

IPAWS Interoperability Configuration

 supportcenter.nc4.com/hc/en-us/articles/217669798-IPAWS-Interoperability-Configuration

The Integrated Public Alert and Warning System - Open Platform for Emergency Networks (IPAWS- OPEN) provides interoperability interfaces for sharing of alerts. This interface provides data structures and rules of operations designed to enable information sharing between diverse systems. In general, this interface conforms to open messaging standards as defined through the Emergency Management Technical Committee sponsored by the OASIS standards organization and through the National Information Exchange Model (NIEM).

E Team can be configured to communicate with IPAWS 3 and supports the following dissemination channels:

- Emergency Alert System (EAS)
- Non Weather Emergency Messages (NWEM)
- Commercial Mobile Alert System (CMAS)

IPAWS configuration is a three-part process:

- **Server Configuration** – requires updating two files with your certificate information and setting the path to your organization's certificate.
- **Configuration Documents** – requires that you log into E Team and set up an IPAWS Data Sharing Configuration document and update two fields in the General Configuration document.
- **Validation** – requires that a user select the IPAWS-OPEN Alerts List under Alerts while logged into E Team to retrieve alerts.

Full instructions and files are found on your E Team server at ETeamWebApp\CustomInstall\IPAWS

Server Configuration

1. Explore to the folder ETeamWebApp\CustomInstall\IPAWS
2. Update the following two files with your certificate info:
 - client_deploy.wsdd
 - crypto.properties
3. crypto.properties – Update the values with the alias and keystore information provided with your certificates:
 - org.apache.ws.security.crypto.merlin.file=enter the file path to where the certificate is kept on your E Team server. For example c:\eTeamInc\eteamWebApp\eteam\userdata\IPAWS_999.jks (be sure to use \ or / in the path)
 - org.apache.ws.security.crypto.merlin.keystore.password=enter your keystore password
 - org.apache.ws.security.crypto.merlin.keystore.alias=enter your keystore alias
 - org.apache.ws.security.crypto.merlin.alias.password=enter your keystore alias password
4. client_deploy.wsdd – Update the following parameter:
 - <parameter name="user" value="enter your keystore alias"/>

Data entered here MUST match the keystore alias in crypto/properties in step 3 above.
5. Once you have saved the above files, open a command prompt and navigate to the directory: eTeamInc\eteamWebApp\eteam\userdata\IPAWS.
6. Run IPAWS.bat You will be prompted if you want to update this info in OPS TRN or BOTH. If you are running different certificates on the Operations and Training databases, you need to run this separately for both, updating the two files above individually with the info for each database.

Configuration Documents

Server configuration MUST be completed before you can communicate with IPAWS. In addition, a Data Sharing Configuration document must be created and the General Configuration document updated.

Updating these configuration documents will require that the user be a member of the have either *E Team System Admin* group or have the privileges *config (EDITOR)* and *datasharing_config (EDITOR)*.

To complete the E Team configuration documents:

1. Log into E Team and go to Administration > Data Sharing
2. Select **Create** to open a new document.
3. Enter the following data under the **General** tab:
 - **Remote System Type:** Always J2EE
 - **Remote System Name:** Always IPAWS
 - **Remote User ID:** Always client_deploy.wsdd
 - **Remote Password:** Not used, however this is a required field in order to submit the configuration document, you may enter any value you wish.

- **Local System Name:** This is the username header of the message, generally used to identify the sender. You may enter any value you wish to identify this system as the message sender. If you are not sure what to enter, it is recommended that you enter your CogName.
- **Local User ID:** Enter your CogId. Ex: 999
- **Local Password:** Not used, however this is a required field in order to submit the configuration document, you may enter any value you wish.
- **Retry Count:** Not used. Retain the default value which is 3
- **Datasharing of Access Control:** Not Used. Retain the default value which is Disable.

4. Enter the following data under the **Sender**

- **Status:** Active
- **Complete URL:** Ex: https://servername/IPAWS_CAPService/IPAWS
- URL for test and/or production will be provided by IPAWS.
- Max Attachment Size: Not used at this time

5. No entries are needed on the **Receiving** tab.

6. When done, **Submit** the Data Sharing Configuration document.

7. Navigate to the General Configuration document, **Administration > Configuration**.

8. Enter the following data under the **Additional Information** tab.

- **Default IPAWS Sender Name:** This is the name of the Sender on the CAP reports for NWEM. The NWEM HazCollect server expects Name, City, State. If this is left blank, the system will enter LastName, FirstName from the author's Personal Profile document.
- **IPAWS Identifier Prefix:** *This is appended to the beginning of the Identifier on all CAP messages. This supports the ability to more easily identify the reports that have been sent by this system when viewing/retrieving alerts using the IPAWS - OPEN Alerts List. If this field is left blank, the system will display your identifier with an **NR**, then the alert number generated by the system. Ex: NR144926568031212.*
- When done, **Submit** the General Configuration document.

Configuration Validation

You should validate your configuration while logged into E Team by navigating to **Alerts > IPAWS - OPEN Alerts List**

The IPAWS - OPEN Alerts List will display a listing of all alerts from IPAWS available to your COG. If you see the message displayed at the top of the view that reads, Connection to IPAWS Alert Server is not available, please review all configuration steps and then repeat this step. If you continue to experience difficulties, please contact support@NC4.us.