BlackBerry AtHoc

Monaco Warning System Installation and Configuration Guide

Last Published: March 2019

Contents

Getting started

The BlackBerry AtHoc management system uses the IIM add-on module interface with Giant Voice (GV) outdoor warning devices to enable wide-area Mass Notification System (MNS) broadcasts. Giant Voice features can broadcast critical information using voice messages, wave files, musical tones, or text-to-speech (TTS) conversion. Monaco Warning System supports outdoor Public Address (PA) systems that have large amplified speakers. Typically, speakers are set on poles in an array that covers a specified area with enough acoustic sound to override the ambient noise with emergency notification.

After the BlackBerry AtHoc management system is integrated with a Monaco Warning System, operators can disseminate emergency alerts to the siren system from the BlackBerry AtHoc management console. Alert messages can be delivered using Key functions programmed in the Monaco Warning System hardware or software or text-to-speech files to dynamically selected targets. Targeting choices are All Poles simultaneously, individual Zones of poles, and Poles.

Configure the Monaco warning system delivery gateway

Configure the Monaco Warning System gateway in the Settings section of the BlackBerry AtHoc management system to enable the BlackBerry AtHoc alerts system to publish alerts through Monaco Warning System.

Enable the Monaco Warning System gateway on the BlackBerry AtHoc application server

Log in to the BlackBerry AtHoc management console and check the Delivery Gateways section to verify that the Monaco Warning System and XML Feed device gateways have been installed. If they are installed, skip this section.

You must enable both the Monaco Warning System and XML Feed device gateways on the BlackBerry AtHoc management system.

1. Log in to the BlackBerry AtHoc application server as an administrator.
2. Navigate to the following folder `<IWSAlerts Install Path>\ServerObjects\Tools` and run the `AtHoc.Applications.Tools.InstallPackage.exe` file.
3. On the **Configure Device Support** screen, select **Monaco Warning System** and **XML Feed**.
4. Click **Enable**.
5. On the **Installation Complete** pop-up window, click **OK**.
6. Click **Close**.

Configure the delivery gateway

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Devices** section, select **Monaco Warning System**.
4. Click **Copy default settings**.
5. Click **Save**.
6. In the navigation bar, click the .
7. In the **Devices** section, select **Xml Feed**.
8. Click **Copy default settings**.
9. In the **Feed Source** section, select **Delivery Gateway ID**.
10. Click **Save**.

Configure the devices

Complete the following steps to configure the Monaco Warning System and XML Feed devices.

Configure the Monaco Warning System device

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. On the **Device Manager** screen, click **Monaco Warning System**.

5. On the **Monaco Warning System** page, click **Edit**.
6. In the **Help Text** section, in the **Targeting Help Text** field, enter the following text:

   "You are publishing to Monaco Giant Voice. Please make sure the endpoints selection is in compliance with vendor specifications."
7. In the **Delivery Gateway** section, click **Add a Delivery Gateway** and select **Monaco Warning System**.
8. Click **Configure** to open the text-entry field for the Monaco Warning System device.
9. By default, the configuration value appears in the text-entry field. If the text-entry field is empty, complete the following steps:

   a. Click **Remove**.
   b. Select **Monaco Warning System** from the list.
   c. Click **Configure**.
   d. Copy the following text into the field:

```
<Configuration>
    <CapParams>
        <GVSystemType>MONACO</GVSystemType>
        <AllMode>0</AllMode>
        <ZoneMode>1</ZoneMode>
        <PoleMode>1</PoleMode>
        <KeyMode>1</KeyMode>
        <UnusedMode>0</UnusedMode>
        <DefaultAllCall>0</DefaultAllCall>
        <DefaultKeyActivationCode>0</DefaultKeyActivationCode>
        <NoPARequired>0</NoPARequired>
        <PARequired>1</PARequired>
        <IsCancelable>false</IsCancelable>
        <ContentSource>MONACO-WARNING-SYSTEM</ContentSource>
    </CapParams>
</Configuration>
```

10. Click **Save**.
11. Click **Enable**.

Configure the XML Feed device

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. On the **Device Manager** screen, click **Xml Feed**.
5. On the **Xml Feed** page, click **Edit**.
6. In the **Delivery Gateway** section, click **Add a Delivery Gateway** and select **Xml Feed**.
7. Click **Configure** to open the text-entry field for the XML Feed device.
8. By default, the configuration value appears in the text-entry field. If the text-entry field is empty, complete the following steps:

   a. Click **Remove**.
   b. Select **XML Feed**.
   c. Click **Configure**.
   d. Copy and paste the following text into the field:

```
<Configuration>
    <DeviceType>FEED</DeviceType>
</Configuration>
```

9. Click **Save**.

The XML Feed must be configured but does not need to be enabled to use the Monaco Giant Voice device.

