BlackBerry AtHoc IPAWS Plug-in for NDS

Installation and Configuration Guide

NDS 2.9.2, IPAWS 2.9.27

Contents

Overview

In an emergency, response officials need to provide the public with life-saving information quickly. The Integrated Public Alert and Warning System (IPAWS), a modern version of the national alert and warning infrastructure, helps organizations collaborate and alert the public in order to save lives and property.

The Open Platform for Emergency Networks (OPEN) enables the sharing of emergency alerts and incident-related data between different standards-compliant incident management systems. IPAWS OPEN serves as the IPAWS Alerts Aggregator, collecting and routing IPAWS emergency alerts to and from emergency systems that serve the public. IPAWS OPEN integrates with the various alert dissemination methods of IPAWS.

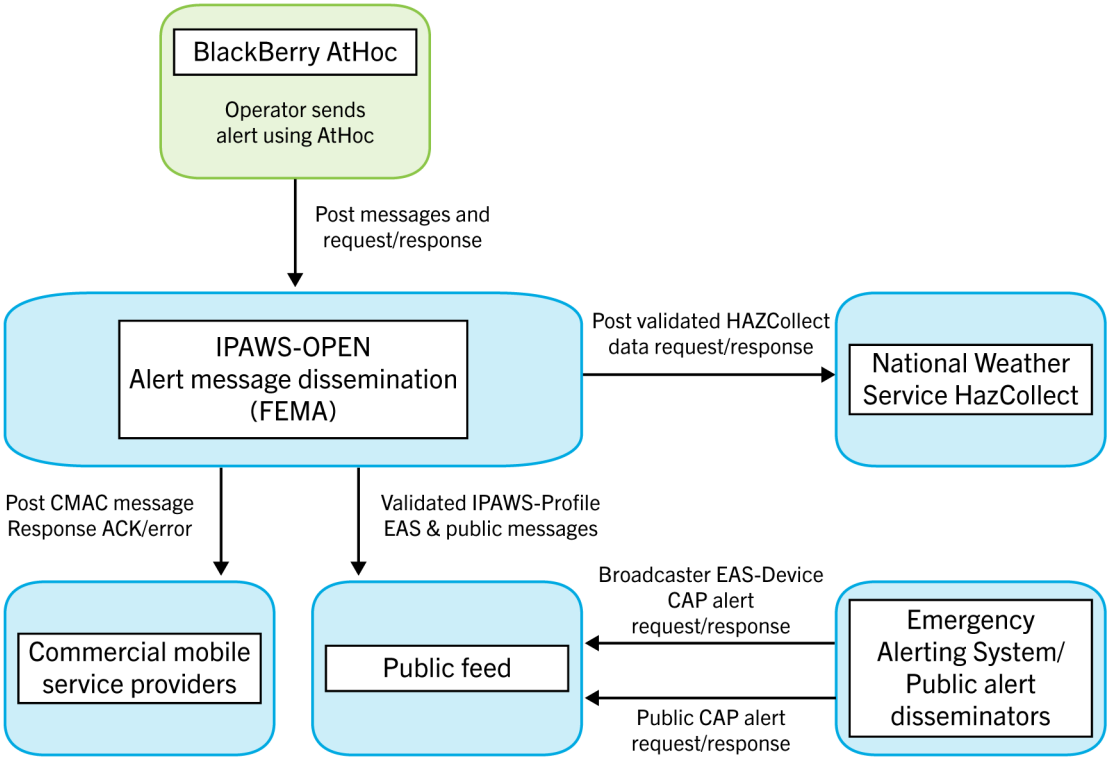


Figure 1: Alert dissemination through BlackBerry AtHoc

IPAWS provides a process for emergency communities at the federal, state, territorial, tribal, and local levels to communicate with each other through alerts. IPAWS helps integrate alerting systems that use Common Alerting Protocol (CAP) standards with the IPAWS infrastructure.

The BlackBerry AtHoc IPAWS plug-in provides support for sending alerts from one Collaborative Operating Group (COG) to other COGs and to public alerting systems such as the Emergency Alert System (EAM), and Wireless Emergency Alerts (WEA).

Using the AtHocNotification Delivery Service (NDS) console, users first configure the plug-in and set up accounts. They then use BlackBerry AtHoc to set up the IPAWS gateways and configure the IPAWS device. In BlackBerry AtHoc, they also create a mass device endpoint for each device as well as their own COG and other COGs with which they want to communicate. Operators can then send alerts through the BlackBerry AtHoc management system and can customize the content for the IPAWS devices. Additionally, users can use the out of the box IPAWS COG to COG Alert Template to notify operators that other COGS have sent alerts to their local system.

Support for WEA2.0

In BlackBerry AtHoc release 7.10 and later releases, the NDS IPAWS plug-in supports both WEA 1.0 and WEA 2.0.

With WEA 2.0, when a specific event type is selected in the Device Options in BlackBerry AtHoc, NDS appends a relevant WEA handling code to the payload before sending it to IPAWS.

The following table shows the mapping of event types and WEA handling codes:

Handling code	Event type	Imminent threat	Public safety	Amber	WEA test	Presidential (restricted)
AVW	Avalanche Warning	X				
CDW	Civil Danger Warning	X				
CEM	Civil Emergency Message	X				
EQW	Earthquake Warning	X				
EVI	Evacuation Immediate	X				
FRW	Fire Warning	X				
HMW	Hazardous Materials Warning	X				
LEW	Law Enforcement Warning	X				
NUW	Nuclear Power Plant Warning	X				
RHW	Radiological Hazard Warning	X				
SPW	Shelter In-place Warning	X				

Handling code	Event type	Imminent threat	Public safety	Amber	WEA test	Presidential (restricted)
VOW	Volcano Warning	X				
BLU	Blue Alert		X			
LAE	Local Area Emergency		X			
TOE	911 Telephone Outage Emergency		X			
CAE	Child Abduction Emergency			X		
DMO	Practice/ Demo Warning				X	
RMT	Required Monthly Test				X	
RWT	Required Weekly Test				X	
EAN	Presidential Alert					X (Restricted for President only. Not applicable to state, territorial, tribal, or local.)

Hardware and software requirements

This section describes the hardware and software requirements for the IPAWS plug-in.

Hardware and firmware requirements

The IPAWS plug-in has the following minimum hardware and firmware requirements:

- A minimum of two Dual-Core Dual CPUs (such as Xeon 51xx family, Xeon E53xx family, or X53xx family), 2 GHz or higher
- One database server core for every two application server cores
- 4 GB for each server
- Dual, redundant Intel NICs and power supplies
- If using BroadCOM NICs, ensure that the latest drivers are installed. Disable the TCP Chimney feature as described in the following Microsoft article: `http://support.microsoft.com/kb/951037`
- The installation procedure requires at least 20 GB free for data.
- Disk space for storage on a RAID 5, RAID 0+1, or RAID 10 configured disk system. The exact allocation of disks depends on the hardware configuration.

Note: Limit SQL RAM usage to 60% of the total system RAM.

Software

The IPAWS plug-in has the following minimum software requirements:

- Notification Delivery Server (NDS) 2.9.27
- BlackBerry AtHoc management system 7.9 or later release
- 64-bit Windows Server 2016
- Microsoft SQL Server 2016
- Internet Information Services (IIS)
- Microsoft .NET Framework 4.7.2

Install and configure the plug-in for NDS

The following sections describe how to install and configure the IPAWS plug-in on the NDS server.

Install the plug-in

The IPAWS plug-in provides the ability to send and receive IPAWS alerts between Collaborative Operating Groups (COGs) using the BlackBerry AtHoc cloud service.

Note: The upgrade steps are the same as the installation steps.

To install the plug-in, complete the following steps:

1. Log in to the NDS server.
2. Stop the BlackBerry AtHoc services:
   a. From **IIS**, select the application server.
   b. On the **Actions** screen, click **Stop**.
   c. Navigate to **Windows Services** and stop `AtHocDeliveryServices`.
3. Copy the IPAWS plug-in .zip file, `AtHoc.NDS.PlugIn.IPAWS_build.zip`, that you received from BlackBerry AtHoc support to a temporary folder.
4. On the file **Properties** screen, click the **General** tab.
5. Click **Unblock** and then extract the contents of the compressed file to a temporary directory.
6. In the temporary directory, rename the following folder: `AtHoc.Delivery.Plugin.IPAWS_build` to the folder name:`IPAWS`
7. Copy the `IPAWS` folder to the following location:

   ```
   <NDSServer>\Program Files (x86)\AtHocENS\DeliveryServer\Plugins\
   ```

   Where <NDSServer> is the name of the server where the NDS is installed.

Open the NDS console

Use the NDS console to manage the NDS.

Prerequisite:The NDS host services must be set up and you must have NDS administration privileges.

1. Open the NDS console in Admin Mode using the following server address:

   ```
   \\AtHocENS\DeliveryServer\Tools\NDSConsole
   ```

For detailed instructions on how to install and configure the NDS console, see the *BlackBerry AtHoc Notification Delivery Service Installation and Configuration Guide*.

Configure the IPAWS plug-in settings

1. Open the NDS console on the NDS server in administrator mode.
2. Navigate to **Management** > **Configuration**.
3. Click **New Configuration**.
4. In the **New Key** field, enter the following value: `nds.plugins.ipaws`

5. From Windows Explorer, open the following file:

```
AtHocENS/DeliveryServer/Plugins/ipaws/AtHoc.NDS.Plugins.IPAWS.dll.config
```

6. Copy the contents and close the file.

```
<nds.plugins.ipaws>
  <supportedDevices>
    <device type="IPAWSNWEM" enabled="true" secondsTimeout="600"
 requiredInilizations="None" maxTasksPerInit="50" maxTasksPerExecution="50"
 maxTasksCanProcess="50" alertCancelOffsetInMin="5"
 certExpirationReminderInDays="40" />
    <device type="IPAWS" enabled="true" secondsTimeout="600"
 requiredInilizations="None" maxTasksPerInit="50" maxTasksPerExecution="50"
 maxTasksCanProcess="50" alertCancelOffsetInMin="5"
 certExpirationReminderInDays="40" />
  </supportedDevices>
  <supportedEvents>
   <event type="Health" enabled="true" />
   <event type="GetMessage" enabled="true" />
  </supportedEvents>
</nds.plugins.ipaws>
```

7. Optionally, configure the value of the `alertCancelOffsetInMin` attribute. The IPAWS plug-in determines when to send an alert termination or cancel message to the IPAWS FEMA server based on the value of the `alertCancelOffsetInMin` attribute. An alert termination or cancel message is sent only when the time difference between the alert expiration time set during alert creation and the actual alert termination time is greater than the `alertCancelOffsetInMin` value. If the alert ends after the specified end time for the alert, or the difference between the alert expiration time set during alert creation and the actual alert termination time is less than the `alertCancelOffsetInMin` value, no alert termination or cancel message is sent.

   Note: The value for the `alertCancelOffsetInMin` attribute must be the same for both devices.
8. Optionally, configure the value of the `certExpirationReminderInDays` attribute. The default is 40 days. When the certificate expiration date is less than or equal to the configured number of days, a warning message is logged in the Event Viewer before every alert publish. The message contains the expiration date of the certificate and the number of remaining days the certificate is valid.

   Note: The value for the `certExpirationReminderInDays` attribute must be the same for both devices.
9. Return to the NDS console and paste the file contents in the **Value** field.
10. Click **Save**.
11. Restart the NDS processes.

    For detailed information, see Restart the NDS processes.

Configure the database server

Before you begin:

- You will need the following information before you configure the database server:
  - The database server name.
  - The SA user password.
  - The name of the ngdelivery database.
- Place the IPAWSConfiguration folder that you obtained from AtHoc sales in a folder on your local computer. This folder contains the `IPAWSConfiguration.bat` and `IPAWSConfiguration.sql` files.

1. Open the **IPAWSConfiguration** folder on your local system.
2. Right-click the `IPAWSConfiguration.bat` file. Click **Edit** and open the file using Notepad.
3. Add the database server instance name, ngdelivery database server name, and the SA user password to the `IPAWSConfiguration.bat` file as shown in the following example:

```
@echo off
@echo Configuring the IPAWS Plugin
rem update the database information in the below statement. Remove the <> from
 <value> and add the respective values.
for %%G in (IPAWSConfiguration.sql) do sqlcmd -S <DatabaseServerInstanceName> -
d <NGDeliveryDBName> -U sa -P "<SAUserPassword>" -i "&&G"
PAUSE
```

4. Save and close the `IPAWSConfiguration.bat` file.
5. Open the `IPAWSConfiguration.sql` file.
6. Verify that the @deviceType values are **IPAWS** and **IPAWSNWEM**.

```
DECLARE @deviceType1 NVARCHAR(50)
DECLARE @deviceType2 NVARCHAR (50)
DECLARE @SQL AS VARCHAR (MAX)

SELECT @deviceType1='IPAWS'
SELECT @deviceType2='IPAWSNWEM'

IF NOT EXISTS (SELECT * FROM NGDeliveryAccount.dbo.DatacenterSiteDetail a INNER
 JOIN ProductInfo b ON a.SiteId=b.SiteId WHERE a.DeviceType=@deviceType1)
    BEGIN
        INSERT INTO NGDeliveryAccount.dbo.DatacenterSiteDetail([DataCenterId],
[SiteId] ,[DeviceType],[CreatedOn])
        SELECT 1,siteid , @deviceType1,GETUTCDATE() FROM ProductInfo
    END
IF NOT EXISTS (SELECT * FROM NGDeliveryAccount.dbo.DatacenterSiteDetail a INNER
 JOIN ProductInfo b ON a.SiteId=b.SiteId WHERE a.DeviceType=@deviceType2)
    BEGIN
        INSERT INTO NGDeliveryAccount.dbo.DatacenterSiteDetail([DataCenterId],
[SiteId] ,[DeviceType],[CreatedOn])
        SELECT 1,siteid , @deviceType2,GETUTCDATE() FROM ProductInfo
    END
IF COL_LENGTH('NGDeliveryAccount.dbo.DatacenterSiteDetail', 'ResourceType') IS
 NOT NULL
BEGIN
    SET @SQL = 'UPDATE NGDeliveryAccount.dbo.DatacenterSiteDetail SET
 ResourceType =''RATE'' WHERE DeviceType = ''IPAWS''OR DeviceType =
 ''IPAWSNWEM'''
    EXEC(@SQL)
END
```

When you log in to the database server, there are **IPAWS** and **IPAWSNWEM** entries in the **DeviceType** column in the **ngdeliveryaccount** > **DatacenterSiteDetail** table and the ResourceType is **RATE**.

Verify the IPAWS plug-in installation

1. Navigate to the following folder: `..\AtHocENS\DeliveryServer\Tools\NDSConsole` and run the `AtHocNDSConsole.exe` file.
2. In the NDS console, navigate to **Console** > **Testing**.

3. Verify that the IPAWS and the IPAWSNWEM devices are included in the **Supported Devices** section.

Manage organization accounts for the plug-in

This section describes how to create the organization account and the user for IPAWS on the NDS server. The NDS account manages all NDS plug-ins that you have.

Do not perform these tasks if you already have an NDS account.

Create a customer account

Create an account for each client site. This account serves all the organizations (formerly called "virtual systems" or "VPS"s) that use IPAWS on the system. The account is associated with an NDS user that manages the NDS plug-ins.

1. Open the NDS console from the NDS server in admin mode.
2. Navigate to **Management** > **Account**.
3. On the **Account Management** screen, click **New Account**.
4. On the **New Account** screen, enter the **Display Name**, which is the name used when configuring the IPAWS delivery gateway in BlackBerry AtHoc management system. Keep the following defaults:
   - **Status**: Active
   - **Enable anonymization**: Selected
5. Click **Save**.

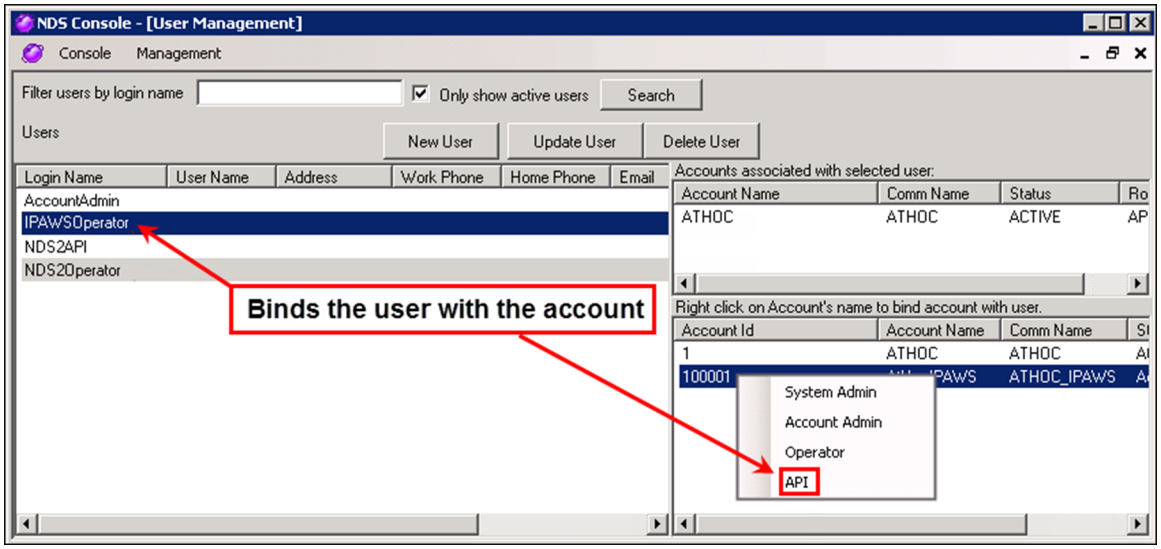
Create a user

Create a user who is associated with the customer account and manages the NDS account and plug-ins.

1. In the NDS console, navigate to **Management** > **User**.
2. Click **New User**.
3. On the **New User** screen, enter values in the **Login Name**, **Password**, and **Confirm Password** fields.

   This login name and password is used to configure the delivery gateway in the BlackBerry AtHoc management system.
4. In the **Status** field, select **Active** from the list.
5. Optionally, add a description.
6. Click **Save**.
7. To associate the user with an account:
   a. On the **User Management** screen, select the user name.
   b. Right-click an account name and click **API**.

      The user is then associated with the IPAWS account.



Enable the IPAWS plug-in for the account

After you have created the user and associated it with the IPAWS account, you must enable the IPAWS plug-in.

1. In the NDS console, navigate to **Management** > **Account**.
2. On the **Account Management** screen, select the account that you created in the Create a customer accountsection.
3. Click the **Account Resource** tab.
4. Select the **IPAWS** and **IPAWSNWEM** device type check boxes.
5. Ensure that the value in the **Resource Type** column is **Rate**.
6. Click **Save**.

Restart NDS processes

After you have configured or modified the plug-in settings, restart the NDS processes.

1. From the NDS server, open the **Server Manager** as an administrator.
2. Navigate to **Configuration** > **Services**.
3. Restart the **AtHocDeliveryService** service.

Verify the IPAWS plug-in process is running

1. Open the NDS console and start NDS.
2. Open the **Task Manager** and check the `AtHocNDSConsole.exe*32` process.
3. If the `AtHocNDSConsole.exe*32` process is not running, perform the following steps:
   a. Open a command prompt and run as administrator.
   b. Navigate to the following directory: *`NDSServer`*`\Program Files (x86)\AtHocENS\DeliveryServer\Plugins\IPAWS`.
   c. Enter `Run AtHocNDSConsole.exe*32`.

Add the IPAWS certificate

For security purposes, you must add the IPAWS certificate to each application server with NDS. This section describes how to generate the certificate for use on the NDS server associated with the sender COG.

Note: You can configure multiple certificates for each virtual system.

Prerequisites

You need the following information provided by FEMA:

- The COG identifier for the sending COG
- The `.jks` certificate file provided by IPAWS.
- The Key and Keystore password for the certificate. These can be found in the <*COG_ID*>`.txt` file.

Convert the certificate

1. Do one of the following:
   - If you are a BlackBerry AtHoc employee, navigate to the `...\Released - GA\I2\IPAWS \IPAWSCertificateConverter` directory and copy the IPAWSCertificateConverter to the NDS server.
   - If you are a BlackBerry AtHoc customer, use the certificate provided by FEMA.
2. Place the .jks file in the same folder as the IPAWSCertificateConverter.exe file.
3. Run the IPAWSCertificateConverter.exe file.
4. On the **JKS to P12 Converter** dialog, enter the following information:
   - **Certificate File Name**: Enter the name of the .jks file without the .jks extension. For example, enter IPAWSOPEN_120009 for the certificate file IPAWSOPEN_120009.jks file.
   - **Key Password**: Enter the Key Password from the <*COG_ID*>`.txt` file.
   - **Keystore Password**: Enter the Keystore Password from the <*COG_ID*>`.txt` file.
5. Click **Convert**.

A .p12 file is created in the same folder as the .jks file with the same certificate file name as the .jks file.

Upload the converted certificate

After you have converted the certificate to the accepted file type, you must upload the certificate to the Keystore through the NDS console.

1. Log in to the NDS console with an administrator account.
2. Click **Utilities**.
3. In the **Import System Certificate** section, enter the certificate information:
   - **Certificate Name**: Enter the COG_ID.
   - **Certificate File**: Click **Load File** to browse to and select the IPAWS certificate .p12 file for the specific COG_ID.
   - **PKCS12 File (.pksl.p12) password**: Enter the password for the .p12 file.
4. Click **Import**.

Tip: Mark your calendar with the date the FEMA certificate expires for license renewal.

Replace an expired certificate

The IPAWS certificate can expire every three years. The steps to replace an expired certificate are the same as uploading a new certificate. When you upload a new certificate, the expired certificate is replaced as long as the same certificate name is used.

Important: If you receive a request from FEMA to replace an expired certificate, do not delete the expired certificate.

1. Log in to the NDS console with an administrator account.
2. Click **Utilities**.
3. In the **Import System Certificate** section, enter the certificate information:
   - **Certificate Name**: Enter the COG_ID.
   - **Certificate File**: Click **Load File** to browse to and select the IPAWS certificate .p12 file for the specific COG_ID.
   - **PKCS12 File (.pksl.p12) password**: Enter the password for the .p12 file.
4. Click **Import**.
5. Configure the certificate for the NDS account.

Tip: Mark your calendar with the date the FEMA certificate expires for license renewal.

Remove a certificate

If you need to replace an expired certificate, do not delete it. Instead Replace an expired certificate.

1. Log in to the NDS console with an administrator account.
2. Click **Management** > **Configuration**.
3. Select the **nds.certificate.repository** node.
4. In the right pane, highlight the encrypted data for the <Certificate> attribute for the certificate you want to delete.

   Important: Do not click the **Delete** button. This will delete all certificates.
5. Press **Delete** on your keyboard to delete the highlighted data.
6. Select and remove the extra space in the XML left after deleting the certificate data.
7. Click **Update**.
8. Configure the certificate for the NDS account.

Configure the certificate for the NDS account

1. Log in to the NDS console.
2. Click **Configuration**.
3. Click **New Configuration**.
4. In the **New Key** field, enter **nds.plugins.ipaws.accountConfig**.
5. In the **AccountId** field, enter the account ID of the specific account that you want to provide authorization for.
6. Leave the **Device Type** field empty.
7. In the **Value** field, enter the following configuration. Add the certificate name (COG_ID) in the <CertName> attribute. The certificate name should be the same name you used when uploading the certificate to NDS.

```
<AccountConfig>
<AuthorizedCertificates>
<CertName>certifcateName</CertName>
</AuthorizedCertificates>
```

```
</AccountConfig>
```

Note: Each account can support multiple certificates. Add additional <CertName> attributes inside the <AuthorizedCertificates> attribute for each certificate.

8. Click **Save**.
9. Optionally, to update the configuration immediately, restart the AtHocDeliveryService.

Configure IPAWS in the BlackBerry AtHoc management system

The following sections describe how to configure support for IPAWS alerting in BlackBerry AtHoc management system. Complete all tasks.

Enable the Inbound Event Manager for IPAWS

After you finish the installation or the upgrade of the database server, enable the Inbound Event Manager (IEM) for IPAWS.

1. Deploy the database script files:
   a. Open Microsoft SQL Server Management Studio and connect to the database server.
   b. Log in as “sa” (or “ngad”).
   c. From the **Query** window, open `Enable_IEM.sql`.
   d. **Click Execute** from the Query window.
2. Restart IIS and the AtHoc Services.
3. Log in to the BlackBerry AtHoc management system as an administrator.
4. Change to the **System Setup (3)** organization.
5. Click .
6. In the **System Setup** section, click **System Jobs**.
7. On the **System Tasks** window, click **IEM IPAWS Plugin Agent - For All VPS**.
8. On the **job details** page, in the **Task Details** section, click **Click to Enable**.

Configure the IPAWS package on the BlackBerry AtHoc server

Before configuring IPAWS in BlackBerry AtHoc management system, you must enable the IPAWS package on the BlackBerry AtHoc application server.

1. Open a remote desktop session and log in to the BlackBerry AtHocapplication server.
2. Navigate to the following folder:

```
..\AtHocENS\ServerObjects\Tools
```

3. Open the following package: `AtHoc.Applications.Tools.InstallPackage`.
4. On the **Configure Device Support** screen, select **IPAWS (East)** and **IPAWS (West)**.
5. Click **Enable**.
6. Click **OK**.

Configure the event codes list for IPAWS devices

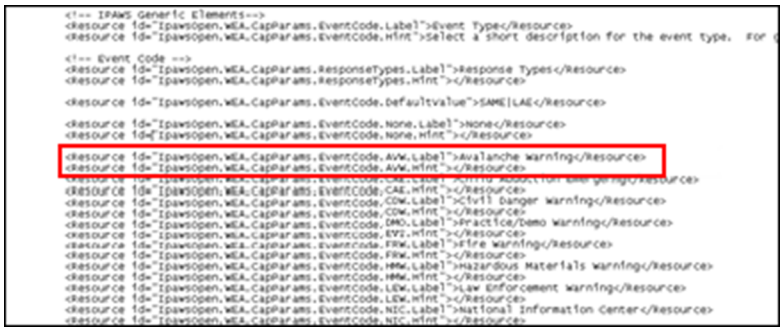
BlackBerry AtHoc has a robust list of event codes. However, you might want to remove some of the codes from the list to simplify choices for operators during an emergency.

1. Log in to the BlackBerry AtHoc application server as an administrator.

2. Navigate to the following folder:

```
<AtHocENS>/ServerObjects/utils/AddOnModules/UAP/Enable
```

3. Locate the file `30-UAP-IPAWS-WEA-EXTENSIONS.xml`.
4. Make a backup copy of the file in a temp folder.
5. Edit the file in Notepad and remove any event codes your organization is not using. For example, in the following image, the avalanche warnings are removed because they are not needed in West Texas.



6. Scroll to the **<Features>** section of the file and remove each feature that matches the codes your removed earlier.

7. Save the file and close Notepad.
8. Log in to the BlackBerry AtHoc management system.
9. In the navigation bar, click ⚙.
10. In the **Devices** section, click **Devices**.
11. On the **Device Manager** screen, select **IPAWS**.
12. Click **Enable**.

Verify the event codes list

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Alerts** > **New Alert**.
3. On the **Select from Alert Templates** window, click **Create a Blank Alert**.
4. On the **New Alert** screen, in the **Mass Devices** section, select **IPAWS**.
5. Click **Options**.
6. On the **Mass Device Options** screen, click the **IPAWS WEA** or **IPAWS WEA 2.0** tab.

7. From the **Event Type** list, select the event types that are associated with the IPAWS device in the system.
8. Confirm that the event codes you selected earlier appear in the list.

Set up BlackBerry AtHoc for IPAWS devices

The following sections describe how to set up IPAWS in BlackBerry AtHoc, including how to set up the BlackBerry AtHoc IPAWS gateways, device, and endpoints.

Public communication

BlackBerry AtHoc supports the following three devices for public alerting systems that disseminate alerts:

- Wireless Emergency Alerts (WEA 1.0 or WEA 2.0)
- Non-Weather Emergency Message (NWEM)
- Emergency Alerting System (EAS)

To send out alerts using these devices, you must first configure three devices through the BlackBerry AtHoc Device Manager screen. You then create mass communication end users for each device: one for WEA, one for NWEM, and one for EAS.

Tip: Create end user accounts that include the device type in the account name: for example, “IPAWS_WEA”.

COG to COG communication

To communicate between COGs, use the CAP Exchange IPAWS device. You can create one mass communication end user for each organization involved.

Before you begin, plan each sender and target COG name that you need along with common user names. Each COG represents an organization. You can create a mass communication end user for your COG (the sender) and for each target COG (another organization) to which you plan to send alerts. The other COGs creates a mass communication end user in their organizations and for any target COG.

Tip: When possible, have each COG create users with consistent user names for each COG that match the names that other COGs are using.

For example, you use BlackBerry AtHoc and IPAWS for your medical center and you plan to communicate with two COGs in your area: the local police, and the local university. You need three mass communication end-users. Working with the other two organizations, you agree to the following user names:

- Town: OurTown
- Police: OurPolice
- University: OurUniversity

Each COG creates three end users in their own organization using these common user names. The following table might help in planning for the sender and target COG user names for your organization. Each COG should do the same. Remember, the sender COG is your own organization and the target COGs are other organizations to which you are sending alerts.

Organization	ORG_ID	User name	Sender COG	Target COG
ORG_Town	12345	OurTown	Yes	No
ORG_Police	23456	OurPolice	No	Yes
ORG_University	34567	OurUniversity	No	Yes

Configure the IPAWS gateways

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click the **IPAWS (West)** gateway.
4. Click **Copy default settings**.

   Note: You must complete this step during upgrade.
5. Enter the **Notification Delivery Server address**, **Username**, and **Password** provided to you by BlackBerry AtHoc support or by your organization.
6. Enter the **COG ID** provided to you by FEMA.
7. Enter your COG name and location in the Sender Name field using the following format: `COGName`, `City`, `State Abbreviation`. For example: `TestCOG`, `San Mateo`, `CA`.
8. In the **End Point** field, enter the server URL for your sandbox or production system as provided by FEMA. For example:

   ```
   https://tdl.integration.fema.gov/IPAWS_CAPService/IPAWS
   ```
9. In the **CAP Default Values** field, change the following values:

   - `sender`: Change the value to an organization name that other COGs can recognize.
   - `source`: Change the value to a name or organization that other COGs or the public can recognize, such as "San Mateo County Emergency Services".

   Note: The values of **sender** and **source** cannot contain spaces, commas, or restricted characters (< or &). The values of **sender** and **source** cannot contain spaces, commas, or restricted characters (< or &).

   Tip: Use a common username among all COGs. Ideally, all COGs can use the same common username in their own organization.
10. Click **Save**.
11. Click **<< Back** to return to the **Settings** page.
12. In the **Devices** section, scroll down and click the **IPAWS (East)** gateway.
13. Repeat Steps 4 to 10 to configure the second IPAWS gateway.

You are now ready to configure the related devices using the Devices Manager.

Configure the device

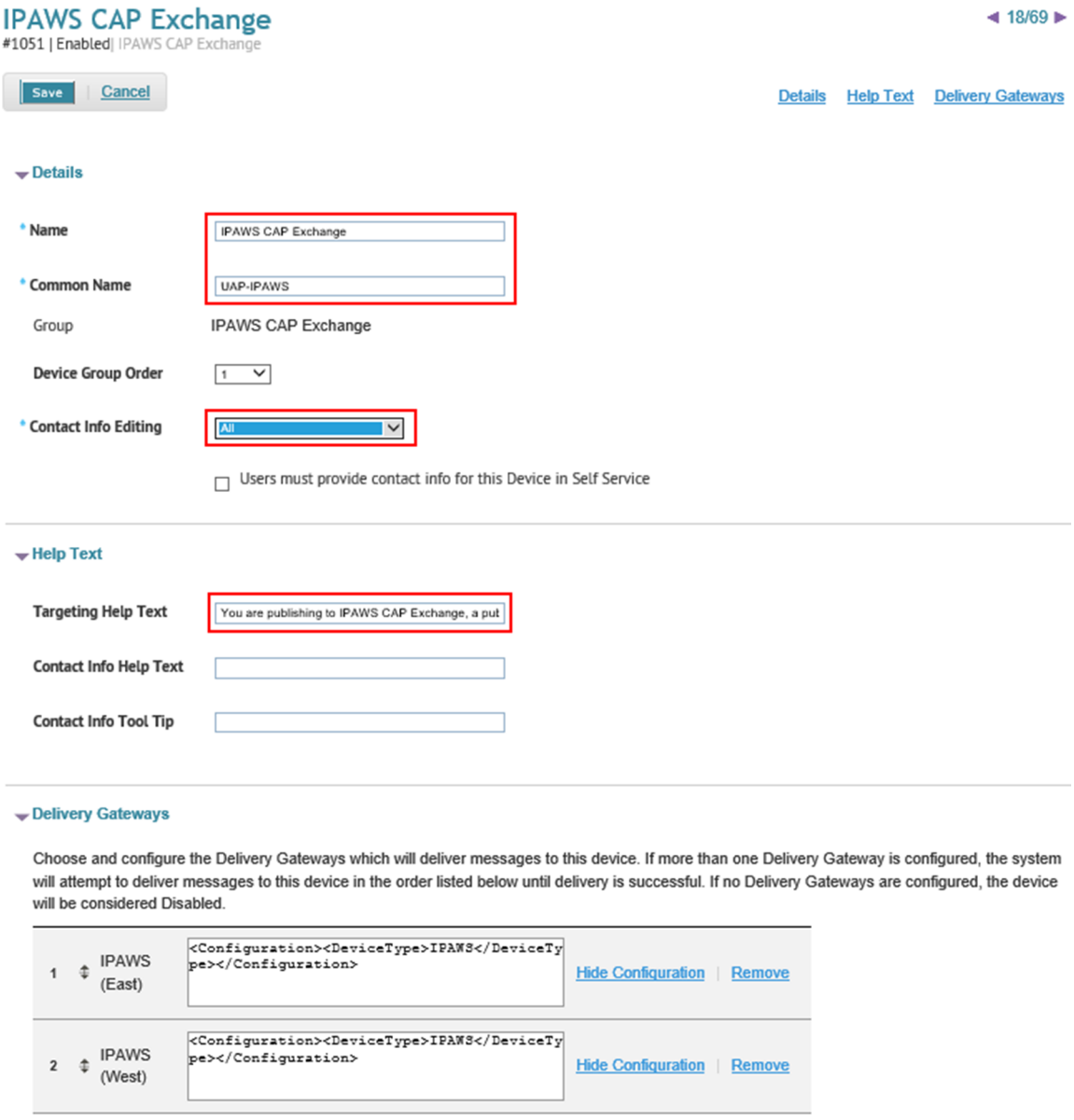
To configure the device, complete the following steps:

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Devices**.
4. Click to open one of the following IPAWS specified devices:

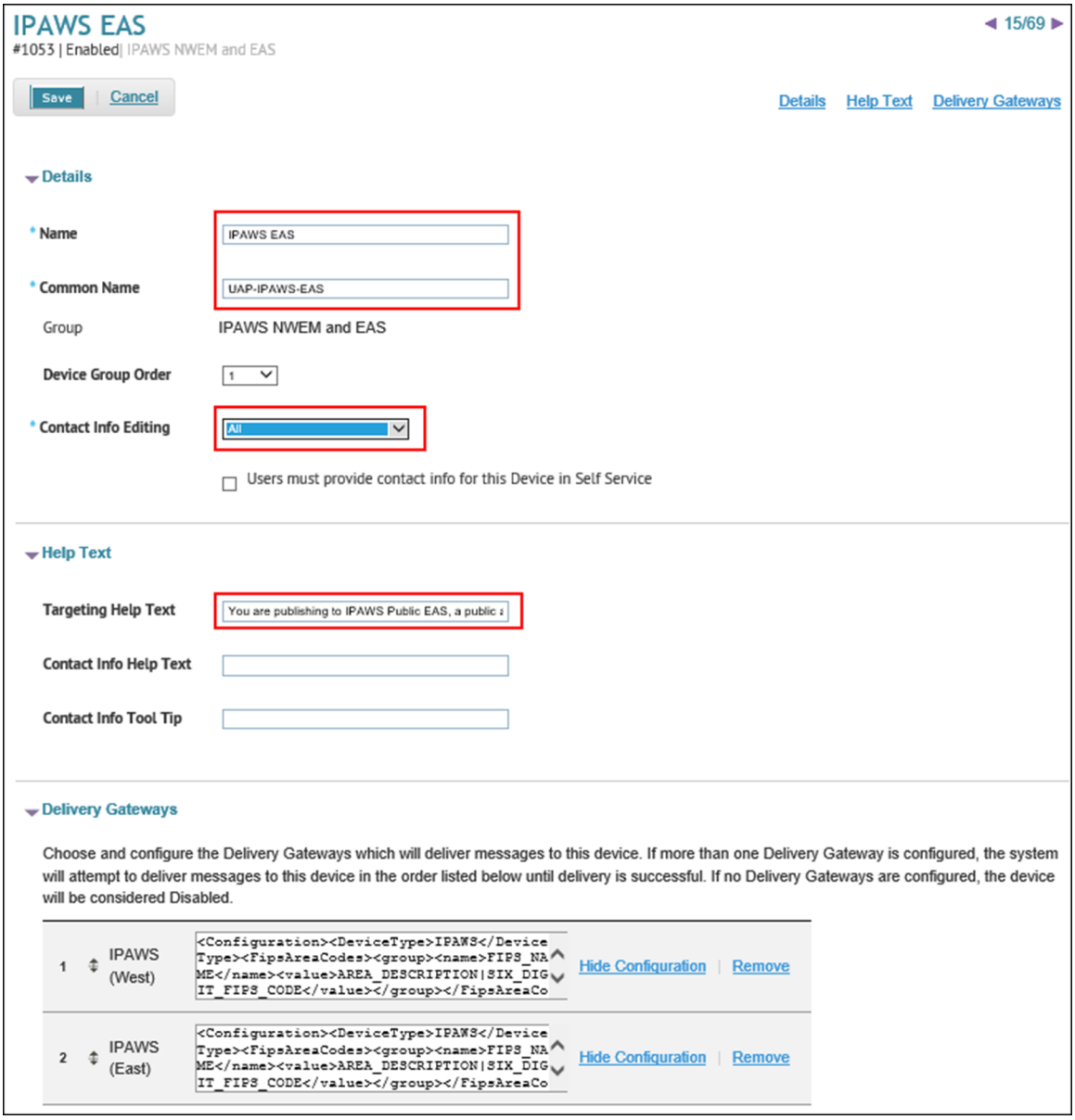
   - IPAWS CAP Exchange
   - IPAWS EAS
   - IPAWS NWEM
   - IPAWS WEA
   - IPAWS WEA 2.0

   A new screen appears, displaying the settings for the device.
5. Click **Edit**.
6. Modify the values in the **Details** section, adding names and information valid for your organization.

7. In the **Contact Info Editing** field, select **All** or **End Users**. Selecting the check box specifies whether end users must provide contact information in Self Service.
8. Update the values in the **Details** and **Help Text** sections as shown in the following images:
   - IPAWS CAP Exchange is used for COG to COG alerts

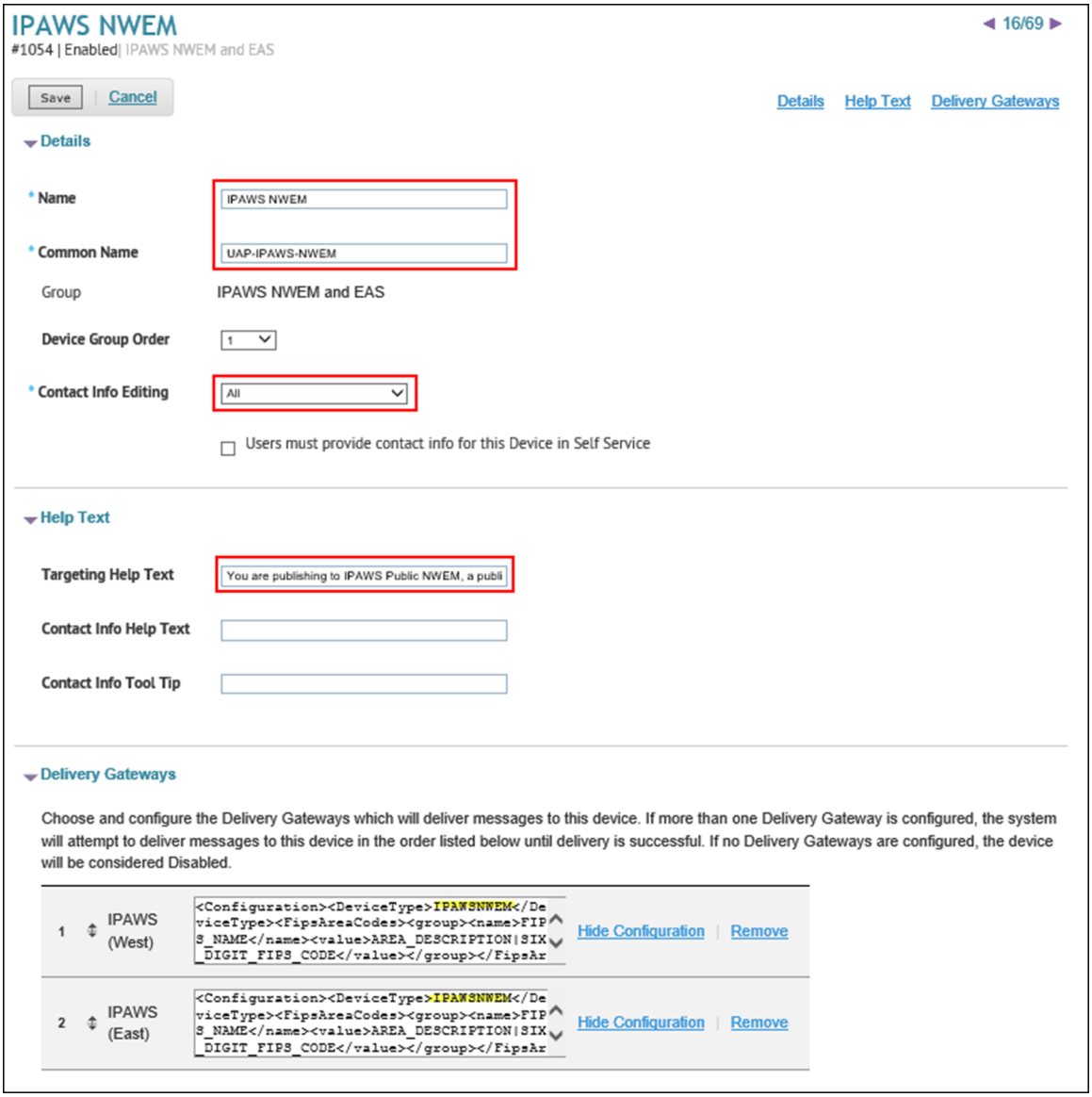


   - Public Communications: IPAWS EAS

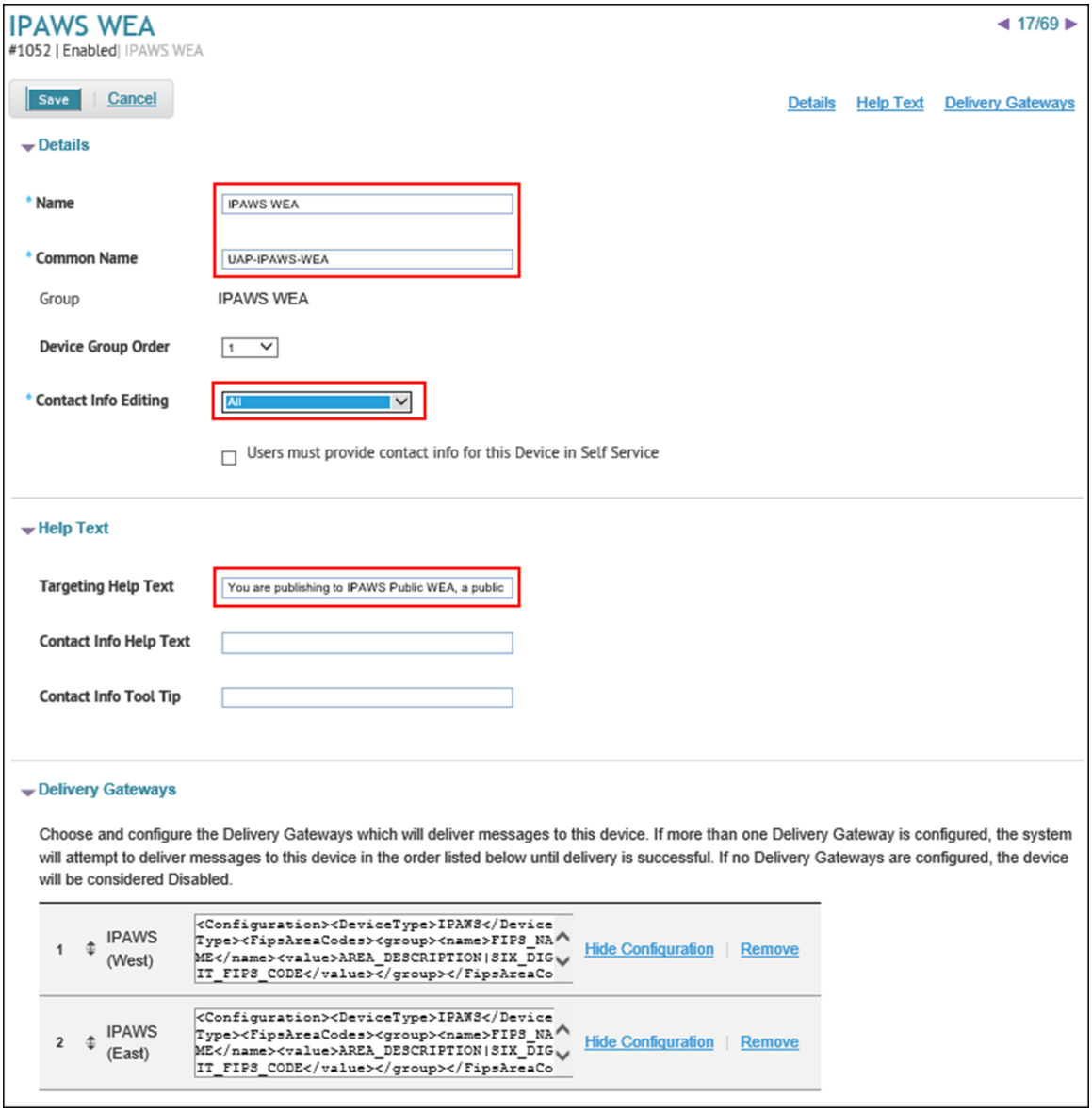


- Public Communications: IPAWS NWEM

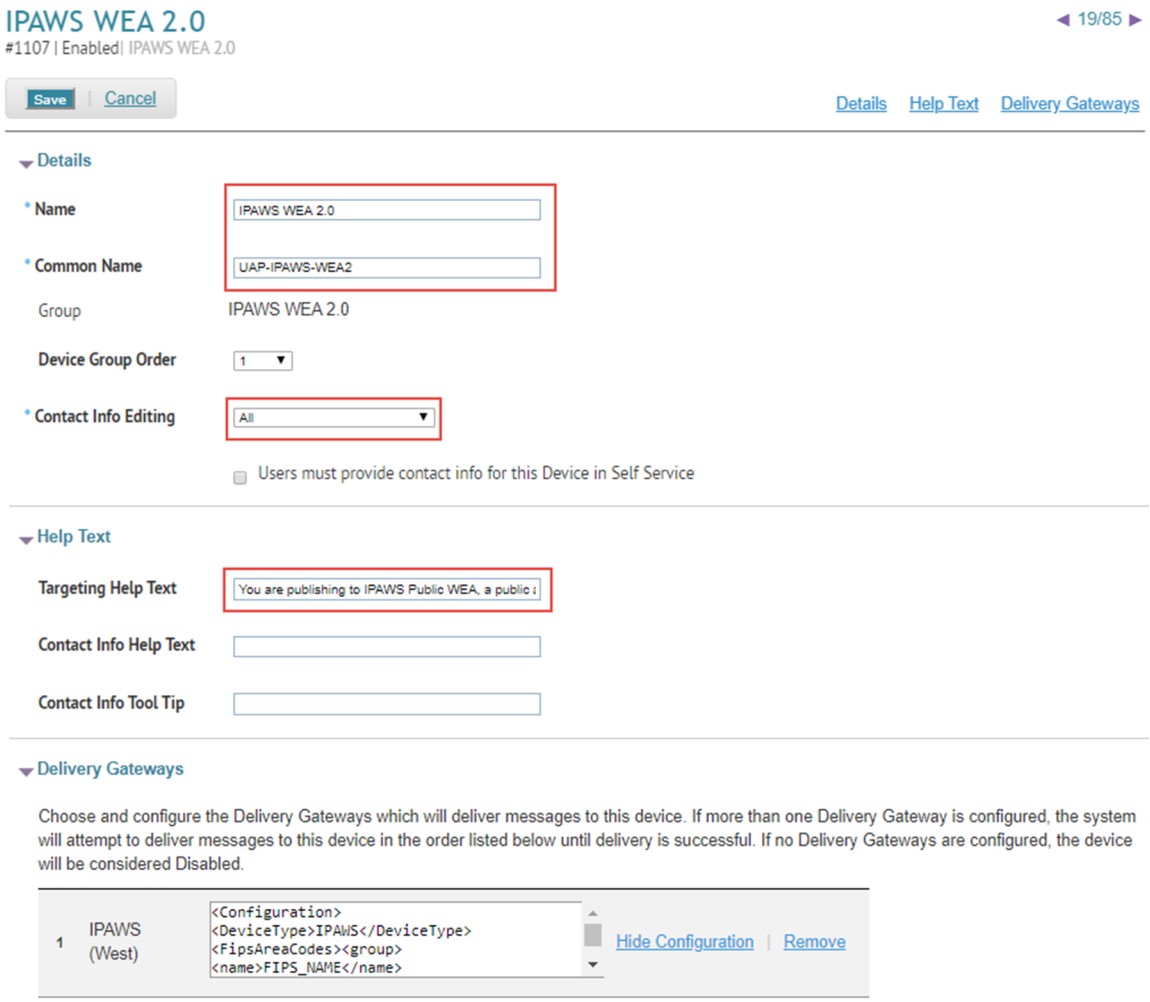
  Note: This device requires a different DeviceType in the Delivery Gateway XML configuration: *IPAWSNWEM*.



- Public Communications: IPAWS WEA



9. Public Communications: IPAWS WEA 2.0



10. For each of the devices, update the **Delivery Gateway XML** content.
11. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and select **IPAWS (West)**.
12. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and select **IPAWS (East)**. The IPAWS (East) gateway can be used as a failover gateway.
13. Click **Configure** to view the XML. Each of the above images shows the XML for the device. The following is the default configuration XML:

```
<Configuration>
    <DeviceType>IPAWS</DeviceType>
    <FipsAreaCodes>
       <group> <name>FIPS_NAME</name>
 <value>AREA_DESCRIPTION|SIX_DIGIT_FIPS_CODE</value> </group>
     </FipsAreaCodes>
</Configuration>
```

14. Make the following updates, with only one value for each field. If you need to input additional names, repeat the <group></group> tag. Commas (,) are not allowed in values:

- `DeviceType`: IPAWS or IPAWSNWEM (for IPAWS NWEM only)
- `name`: A geographical area name, such as a county name and the FIPS code for the area. For example: “San Mateo County-006081”
- `value`: An area description and the six-digit FIPS code provided by FEMA. For example: “San Mateo County|006081”

For example:

```
<Configuration>
    <DeviceType>IPAWS</DeviceType>
    <FipsAreaCodes>
       <group> <name>San Mateo County-006081</name> <value>San Mateo County|
123456</value> </group>
       <group> <name>Contra Costa County</name> <value>San Mateo County|
234567</value> </group>
     </FipsAreaCodes>
</Configuration>
```

15. Click **Save**.
16. Click **Enable** if you are ready to make the device available for alert publishing.

Create a mass device endpoint for each COG

To distribute messages to other COGs, you must create a BlackBerry AtHoc mass device endpoint for your local COG and for each target COG to which you send alerts. You can name each user something relevant like "COG-ContraCostaCounty_<cogid>" or "COG-MyCOG_<cogid>".

Tip: When possible, plan to use consistent usernames for each mass communication endpoint across each COG.

Note: You must have administrator, advanced alert manager, or end-user manager privileges to create end users.

1. Log in to the BlackBerry AtHoc management system as an administrator, advance alert manager, or end-user manager.
2. In the navigation bar, click .
3. In the **Devices** section, click **Mass Device Endpoints**.
4. Click **New**, and then select the **IPAWS CAP** exchange.
5. On the **New Mass Device Endpoint** screen, in the **General** section, in the **Endpoint Name** and **Common Name** fields, enter a descriptive label, such as “COG123456.”
6. In the **Configuration** section, in the **Address** field type the **COG ID**.
7. Click **Save**.
8. Repeat steps 1 to 7 for all peer COGs.

Create mass device endpoints for public alerting devices

To distribute messages to the public through one or more IPAWS public alerting devices (EAS, NWEM, WEA, or WEA 2.0), create a mass device endpoint for the device. Name each endpoint something relevant like "IPAWS WEA”.

Note: You must have Administrator, Advanced Alert Manager, or End-User Manager privileges to create the end users.

1. Log in to the BlackBerry AtHoc management system as an administrator, advance alert manager, or end-user manager.
2. In the navigation bar, click .
3. In the **Devices** section, click **Mass Device Endpoints**.
4. Click **New**, and then select the IPAWS device.
5. On the **New Mass Device Endpoint** screen, in the **General** section, in the **Endpoint Name** and **Common Name** fields, enter the name of the device.
6. In the **Configuration** section, enter the COG ID for your organization in the **Address** field.
7. Click **Save**.
8. Repeat steps 1 to 7 for each IPAWS device.

Send a test alert to target COGs

You can create alerts and send them to target COGs using standard alert processes.

1. Log in to the BlackBerry AtHoc management system with an administrator account.
2. Do one of the following:
   - On the BlackBerry AtHoc home page, in the Quick Publish section, click **Create a Blank Alert**.
   - In the navigation bar, click **Alerts** > **New Alert**. On the **New Alert** screen, click an existing alert to edit an alert template or click **Create a Blank Alert**.
3. On the **New Alert** screen, in the **Content** section, enter the title and content of the alert.
4. Select the severity and type of the alert.
5. In the **Mass Devices** section, select **IPAWS Cap Exchange** and then from the list select one or more COGs.
6. On the **Mass Devices** section, click **Options**.
7. On the **Mass Devices Options** screen, complete the following steps:
   a. From the **Event Type** list, select the **FEMA event type** to be used for the alert.
   b. Optionally, select a severity from the **Severity** list. The default is Severe.
   c. Optionally select a certainty from the **Certainty** list. The default is Observed.
   d. Optionally, select an urgency from the **Urgency** list. The default is Immediate.
   e. In the **IPAWS Alert Content** section, select the **Alert Title and Body** to use the content that you specified in the **Content** section.
8. If you are sending an alert to multiple audiences, you might want to customize the text for the FEMA recipient. For example, you can send an alert to your emergency team with instructions for handling the emergency. If you also include a COG, you might want to alert them to the situation without providing instructions. In this case, select **Custom Text** and then provide alert text that is appropriate for COG alerts.
9. Click **Apply**.
10. Click **Review & Publish** to review the alert.
11. Click **Publish** to send the alert.

Note: The severity you selected in the IPAWS device options is not the severity that is displayed on the Review and Publish page. The severity displayed on the Review and Publish page is the severity of the delivered IPAWS alert.

Send a test alert to public alerting devices

You can create and send alerts to the public using standard alert processes. You can select a map shape to specify which FIPS codes are selected for the IPAWS public alert devices such as, NMEW, EAS, WEA, and WEA 2.0.

Note: Public alerting devices are activated by geolocation. When you target by location (with a map shape), FIPS codes are automatically appended to the alert and sent to FEMA.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Do one of the following:
   - On the BlackBerry AtHoc homepage, in the **Quick Publish** section, click **Create a Blank Alert**.
   - In the navigation bar, click the **Alerts** > **New Alert**. On the **New Alert** screen, click an existing alert to edit an alert template or click **Create a Blank Alert**.
3. On the **New Alert** screen, enter the title and content of the alert in the **Content** section.
4. Select the severity and type of the alert.
5. In the **Location** field, click **Add**.
6. On the map that appears, use the drawing tools to specify an alert location and click **Apply**.
7. In the **Mass Devices** section, select one or more IPAWS public devices. For example, IPAWS EAS.

Note: You must select an area on the map in the Content section to activate the IPAWS public alert devices. If you do not, warnings appear next to the selected devices.

8. Click **Options** in the **Mass Devices** section.
9. On the **Mass Devices Options** screen, complete the following steps:
   a. Select the tab for the device you need to customize.
   b. Select an **Event Type** from the list.
   c. Optionally, select a **Severity** from the list. The default is Severe.
   d. Optionally, select a **Certainty** from the list. The default is Observed.
   e. Optionally, select an **Urgency** from the list. The default is Immediate.
   f. Select a response type from the **Response Types** list. This option tells the public how to respond to the alert.

      Important: Before sending an alert to the public, test it thoroughly to avoid providing confidential, confusing, or incorrect information.
   g. Select an **IPAWS Alert Content** option.

      If you are sending an alert to both your team and to the public, you can customize the text for public recipients. For example, you send an alert to your emergency team with instructions for where to report for work. You would customize text for the general public to alert them to the situation without providing work instructions.

      - For NWEM and EAS, you can choose between the alert title and body text or custom text.
      - For WEA, you can choose between the alert title text, custom text, or the FEMA text. If you have authorization from FEMA, you can use Commercial Mobile Alert Message (CMAM) content. Choose one of the following:
        - **Use FEMA Standard Text**: Use text provided by the FEMA template.
        - **Use Text from Title of Alert**: Use the title text from the alert Content section. This is the default.
        - **Custom Text**: Enter alert content that is appropriate for public alerts. You must have CMAM authorization from FEMA.

        Note: WEA has a text limit of 100 characters.
      - For WEA 2.0, you can choose between the alert title text or custom text. Choose one of the following:
        - **Use Text from Title of Alert**: Use the title text from the alert Content section. This is the default.
        - **Custom Text**: Enter alert content that is appropriate for public alerts.

          Choose one of the following options:
          - **English**
          - **English and Spanish**

        Note: WEA 2.0 has a text limit of 360 characters for each custom text entry.
10. Click **Apply**.
11. Click **Review & Publish** to review the alert.
12. Click **Publish** to send the alert.

Note: The severity you selected in the IPAWS device options is not the severity that is displayed on the Review and Publish page. The severity displayed on the Review and Publish page is the severity of the delivered IPAWS alert.

Configure BlackBerry AtHoc to receive alerts from external COGs

To receive alerts from other COGs, you must create an incoming alert. You then link the incoming alert with an alert template that triggers an alert for the operator.

The operator can then alert the organization as appropriate.

Note: IPAWS incoming alerts do not appear in the Inbox. To see the alerts, you must trigger an alert to notify the operator.

1. Create custom placeholders for the alert template
2. Update the IPAWS alert template that notifies the operator
3. Configure COG incoming alerts
4. Test the incoming alert

Create custom placeholders for the alert template

Alert placeholders correspond to XML nodes in the CAP Payload XML. You create the placeholders to provide specific information in the alert that is delivered by the CAP Payload.

To see the XML for the CAP Payload, see Appendix A: CAP Payload XML.

1. Log in to BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Alerts** > **Alert Placeholders**.
3. Click **New** > **Text**.
4. Create a placeholder called `sender` using the values in the placeholder fields:
   - Name: `sender`
   - Minimum length: `1`
   - Maximum length: `400`
   - Lines to show: `3`
   - Default value: `sender`
5. Click **Save**.
6. Repeat steps 3 to 6 for each of the following additional placeholders, using the same Minimum length, Maximum length, and Lines to show values for each of the placeholders. The Default value field should contain the following placeholder names:
   - sent
   - msgType
   - severity
   - expires
   - headline
   - description
   - instruction
   - urgency
   - category
   - responseType
7. Click **Save** after creating each placeholder.

When you have created all of the placeholders, you are ready to create the alert template that is used to alert the operator.

Update the IPAWS alert template that notifies the operator

In this section, you update the out of the box IPAWS COG to COG Alert Template that is triggered when a message from an outside (sender) COG arrives as an incoming alert. The template contains the custom placeholders that were previously created. When the template gets triggered, the placeholders are replaced by the contents of the CAP Payload XML from the sender COG. The alert is sent to the operator with the content of the message from the sender COG. For more information about creating alert templates in BlackBerry AtHoc, see the *BlackBerry AtHoc Manage Alert Templates User Guide*.

1. Log in to BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Alerts** > **Alert Templates**.
3. Select the **IPAWS COG to COG** Alert Template.
4. Optionally, in the **Alert Template** section, modify the name for the template. For example, IPAWS Alert.
5. Optionally, modify the description of the alert template.
6. Optionally, in the **Content** section, modify the **Title** to include any non-predefined content such as [[severity]]. The following predefined text is included the Title field, using the IPAWS custom placeholders:

```
CAP Exchange message from [[sender]] [[sent]]
```

7. Optionally, modify the text in the **Body** field. The following text is predefined in the template:

```
[[msgType]] received with [[severity]] until [[expires]].
Headline: [[headline]]
Descripton: [[description]]
Instructions: [[instruction]]
Urgency: [[urgency]]
Category: [[category]]
Response Type: [[responseType]]
```

8. In the **Target Users** section, use the **By Groups**, **By Users**, **By Location**, and **By Advanced Query** tabs to identify the end users who should receive the alert. These are typically operator users.
9. Click the **Select Personal Devices** tab and then specify the appropriate devices on which operators receive alerts.
10. Optionally, make selections in the other sections of the alert template.
11. Click **Save**.

When you have finished creating the alert template, you are ready to configure the incoming alert.

COG incoming alerts

Incoming alerts for IPAWS, are predefined in the BlackBerry AtHoc system. When an incoming IPAWS alerts is received, the out of the box IPAWS COG to COG Alert Template that you modified in the previous section is triggered.

Test the incoming alert

1. Configure two organizations for IPAWS, Org A and Org B:
   a. Set up the IPAWS gateway and devices for IPAWS from the **Devices** section of the **Settings** page.
   b. Create a mass device endpoint for each COG for each device in **Settings** > **Mass Devices**.
   c. Create an operator account for each organization.
2. On Org B, update the IPAWS alert that notifies the operator Update the IPAWS alert template that notifies the operator:
   a. Create custom placeholders and update the out of the box IPAWS COG to COG Alert Template that targets the operator account.
   b. In the **Alert Template** section, modify the **Name** and **Description**, or keep the predefined values.

c. In the **Content** section, modify the **Title** and **Body**, or keep the predefined values.

3. Log in to Org A as an operator and create an alert for the Org B COG.
4. Target the IPAWS CAP Exchange mass device for IPAWS and publish the alert.
5. Verify that the alert triggers the alert template by having the Org B operator check for an alert with the associated end user.

Note: IPAWS incoming alerts do not appear in the Inbox. To see the alerts, you must trigger an alert to notify the operator.

Monitor system health

You can monitor and supervise the operational status of the following system components:

- BlackBerry AtHoc internal modules and processes
- Integrated systems and devices

This supervision and monitoring framework operates at system and Virtual System levels to provide the ability to do the following:

- Define scheduled monitors of different types to check various system operational conditions.
- Designate normal and abnormal operating conditions.
- Define what actions to take when state transitions take place including proactive notification to system administration and operation teams.
- Provide access to every monitor associated with the system and display on the Home page in the system.

The following system health monitor information can be edited:

- The name of the monitor.
- The threshold values for what constitutes a warning, an error, or a good test result.
- The state change criteria. The state of a monitor does not change with each returned test result, unless configured to do that. State is typically determined by a combination of returned test results over a specified number of results. For example, a state change occurs when a test result is returned 3 out of 5 times in the last 5 tests.
- Action the system performs and text that is displayed on BlackBerry AtHoc home page, when the state change criteria are met.

System health monitoring visibility is based on the following user roles:

- Enterprise administrators have access to the Global System Health option in the System Setup section.
- Organization administrators have access to the System Health option in the System Setup section.
- Operators can view the system health on the BlackBerry AtHoc home page.

Create an IPAWS health monitor

Two kinds of health monitors can be created to monitor IPAWS connectivity and other statuses:

- **IPAWS COG Health**: Checks the connectivity of IPAWS and the validity of COG accounts in the IPAWS system.
- **IPAWS Health Monitor**: Monitors the Unified Alerting Protocol (UAP) connectivity between the BlackBerry AtHoc server and the NDS application server.

To create these health monitors, complete the tasks in the following sections.

Create an IPAWS COG health monitor

1. Log in to the BlackBerry AtHoc management system as an administrator.

2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **System Health**.
4. In the **Organization Visibility Console**, in the **General** section, click **Create new monitor**.
5. Enter a name for the monitor, such as `IPAWS COG Health`.
6. From the **Is it associated with other Health Monitors?** list, select **General**.
7. Optionally, to show warnings and errors on the home page, select **Show errors and warnings for this monitor on the Home page**.
8. Specify how often and at what time you want the monitor to check the system status.
9. In the **How does this Monitor test the system** section, from the **Choose a test** list, select **AtHoc Event Logs**.
10. Copy the following sample configuration XML text into the **Test Configuration** field:

```
<EventLogTestConfig>
   <Filters>
     <Filter>
       <A>shortMessage</A>
       <B>IPAWS PING Error. COG: <COGID></B>
       <OffsetSeconds>0</OffsetSeconds>
       <Comparison>Contains</Comparison>
     </Filter>
     <Filter>
       <A>time</A>
       <B>[NOW]</B>
       <OffsetSeconds>-330</OffsetSeconds>
       <Comparison>GreaterThan</Comparison>
     </Filter>
   </Filters>
   <WarningConditions />
   <WarningCountThreshold>2</WarningCountThreshold>
   <ErrorConditions />
   <ErrorCountThreshold>1</ErrorCountThreshold>
</EventLogTestConfig>
```

11. Add the current organization COGID in the following line:

```
<B>IPAWS PING Error. COG: <COGID></B>
```

12. Configure the rest of the Health Monitor as appropriate. For more information about health monitors, see the *BlackBerry AtHoc System Administrator Configuration Guide*.
13. Click **Save**.

Create an IPAWS health monitor (UAP)

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **System Health**.
4. On the **Organization Visibility Console**, in the **General** section, click **Create new monitor**.
5. Enter a name for the monitor, such as `IPAWS Health Monitor`.
6. From the **Is it associated with other Health Monitors?** list, select **General**.
7. Optionally, to show warnings and errors on the home page, select **Show errors and warnings for this monitor on the Home page**.
8. Specify how often and at what time you want the monitor to check the system status.
9. In the **How does this Monitor test the system** section, from the **Choose a test** list, select **AtHoc Event Logs**.

10. Copy the following sample configuration XML text into the **Test Configuration** field:

```
<UAPHealthTestConfig>
   <ProtocolID>UAP-IPAWS</ProtocolID>
   <ProviderID>yourVPSID</ProviderID>
   <Devices>
       <Device>IPAWS</Device>
   </Devices>
</UAPHealthTestConfig>
```

11. Enter your organization ID for `yourVPSID` in the <Provider ID> attribute.
12. Configure the rest of the Health Monitor as appropriate. For more information, see the *BlackBerry AtHoc System Administrator Configuration Guide*.
13. Click **Save**.

View system status through BlackBerry AtHoc system health

Each time a health monitor system status test runs, the result is recorded. You can see the results as collected over time. System status is available for administrators with proper access privileges.

You can view monitors created through either of the System Setup sub-tabs Global System Health or Virtual System Health windows. However, you can edit a monitor only through the sub-tab where it was created.

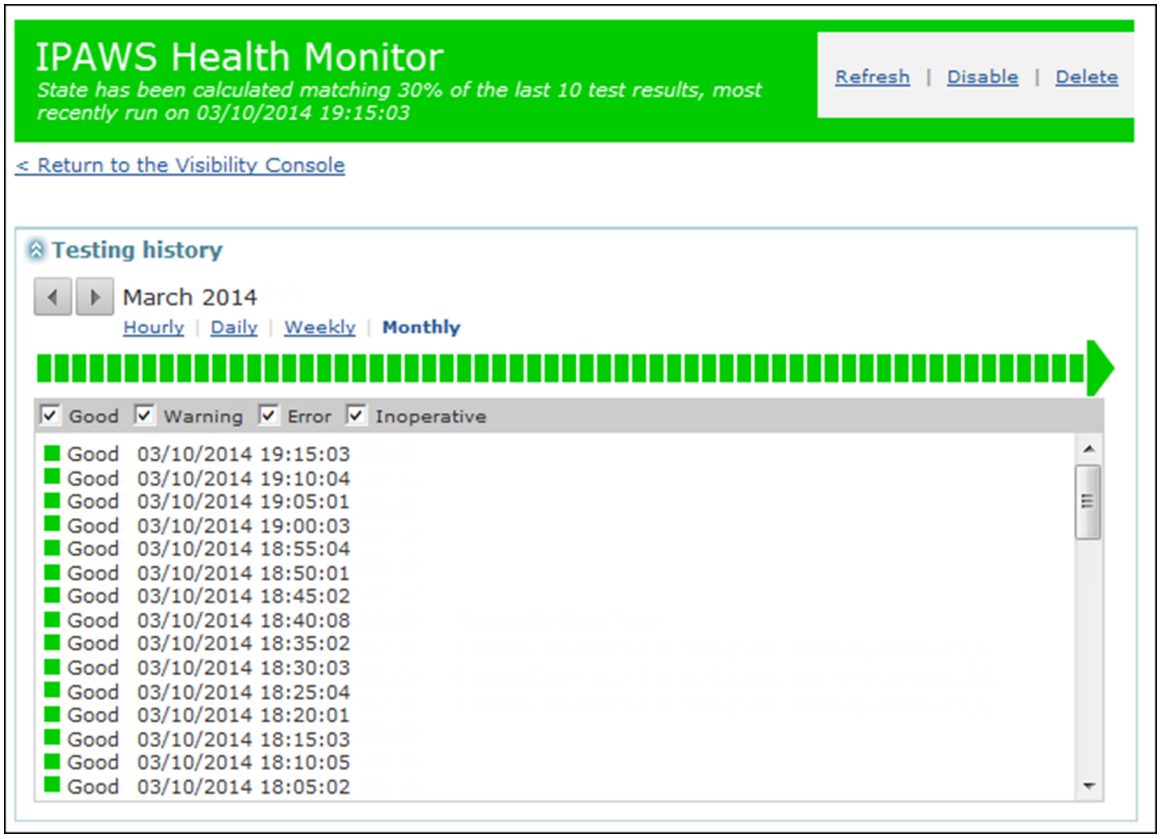
1. Log in to BlackBerry AtHoc management system as an enterprise administrator or system administrator.
2. In the navigation bar, click .
3. In the **System Setup** section, select the system health option that corresponds to your login access: **Global System Health** or **System Health**.

   The relevant visibility console opens, displaying monitors organized into the following categories: Errors & Warnings, Database, Web Applications, Services, Delivery Gateways, and General. The following table describes the different icons that appear on the screen.

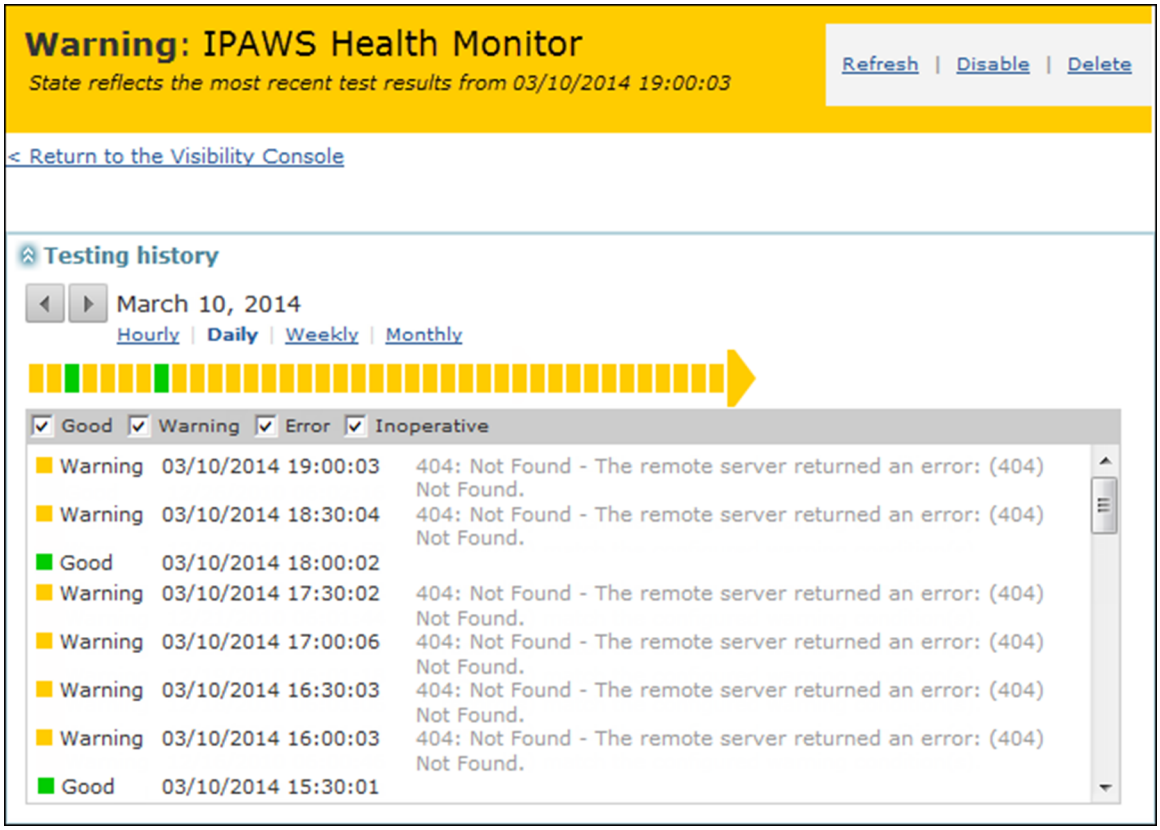
Icon	Description
	Error status. Indicates that the monitor test results meet the defined criteria for an error status.
	Warning status. Indicates that the monitor test results meet the defined criteria for a warning status.
	Good status. Indicates that the monitor test results meet the defined criteria for a good status.

4. Click the link to the monitor whose status you want to view.

   When all tests for a monitor return the same result, the overall status of the monitor is assigned that result status. In the following example, all tests have returned a Good status, so the overall monitor status is Good.



When a predetermined number of test cycles returns the same status, the status of the monitor changes. In the following example, even though two tests have returned a Good status, the overall monitor is in a Warning state.



BlackBerry AtHoc home page system status

On the Home page you can view the status of selected BlackBerry AtHoc system monitors. This is available to all system users: general operators, enterprise, and system administrators. The System Status area displays the status of system monitors that are configured to be visible from the Home page. Typically, the System Status area is used to display the status of critical functions that are required for system operations. This is not intended for day-to-day monitors.

The System Status area messages display the following items:

- Status icon
- Monitor group name
- Monitor name

See the **Global System Health** or **System Health** screen for an expanded view of the monitor status.

Upgrade the IPAWS plug-in

Complete the tasks in the following sections to upgrade IPAWS.

Copy the upgraded package to the NDS server

1. Log in to the NDS server.
2. Stop the BlackBerry AtHoc services:
   a. From **IIS**, select the application server. Click **Stop** on the **Actions** screen.
   b. Navigate to Windows Services and stop `AtHocDeliveryServices`.
3. Copy the IPAWS plug-in .zip file, `AtHoc.NDS.PlugIn.IPAWS_build.zip`, that you received from BlackBerry AtHoc support to a temporary folder.
4. On the file **Properties** screen, click the **General** tab.
5. Click **Unblock** and then extract the contents of the compressed file to a temporary directory.
6. In the temporary directory, rename the following folder:

   ```
   AtHoc.Delivery.Plugin.IPAWS_build
   ```

   to the folder name: `IPAWS`
7. Copy the `IPAWS` folder to the following location:

   ```
   <NDSServer>\Program Files (x86)\AtHocENS\DeliveryServer\Plugins\
   ```

   Where <NDSServer> is the name of the server where the NDS is installed.

Update the IPAWS plug-in on NDS

The plug-in key for IPAWS has been updated and you need to paste in the new configuration values.

Follow the steps in Install and configure the plug-in for NDS.

Update IPAWS settings in the BlackBerry AtHoc management system

1. On the BlackBerry AtHoc server, re-enable the device. See Configure IPAWS in the BlackBerry AtHoc management system.
2. From the BlackBerry AtHoc management system, configure the gateways.

   Note: Select the **Copy the default settings** check box.
3. From the BlackBerry AtHoc management system, configure or verify the IPAWS device settings for each device that you use:
   - Public Devices: IPAWS EAS, NWEM, WEA, and WEA 2.0.
   - COG to COG device: IPAWS CAP Exchange
4. **Upgrade to BlackBerry AtHoc 6.1.8.87 only:**
   a. Update the alert templates (formerly called scenarios) for each organization. See the *BlackBerry AtHoc Manage Alert Templates Guide* to learn about alert templates. The following parts of the template need to be updated:

- Add a geo-location for IPAWS public alerting devices (EAS, NWEM, WEA, and WEA 2.0.)These devices require a geo-location for activation.
- Update the target lists.

b. Replace the XML configuration content for each device:

1. In the **Devices** section, click **Devices**.
2. In the **Device Manager** section, select the device.
3. Click **Edit**.
4. In the **Delivery Gateway** section, for IPAWS click **Configure**.
5. Click **Remove** to delete the existing XML content.
6. From the **Add a Delivery Gateway** list, select **IPAWS** to get the new XML configuration content.
7. Click **Save**.

5. Send a Test Alert to Public Alerting Devices.

Appendix A: CAP Payload XML

The following figure shows the CAP payload XML, which is used to deliver COG-to-COG messages through incoming alerts in BlackBerry AtHoc. Nodes that have related custom placeholders appear in **bold** font.

```
<?xml version="1.0" encoding="utf-16"?>
  <alert xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance xmlns:xsd=
        "http://www.w3.org/2001/XMLSchema">
     <identifier
 xmlns="urn:oasis:names:tc:emergency:cap:1.2">10212152014020402562928 7
     </identifier>
     <sender xmlns="urn:oasis:names:tc:emergency:cap:1.2">AtHoc</sender>
     <sent xmlns="urn:oasis:names:tc:emergency:cap:1.2">
       2014-02-03T18:56:29-08:00</sent>
     <status xmlns="urn:oasis:names:tc:emergency:cap:1.2">Actual</status>
     <msgType xmlns="urn:oasis:names:tc:emergency:cap:1.2">Alert</msgType>
     <scope xmlns="urn:oasis:names:tc:emergency:cap:1.2">Public</scope>
     <addresses xmlns="urn:oasis:names:tc:emergency:cap:1.2">120113</addresses>
     <code xmlns="urn:oasis:names:tc:emergency:cap:1.2">IPAWSv1.0</code>
     <info xmlns="urn:oasis:names:tc:emergency:cap:1.2">
      <category>category</category>
      <event>event-type</event>
      <urgency>urgency</urgency>
      <severity>severity</severity>
      <certainty>certainty-level</certainty>
      <eventCode>
        <valueName>SAME</valueName>
        <value>LAE</value>
      </eventCode>
      <expires>expiration-date</expires>
      <headline>event-headline</headline>
    <description>content of the alert</description>
     </info>
     <Signature:Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
        xmlns:Signature="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
       <CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
         <SignatureMethod
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
         <Reference URI="">
            <Transforms>
          <Transform
           Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>digest-value</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>signature-value</SignatureValue>
      <KeyInfo>
      <X509Data>
         <X509SubjectName>CN=IPAWSOPEN_120009, OU=Devices, OU=FEMA, OU=Department
            of Homeland Security, O=U.S. Government, C=US</X509SubjectName>
         <X509Certificate>x509-certificate</X509Certificate>
      </X509Data>
    </KeyInfo>
     </Signature:Signature>
```

```
  </alert>
```

Glossary

CAP: The Common Alerting Protocol (CAP) is an XML-based data format for exchanging public warnings and emergencies between alerting technologies.

COG: A Collaborative Operating Group as defined by FEMA. A COG can have members from multiple organizations that act as a mutual aid organization. Examples of organizations include local, territorial, tribal, state, or federal governmental organizations of the United States.

COG ID: The six-digit identifier for a COG provided by FEMA.

EAS: Emergency Alerting Service as defined by FEMA.

FEMA: Federal Emergency Management Administration. FEMA created the IPAWS system to communicate and mobilize organizations during emergencies.

IPAWS: The Integrated Public Alert and Warning System developed by FEMA. This sytem provides a process for emergency communities to communicate with each other through alerts. Federal, State, territorial, tribal, and local alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol standards with the IPAWS infrastructure.

NWEM: Non-Weather Emergency Messages as defined by FEMA.

Peer COG: Any COG from which you receive alerts, or to which you send alerts.

Public Alert Device: One of the devices IPAWS uses to send alerts to the general public. BlackBerry AtHoc supports several public alert devices, including NWEM, EAS, WEA, and WEA 2.0.

Sender COG: The COG sending an alert to other organizations. Typically your own COG.

Target COG: The COG to which you are sending a message. Typically, another COG with whom you need to communicate about situations that affect both organizations.

UAP: Unified Alerting Protocol. Protocol to exchange data between the AtHoc server and the NDS application server.

WEA: Wireless Emergency Alerts as defined by FEMA. Formerly known as Commercial Mobile Alert System (CMAS).

BlackBerry AtHoc Customer Support Portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Support Portal:

https://support.athoc.com/customer-support-portal.html

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user guides.

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada