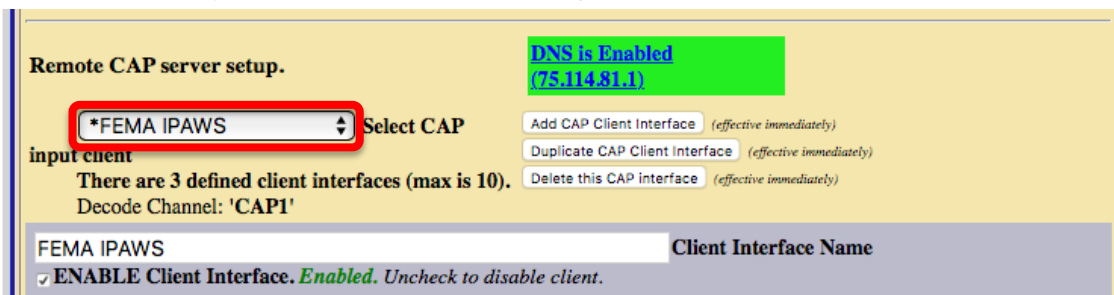
The One-Net and DASDEC EAS/CAP devices can use a special digital certificate provided by FEMA to validate the authenticity of IPAWS sourced CAP alerts. These certificates are designed to expire at a specific date and time, requiring the issuing authority to issue new certificates from time to time.

The current FEMA certificate will be expiring on August 21, 2021. FEMA recently issued a newer certificate which means IPAWS users should update their equipment before the August 21, 2021 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.,” or not processing valid IPAWS alerts.

### 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 has been tested and works correctly with Firefox V89.0.2.*

1. Download the current certificate authority file IPAWS\_Valid-until-04-14-2024.crt from here: [http://www.digitalalertsystems.com/download/IPAWS\\_Valid-until-04-14-2024.crt](http://www.digitalalertsystems.com/download/IPAWS_Valid-until-04-14-2024.crt)  
*NOTE: This certificate expires on April 14, 2024. Prior to that date, FEMA will issue a replacement.*
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.)*



(continues on next page)

- 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 0:01:16) Last alert info at 'Thu Jul 8 13:31:52 2021'

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 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** (uncheck 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 \_\_\_\_\_  
 Accept unsigned alerts. Enabled. Uncheck to reject unsigned alerts.  
 Accept unverifiable signed alerts. Enabled. Uncheck to reject unverifiable signed alerts.

XML Digital Signature Certificate Authority (CA) Name (upload below.) IPAWS\_Valid-until-08-21-2021.crt

CA Information Delete CA file

- Scroll to the bottom of the page to find the appropriate installation dialog box as shown below:

Version 3.x	Version 4.x
<p><b>Upload Certificate Authority file to DASDEC Server.</b></p> <p>Choose File no file selected</p> <p>Upload Certificate Authority file</p>	<p><b>Certificate Authority Bundle Installation</b></p> <p>Choose File no file selected</p> <p>Upload Certificate Authority file</p>

- Click **Choose File** and select the recently downloaded file: **IPAWS\_Valid-until-04-14-2024.crt**
- Click **Open**. The screen should now appear as shown below

Version 3.x	Version 4.x
<p><b>Upload Certificate Authority file to One-Net Server.</b></p> <p>Choose File IPAWS_Valid-un...04-14-2024.crt</p> <p>Upload Certificate Authority file</p>	<p><b>Certificate Authority Bundle Installation</b></p> <p>Choose File IPAWS_Valid-un...04-14-2024.crt</p> <p>Upload Certificate Authority file</p>

- Click **Upload Certificate Authority file** button. When the file is successfully installed the screen will display...

Version 3.x	Version 4.x
<p><b>Upload Certificate Authority file to DASDEC Server.</b></p> <p>Choose File no file selected</p> <p><b>CA File Upload Succeeded.</b></p> <p>Upload Certificate Authority file</p>	<p><b>Certificate Authority Bundle Installation</b></p> <p>Choose File no file selected</p> <p><b>CA File Upload Succeeded.</b></p> <p>Upload Certificate Authority file</p>

- 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-04-14-2024.crt"** selection as shown below.

**View Advanced Options** (uncheck 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 \_\_\_\_\_  
 Accept unsigned alerts. Enabled. Uncheck to reject unsigned alerts.  
 Accept unverifiable signed alerts. Enabled. Uncheck to reject unverifiable signed alerts.

XML Digital Signature Certificate Authority (CA) Name (upload below.) IPAWS\_Valid-until-04-14-2024.crt

CA Information Delete CA file

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

**Accept Changes** Cancel Changes

END