Set up mass device endpoints (targets)

To create a speaker pole, zone, or an all-poles user, an operator should perform the normal Mass Device Endpoint creation flow. You should give the endpoint a functionally descriptive name, so that it is recognizable in End User Manager and Report windows as a mass-communication device target entity.

Note: An operator must target either a single GV Group (Zone) or multiple GV Towers (Poles) in the alert. Otherwise, the publishing to Monaco can fail and you may get some unexpected errors.

Create mass device zone and pole endpoints

1. Log in to BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Mass Devices Endpoints**.
4. Click **New**.
5. From the list of options, select **Monaco Warning System**.
6. In the **Display Name** field, enter a name.
7. To create a new endpoint for a pole, complete the following steps:
   a. In the **Configuration** section, for **Giant Voice type**, select **Pole**.
   b. In the **Address** field, enter **P,J1**.
8. To create a new endpoint for a zone, complete the following steps:
   a. In the **Configuration** section, for **Giant Voice type**, select **Zone**.
   b. In the **Address** field, enter **Z,1**.
9. Click **Save**.

Create a mass device key endpoint

To create the object that displays the list of keys associated with Monaco D-21, complete the following tasks:

- Create the ATHOC-GV-KEYS attribute XML configuration.
- Perform the normal Mass Device Endpoint creation flow.

Configure the Key XML attribute

Note: The key name and description parameters cannot contain spaces or any of the following characters: `' ! $ % ^ ( ) = { } , ; : ? " < > |`

The following is the Key XML configuration:

```
<giantVoiceSetting>
<messages>
    <message id = "MSG-TARGETING-NOT-ALLOWED">The Giant Voice Key you have
 selected on the previous page does not allow
additional selection of Giant Voice poles or zones.  You may still target users
 for other devices, but Giant Voice targeting
will be ignored.</message>
    <message id = "MSG-TARGETING-ALLOWED">The Giant Voice Key you have selected on
 the previous page already has Giant
```

```
Voice poles and zones targeted, but you can override them by targeting different
 zones in the Targeting area just below.</message>
    <message id = "MSG-TARGETING-REQUIRED">The Giant Voice Key you have selected
 on the previous page does not have any
targeting information built-in, and will require you to target at least one Giant
 Voice pole or zone below.</message>
</messages>
<keys>
    <key
            id = "1"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 1</name>
            <description>Message 1</description>
    </key>
    <key
            id = "2"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 2</name>
            <description>Message 2</description>
    </key>
    <key
            id = "3"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 3</name>
            <description>Message 3</description>
    </key>
    <key
            id = "4"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 4</name>
            <description>Message 4</description>
    </key>
    <key
            id = "5"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 5</name>
            <description>Message 5</description>
    </key>
    <key
            id = "6"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 6</name>
            <description>Message 6</description>
    </key>
    <key
            id = "7"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Message 7</name>
            <description>Message 7</description>
    </key>
    <key
            id = "8"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
```

```
            <name>Message 8</name>
            <description>Message 8</description>
            </key>
    <key
            id = "18"
            messageIdRef = "MSG-TARGETING-REQUIRED"
            targetingRule = "TargetingRequired">
            <name>Biological Agent</name>
            <description>Biological Agent</description>
    </key>
</keys>
</giantVoiceSetting>
```

Create a key mass device endpoint

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Mass Device Endpoints**.
4. Click **New**.
5. From the list of options, select **Monaco Warning System** from the list.
6. In the **General** section, enter a name in the **Endpoint Name** field.
7. In the **Configuration** section, for **Giant Voice Type**, select **Key**. The Address field auto populates **K**.
8. Copy the Key XML configuration into the **Giant Voice Key** field.
9. Click **Save**.

Create and publish a Monaco warning system alert template

Prerequisites

- Before you start sending test alerts through the Monaco warning system, consider the impact it has on everyone within hearing distance of the poles you are using during the test.
- This process assumes that the IIM is not configured to download data from the BlackBerry AtHoc management server and is not connected to the Giant Voice equipment.
- Consult with your POC about the acceptable content of the test alert. For example, the word "test" should appear at, or very near to, the start of the broadcast message.
- Although the initial use of this template is to test the data creation process, this template can be used during the audio tuning phase after the IIM and Giant Voice hardware are connected.

To confirm that the Monaco Giant Voice device is installed correctly on the BlackBerry AtHoc management system, create a template.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click **Alerts** > **Alert Templates**.
3. Click **New**.
4. On the **New Template** screen, in the **Alert Template** section, enter a template name and description.
5. Select a folder from the **Folder** list.
6. Select **Available for quick publish**.
7. In the **Content** section, enter the title and content of the alert.
8. In the **Mass Devices** section, select **Monaco Warning System** and then from the list, select one or more mass alert endpoints.
9. In the **Mass Device** section, click **Options**.
10. On the **Mass Devices Options** screen, select **Text to Speech** and then **Alert Body** or **Custom Text**.

11. Click **Apply**.
12. In the **Schedule** section, change the **Alert Duration** to 15 minutes.
13. Click **Save**.
14. Click .
15. On the **Home** page, in the **Quick Publish** section, find the alert template you just created.
16. Click **Review and Publish**.
17. Review the Warning on Review and Publish page.

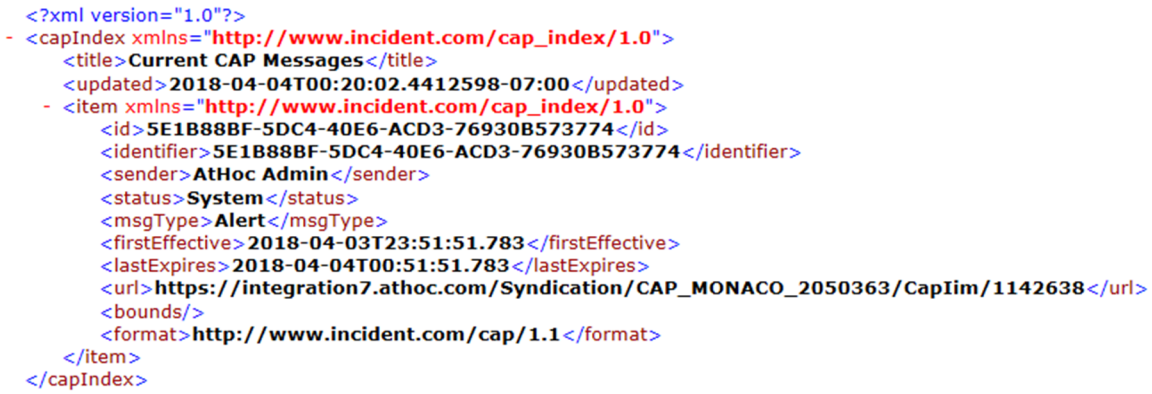
    For detailed steps about how to add the help text to the alert template, see Configure the Monaco Warning System device.
18. Click **Publish**.

Verify the published alert

To verify that the alert was published successfully to the syndication feed, complete the following steps:

1. Open a browser and navigate to the following URL: `https://<url>/syndication/cap_monaco_<vpis-id>/capindex`.

   Where <url> is the base URL of the BlackBerry AtHoc management system and <vps-id> is the 7 or 8-digit organization ID.
2. Copy the content in the <url> field into another browser. The “capIndex” XML format must be similar to the content in the following image:



3. Verify the <addresses> and <code> and match with the following format. The “alert” XML format must be similar to the content in the following image:

```
<?xml version="1.0"?>
- <alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
    <identifier>CAP_MONACO|535862|5E1B88BF-5DC4-40E6-ACD3-76930B573774|1142638|PUBLISH</identifier>
    <sender>IWSAlerts</sender>
    <sent>2018-04-03T23:51:51-07:00</sent>
    <status>Actual</status>
    <msgType>Alert</msgType>
    <source>System Default</source>
    <scope>Public</scope>
    <addresses>MONACO,1,11</addresses>
    <code>0,1</code>
  - <info>
      <category>Other</category>
      <event/>
      <urgency>Unknown</urgency>
      <severity>Unknown</severity>
      <certainty>Unknown</certainty>
    - <eventCode>
        <valueName>ATHOC</valueName>
        <value>IWSA</value>
      </eventCode>
      <effective>2018-04-03T23:51:51-07:00</effective>
      <expires>2018-04-04T00:51:51-07:00</expires>
      <senderName>MassDev</senderName>
      <headline>Monaco Zone TTS</headline>
      <description>Monaco Zone TTS. Please ignore</description>
      <instruction/>
      <contact>support@athoc.com</contact>
    </info>
</alert>
```

4. If any of the formatting does not match, review the Monaco Warning System gateway XML content and mass communication users' Monaco Warning System device addressing. Errors in these sections are the most common reason for malformed Alert XML fields.

Configure IIM IP connectivity

This section describes how to configure the IP Integration Module (IIM) to communicate with the BlackBerry AtHoc Monaco Warning System device.

Prerequisite

Ensure that the following packages are installed and configured before performing any tasks:

- Latest Monaco Warning System package
- Latest Capnode package

To work as part of the BlackBerry AtHoc system, IIM must be able to communicate with the BlackBerry AtHoc server to download the CAP packets.

The initial configuration data you need to collect are:

- The BlackBerry AtHoc Alerts system base URL
- The BlackBerry AtHoc Alerts organization ID
- Customer's proxy server and port information

To find this information, use a local PC to log in to your local instance of the BlackBerry AtHoc management console. The URL can be a base "https" address used to access a specific system.

You can obtain the URL of the system from the local system administrator or from the BlackBerry AtHoc Customer Support team. Launch the management console. The URL from the "https" to the last character before the third forward slash (/) is the "base URL" of the system. For example, in the following URL address bar, the full URL for the sign-on page is: "https://integration7.athoc.com/client/auth/login?ReturnUrl=%2fclient%2fathoc-iws". The "base-URL" of the system is "https://integration7.athoc.com".

The organization ID is a 7 or 8-digit numerical identifier of the specific system of that customer. To obtain this organization ID, log in to the BlackBerry AtHoc management system for the customer. Once logged in, you can find the system's organization ID at the top right of the Home Page of the system.

Navigate to the settings page of the browser and determine if you are using any type of Proxy server for routing internet traffic. For example, if the browser you are using is Microsoft Internet Explorer (IE), go to the LAN settings, in IE, select **Tools** > **Internet Options**. On the **Internet Options** screen, click the **Connections** tab. At the bottom of the window, click **LAN settings**.

In the **Proxy Server** section, click **Advanced**. The **Proxy Settings** screen displays the Proxy Server Address.

Record the proxy server address and the port number. You can now close these settings windows and exit IE.

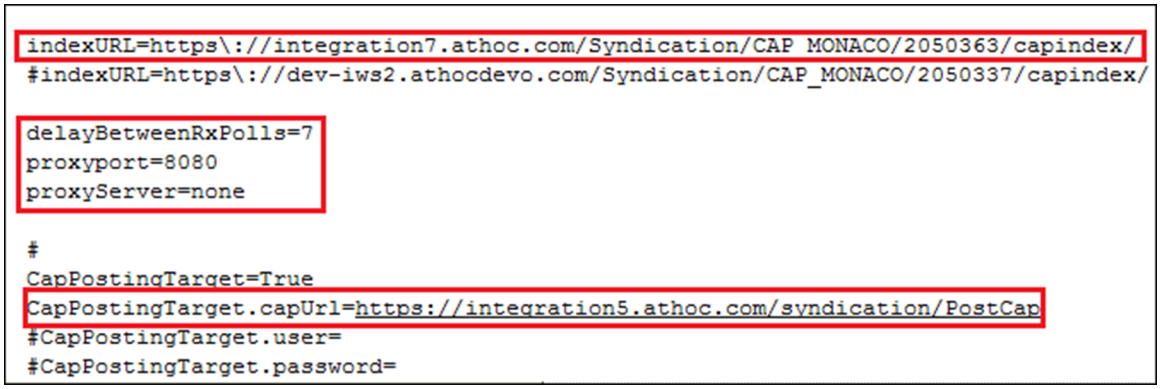
Note: It is also possible that your IE instance may not use proxy servers. If this is the case, when you click the LAN settings button, no proxy server is used for internet traffic on this network.

Configure the IIM and property files

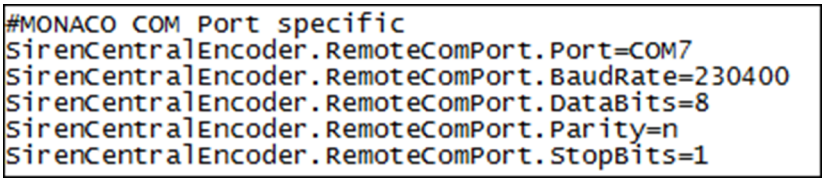
1. Open Microsoft Notepad as an administrator.
2. Click **File** > **Open**.
3. Navigate to `C:\Program Files\capnode` and change the file selection from "Text Documents (*.txt)" to "All Files (*.*)".
4. Select the `system_private.config` file.
5. Click **Open**.
6. Verify the following items in the system_private.config file:

a. The `indexURL` variable should be formatted similar to the following image. The base URL should be followed by “/syndication/”, then the device gateway protocol ID (for example, CAP_MONACO for Monaco Warning System), the Organization ID number, followed by "/capindex".
b. The “#” at the beginning of a line in the `system_private.config` file is used to comment out an unused line. The “#” should be removed from a line to use the variable.

7. Enter the proxy server and proxy port information you collected earlier in the proxyserver and proxyport parameters. If the settings on the machine that you tested with is set for “Automatic” in the proxy settings, the settings for those two lines displays as follows:
   - proxyServer=none
   - proxyPort=8080
8. Update the CapPostingTarget variables to reflect the correct URL using the same base URL as in the `indexURL` variable.



9. The Monaco Warning System COM Port settings displayed in the following images are default values and should not be changed.



10. Click **File** > **Save**. Close the `system_private.config` file.
11. Restart the CapCon service .

Restart the CapCon service

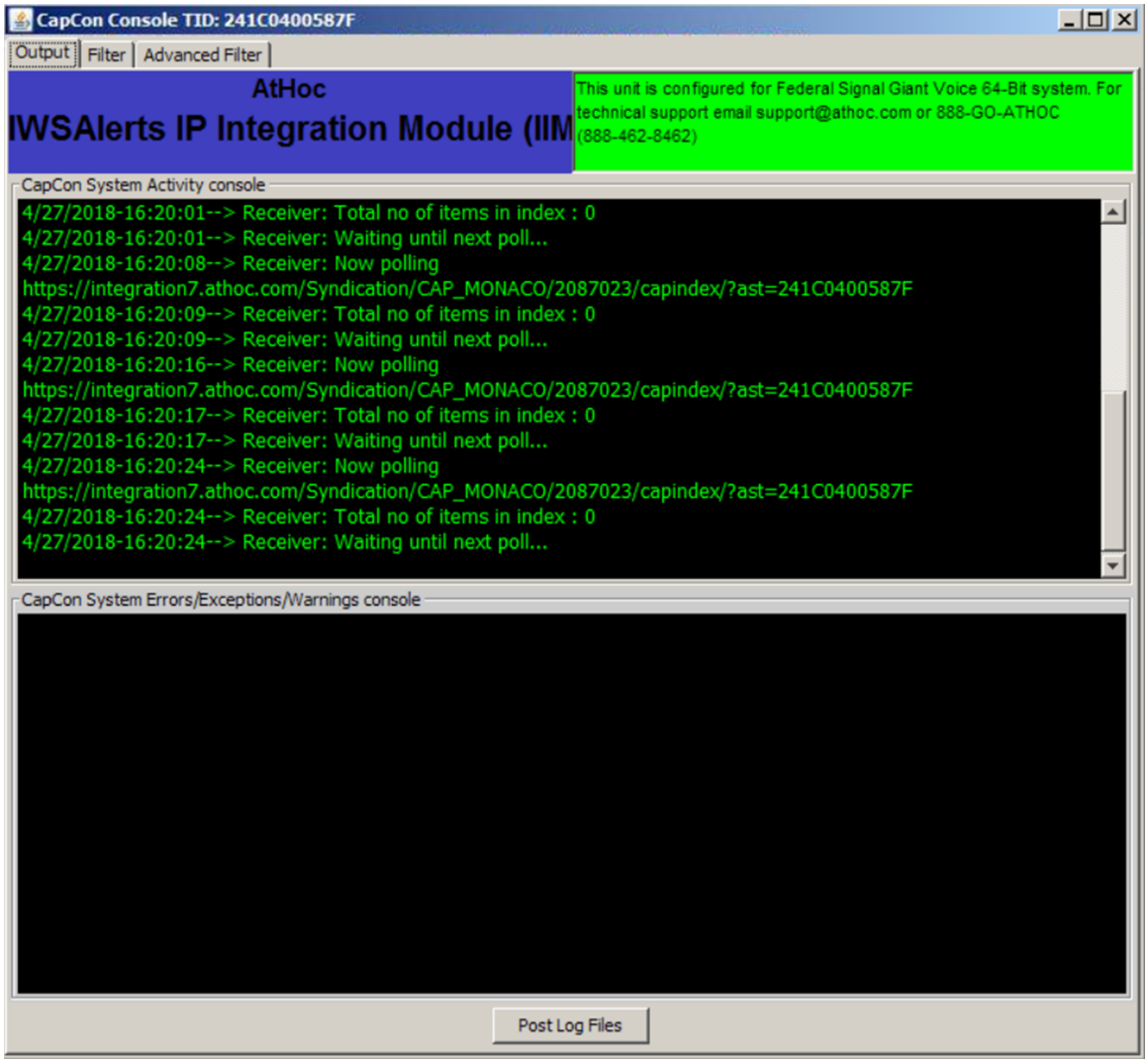
After you configure the CapCon service, you must restart it.

1. Navigate to your IIM system.
2. Go to **Start** > **Run** > **Services**.
3. Launch an instance of the Services Manager application. There should be a quick-launch icon in the taskbar of the desktop.
4. Scroll down to **IIM CapCon Service**.
5. Right-click the CapCon Services row and select **Restart** or **Stop**.
6. Right-click the CapCon Services row and select **Start**.

Verify the CapCon system activity console (GUI)

1. Log in to the IIM console as an administrator. The CapCon Console loads automatically.

   The data in the CapCon System Activity console polls at the rate set by the `delayBetweenRXpolls` variable in the `system_private.config` file. The default is set to 7 seconds. A message indicates the total number of items in the index. The index number is the number of active alerts on the BlackBerry AtHoc system at that time.
2. Verify that the IIM console does not show any new errors.



3. Verify that the console icon in the task tray appears green, indicating that the connectivity between the IIM and the BlackBerry AtHoc Alerts system is good.

Troubleshooting

If the CapCon System Activity console indicates anything other than a total number of items in the index and a number, or if the CapCon System Errors/Exceptions/Warnings console has content in red, this indicates that the configuration has not been executed correctly.

1. If the BlackBerry AtHoc management system, for example, https://integration7.athoc.com/athoc-iws is available on Microsoft Internet Explorer on a local workstation, then the indexURL should also be available. Enter the indexURL in the browser. For example, https://integration7.athoc.com/syndication/cap_Monaco_2050363/capindex.

   If there are no items in the syndication feed, an XML similar to the following image should be displayed:

2. If connectivity is still not good, try commenting out the `proxyServer` and `proxyPort` variables.
3. If an HTTP or HTTPS error is displayed instead of XML, this may indicate a firewall or certificate issue or a configuration problem with the BlackBerry AtHoc server syndication folder or subfolders.
4. Check the indexURL and proxy settings in the `system_private.config` file for any misspellings. If any line have been misspelled, repeat the configuration steps.
5. Check the `capnodelog` file for errors. Open Windows Explorer by right-clicking on the IIM Start button and navigate to `C:/Program Files/capnode/capnodelogs` and open the `capnode.log` file with Notepad. Browse the file to find the time that the indexURL was changed and the CapCon service restarted.
6. Contact BlackBerry AtHoc technical support. Be prepared to provide the `system_private.config` and `capnode.log` files and screen shots of the console screen and the BlackBerry AtHoc management console pages.

Migrate to SDK

Note: The SDK user should have the correct username and password for this specific organization on the AtHoc server. If this organization has no SDK user, create one and continue with configuration system file on Monaco IIM.

1. Download the capnode build from:

```
https://repo.athoc.com/artifactory/webapp/#/artifacts/
browse/tree/General/IIM/Integrations/Monaco/Builds/366/capnode.zip
```

2. Rename the existing folder in IIM to `capnode_back`.
3. Create new Capnode folder in `C:/Program Files` folder.
4. Extract the Capnode folder from the `capnode.zip` file to `C:/Program Files/capnode` of IIM.
5. Change the values in the `system.config` file as required for the following parameters:

```
#SDK Alert Related Parameters :
#This declares the  Alert Mechanism must be SDK
AlertPostingMechanism=SDK
#This declare weather the SDK URL is mentioned or not
SDKPostingTarget=true
#Alert posting URL
SDKAlertPosting.Url=https://integration5.athoc.com/sdk/listener/listen.asp
#Organisation Id
SDKAlertPosting.VPS_ID=2076902
#Username of the server
SDKAlertPosting.Username=iwsusername
#Checks if the password is encrypted or not
SDKAlertPosting.IsPasswordEncrypted=no
#The password of the server
SDKAlertPosting.Password=iwspassword

encoder.SirenCentralDriverMonaco.DelayBeforeAudio = 1000
```

6. The Alert is sent to the user whose email ID is configured to that organization code.
7. Open services and run the CapCon service.
8. Check Monaco IIM after restarting capnode with HB stabilization. Every 30 seconds a new HB may be found in CapAlertsResivedFromMonaco and CapSentToMonaco.

Set up inbound alert activation

The Monaco D-21 uses XML CAP payload to activate BlackBerry AtHoc alerts. The IIM receives the message, verify its transmission envelope, and relays to BlackBerry AtHoc alerts, which validates the payload, executes the request, and responds appropriately. All BlackBerry AtHoc alerts activation use templates identified by their common names. The template can be modified at the activation level based on the CAP XML and the `DynamicTextMode` parameter.

```
/alert/info/eventCode/valueName/SCENARIO
/alert/info/eventCode/value/[name of scenario]
```

The node <eventCode> shall have the <valueName> element template, and <value> node shall contain the template name. Templates are identified by unique names of up to 128 characters.

The node <headline> can be used to override the template header and includes 3 to 200 characters.

The nodes <description> and <instruction> can be used to override the template body, and includes 0 to 2000 characters.

```
/alert/
identifier    unique identifier generated by Monaco D-21
sender        Sender identity, from Monaco D-21
sent        Date & time of message origination
status        “Actual” / “Exercise”
msgType    “Alert”
scope        “Private” / “Public”
addresses    (optional) Receiver identity
info/        (required for Alert” msgType)
    category     “Other”
    event         The alert message header / title; informational
    urgency         “Unknown”
    severity     “Unknown”
    certainty    “Unknown”
    eventCode/
          valueName    “TEMPLATE”
          value        Scenario common name – CASE SENSITIVE
    expires         optional time to and the delivery
    headline     optional message title
    description     optional message pre-body
    instruction     optional message post-body
    parameter     optional code to indicate use of optional text
```

Note: GUIDs are generated and used as “identifier” values. If expired, the timestamp specifies that is the time to end playing the delivery of the audio / visual alert.

The parameter `DynamicTextMode` is located in the `CAP XML /alert/info/parameter` with valueName of `DynamicTextMode`. The values allowed in the value field are None, Replace, and Append.

If the `DynamicTextMode` parameter is blank, missing, or invalid the template is treated as if in None mode. If the headline, description, and instruction CAP XML fields are blank or missing, the template is treated as if in None mode.

None

The CAP XML contains a single template to execute. This is default mode of implementation.

- The Header is predefined by the template.
- The Body is predefined by the template.

Example XML:

```
<eventCode>
        <valueName>SCENARIO</valueName>
        <value>MONACO_ALERT</value>
    </eventCode>
    <headline></headline>
    <description></description>
    <instruction></instruction>
    <parameter>
        <valueName>Value</valueName>
        <value>ON</value>
    </parameter>
```

Note: Headline, description, and instruction fields are all ignored.

Replace

The CAP XML contains the template to execute and text for topic and body of the template. This mode is identified by a new `/alert/info/parameter` with valueName of `DynamicTextMode` and a value of `Replace`

- The Header is populated by the CAP XML field /alert/info/headline.
- The Body is populated by the CAP XML fields /alert/info/description and /alert/info/instruction. The two fields are concatenated with a single space between the two fields. For example, description + “ ” + instruction.

Example XML:

```
<eventCode>
        <valueName>SCENARIO</valueName>
        <value>MONACO_ALERT</value>
    </eventCode>
    <headline>Chemical Spill</headline>
    <description>1 Contaminated waste leaking from tanker in sector 4.</
description>
    <instruction>2 Please evacuate sector 4 in a orthwestdirection.</instruction>
    <parameter>
        <valueName>Value</valueName>
        <value>ON</value>
        <valueName>DynamicTextMode</valueName>
        <value>Replace</value>
    </parameter>
```

Example:

Header: Chemical Spill

Body:

1. Contaminated waste leaking from tanker in sector 4.
2. Please evacuate sector 4 in a northwest direction.

Append

The CAP XML contains the template to execute and additional text for the body of the template. This mode is identified by a new `/alert/info/parameter` with valueName of `DynamicTextMode` and a value of `Append`.

- The Header is predefined by the template.
- The Body is modified by appending the CAP XML fields /alert/info/description and /alert/info/instruction.

Let template_body be the current text body predefined in the template.

The fields description, template_body, and instruction are concatenated with a single space between the fields. For example, description + " " + scenario_body + " " + instruction.

Example XML:

```
<eventCode>
  <valueName>SCENARIO</valueName>
  <value>MONACO_ALERT</value>
 </eventCode>
 <headline></headline>
 <description>1 Hazardous chlorine gas leak.</description>
 <instruction>2 vacuate the area in a southeast direction.</instruction>
 <parameter><
  valueName>Value</valueName>
  <value>ON</value>
  <valueName>DynamicTextMode</valueName>
  <value>Append</value>
 </parameter>
```

Example:

Let template_body = "Hazmat alert. Please follow protocol for hazardous material."

Header: <pre-defined AtHoc Template Topic>

Body:

1. Hazardous chlorine gas leak. Hazmat alert. Please follow protocol for hazardous material.
2. Evacuate the area in a southeast direction.

Alert activation response

The BlackBerry AtHoc system parses the payload and responds to the message activation. Generally, parse / payload errors such as missing mandatory nodes or parameters, results with Error. Otherwise, if the payload is OK, the response is "Ack" and the response <note> node indicates the success, failure, or issues with the activation. Such failures can include unknown template identifier, unknown or incorrect addresses.

Note: Partial activations are encouraged. For example, if some node or zone addresses are unknown, activation can still take place.

In case of a payload error, BlackBerry AtHoc responds with the following information:

```
/alert/
    identifier    unique identifier generated by AtHoc
    sender        Sender identity, from Monaco D-21
    sent        Date & time of message origination
    status        "System"
    msgType     "Error"
```

```
    scope        “Private” / “Public”
    note        Text describing the error
    references    the original message “sender,identifier,sent”
```

When the payload is valid, BlackBerry AtHoc completes the activation, and, if successful, responds with the following information:

```
/alert/
    identifier    unique identifier generated by AtHoc
    sender        Sender identity, from AtHoc
    sent        Date & time of message origination
    status        “System”
    msgType            “Ack”
    scope        “Private” / “Public”
    note        Activation related informative text (if any)
    references    the original message “sender,identifier,sent”
```

If the activation failed, BlackBerry AtHoc responds with the following information:

```
/alert/
    identifier    unique identifier generated by AtHoc
    sender        Sender identity, from AtHoc
    sent        Date & time of message origination
    status        “System”
    msgType            “Error”
    scope        “Private” / “Public”
    note        Text describing activation errors
    references    the original message “sender,identifier,sent”
```

Alert end or cancel

The Cancellation message is optional. BlackBerry AtHoc supports cancellation for live messages.

The Monaco D-21 issues the following payload for an ended or canceled alert:

```
/alert/
identifier    unique identifier generated by Monaco D-21
sender        sender identity, from Monaco D-21
sent        Date & time of message origination
status        “System”
msgType    “Cancel”
scope        “Private” / “Public”
references    the original message “sender,identifier,sent”
```

BlackBerry AtHoc ends an alert if still live, and responds with the following payload if OK:

```
/alert/
identifier    unique identifier generated by AtHoc
sender        Sender identity, from AtHoc
sent        Date & time of message origination
status        “System”
msgType    “Ack”
scope        “Private” / “Public”
references    the original message “sender,identifier,sent”
```

BlackBerry AtHoc ends an alert if still live, and responds in case of a cancel error:

```
/alert/
identifier    unique identifier generated by AtHoc
sender        Sender identity, from AtHoc
sent        Date & time of message origination
status        “System”
msgType    “Error”
scope         “Private” / “Public”
note        Text describing the error
references    the original message “sender,identifier,sent”
```

Publish and verify a pre-test alert template

Prerequisite

- Before you start sending test alerts through Monaco warning system, consider the impact on everyone within hearing distance of the poles you are using during the test.
- Consult with your POC about the acceptable content, user targeting, and device selection of the pre-test notification.

To create a template that targets end users using the Desktop Popup, email, and messages to other devices to inform them of a Giant Voice System test, complete the following steps:

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click **Alerts** > **Alert Templates**.
3. Click **New**.
4. On the **New Template** screen, in the **Alert Template** section, enter a template name and description.
5. Select a folder from the **Folder** list. Select **Test** if available.
6. Select **Available for quick publish** and **Available for mobile publishing**.
7. Select **Informational** from the **Severity** list.
8. Select **Other** from the **Type** list.
9. In the **Content** section, enter an alert title. The alert title can be the same as the template name.
10. In the **Alert Body** field, enter the text to be read by the text-to-speech. The body should contain the details of the testing with information such as the time testing will start and finish and any actions that should be taken as a result.
11. In the **Target Users** section, select the appropriate targeting group, individual users, or query to send the pre-test notification to.
12. Click **Select Personal Devices** and then select **Desktop App** and **Email-Personal**.
13. In the **Personal Devices** section, click **Options**.
14. In the **Personal Device Options** screen, select **App Template** and **App Audio**.
15. Click **Apply**.
16. In the **Schedule** section, change the **Alert Duration** to the expected duration of the testing.
17. Click **Save**.
18. Click  to return to the Home page.
19. In the **Quick Publish** section, find the Giant Voice System Test Notification template and click **Review and Publish**.
20. Review the settings and selections.
21. Click **Publish**.
22. To verify that the alert was published correctly, observe the receipt of Desktop Popup or email messages on the POC workstation.

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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada