BlackBerry AtHoc

IPAWS Alerts User Guide

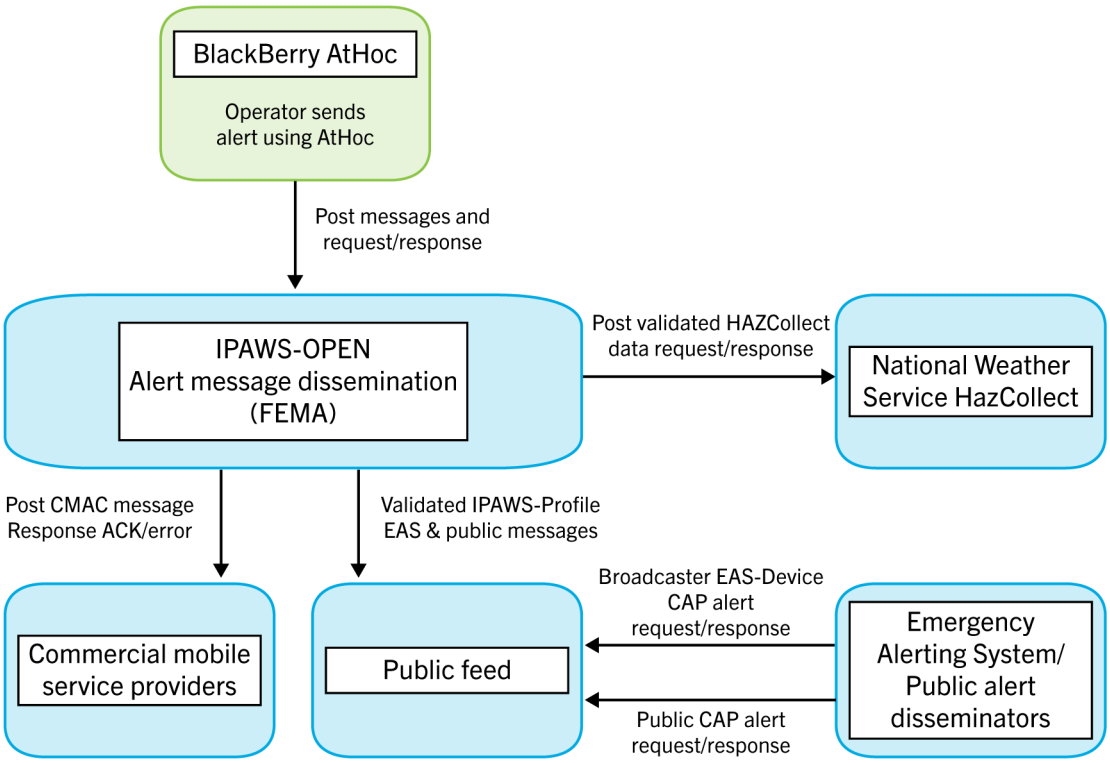
Contents

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.

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 (EAS), and Wireless Emergency Alerts (WEA).

Using the AtHoc Notification 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.

Send and Receive IPAWS Alerts

From BlackBerry AtHoc, you can send and receive alerts to and from other COGs with IPAWS CAP exchange. You can also send public alerts using IPAWS public services, such as EAS, NWEM, WEA and WEA 3.0. The following sections describe how to publish and manage IPAWS alerts.

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. In 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, do one of the following:
      - Select **Use Text from Alert Title of Alert** to use the content that you specified in the **Content** section.
      - 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.
8. Click **Apply**.
9. Click **Review and Publish** to review the alert.
10. On the **Review and Publish** screen, click **Publish**.

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 3.0.

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, 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 beside the selected devices.
8. In the **Mass Devices** section, click **Options**.
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 IPAWS WEA 3.0, 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: IPAWS WEA 3.0 has a text limit of 360 characters for each custom text entry. You can also specify a 90-character custom text entry for users whose devices or carriers support only WEA.
10. Click **Apply**.
11. Click **Review and Publish** to review the alert.
12. On the **Review and Publish** screen, click **Publish**.

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.

Duplicate an alert

In some situations, you might want to create an alert based on another alert displayed in the Alert Manager.

1. Log in to the BlackBerry AtHoc management system with an administrator account.
2. From the navigation bar, click **Alerts** > **Sent Alerts**.
3. Select an alert in the **Sent Alerts** list.
4. Click **Duplicate**. The Alert Publisher displays a copy of the selected alert.
5. Edit the new alert and publish when you are ready. The default duration of a duplicate alert is four hours.

Note: The new alert has the same header as the original, but has the word "copy" at the end. You should change the alert title.

End a live alert

You can end the delivery of a live alert and place it in an Ended state.

When ending an alert, note that some users might have already received and viewed the alert, depending on the amount of time that elapsed between publishing and ending the alert, and how quickly the system can deliver alerts.

1. Log in to the BlackBerry AtHoc management system with an administrator account.
2. From the navigation bar, click **Alerts** > **Sent Alerts**.
3. From the list, select one or more live alerts.
4. Click **More Actions** > **End**.
5. On the **End Alert** window, click **OK**.

Delete an alert

You can delete alerts that are in a Standby or Scheduled status.

1. Log in to the BlackBerry AtHoc management system with an administrator account.
2. From the navigation bar, click **Alerts** > **Sent Alerts**.
3. From the list, select one or more alerts and click **Delete**.
4. On the confirmation screen, click **OK**.

The alert is removed from Sent Alerts.

View alerts from other COGs

When an IPAWS alert arrives from another COG, the message is received by BlackBerry AtHoc as an incoming alert. If you have specified an alert template for the incoming alert, this triggers the alert targeted to an operator account. The operator can view the alert on the devices enabled for their user profile.

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

To learn how to set up the incoming alert and triggered alert template, see "Configure BlackBerry AtHoc to receive alerts from external COGs" in the *BlackBerry AtHoc IPAWS Plug-in for NDS Installation and Configuration Guide*.

Track alerts through BlackBerry AtHoc reports

The following sections describe how to track IPAWS alert usage.

Monitor alerts in Sent Alerts

You can track alerts that you send to other COGs and the public from the Sent Alerts screen in the BlackBerry AtHoc management system. You can access the Sent Alerts screen, by clicking on **Alerts** > **Sent Alerts** in the navigation bar.

All saved and sent alerts are display in the Sent Alerts list. By default, alerts are displayed in order of the start date, with the most recently created alert displayed first.

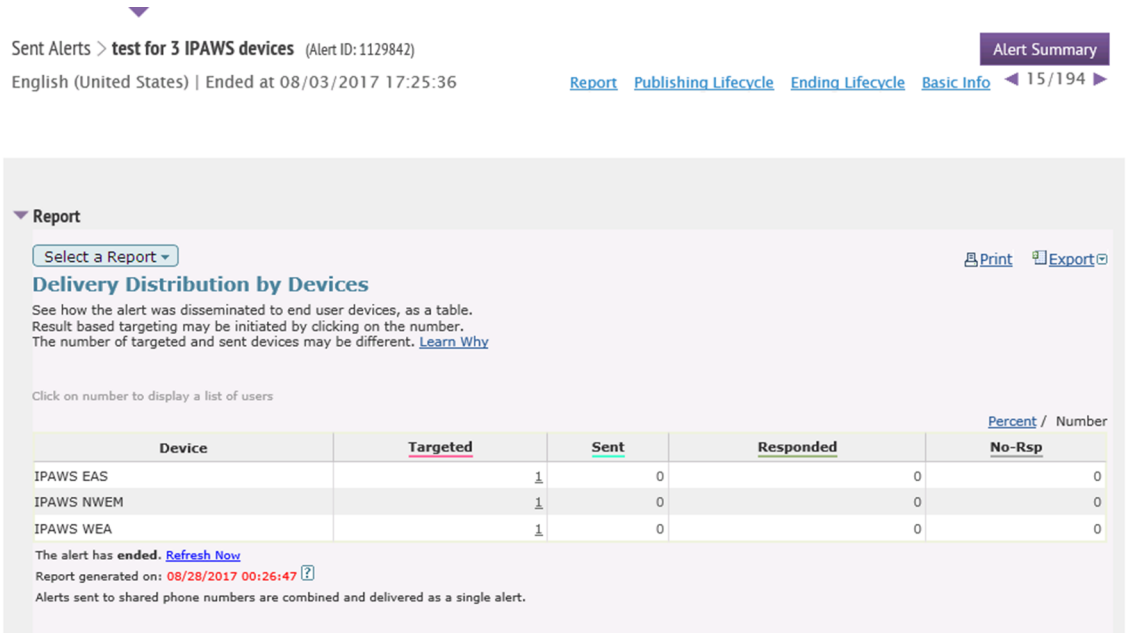
You can open a sent alert to view alert summary reports, batch delivery results, and a summary of recipients and responses. For detailed information about these reports, see the *BlackBerry AtHoc Alert Tracking and Reporting* guide.

Track published alerts

In an alert summary, the Reports list provides access to a set of reports that allow you to analyze the effectiveness of published alerts. Charts and summary data indicate if an alert has reached all intended recipients and also help you gauge their responses.

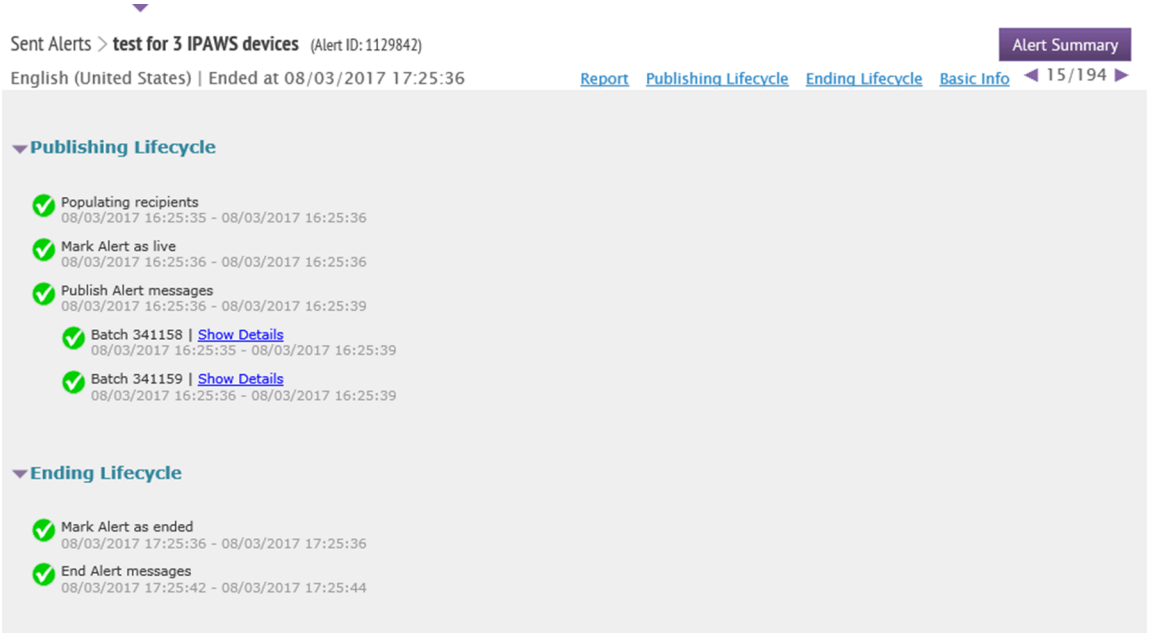
For example, if an alert did not reach all of the targeted recipients, there might be a problem with specific delivery devices. If you need to drill down to the user level, open one of the user tracking reports to see the alert delivery statistics for each target recipient. All tracking reports can be printed and exported.

1. Do one of the following:
   - On the BlackBerry AtHoc home page, in the **Live Alerts** section, click **Sent Alerts**.
   - In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alert** list, open an alert and click **Advanced Reports**.
3. In the **Reports** section:
   - The default report displayed is Delivery Distribution by Devices, which shows whether an alert reached all intended recipients and how they responded.
   - The Targeted number represents the number of users selected to receive the alert when the operator selected targets using distribution lists, attributes, or organizations.
   - The Sent number represents the number of alerts sent by the BlackBerry AtHoc system.



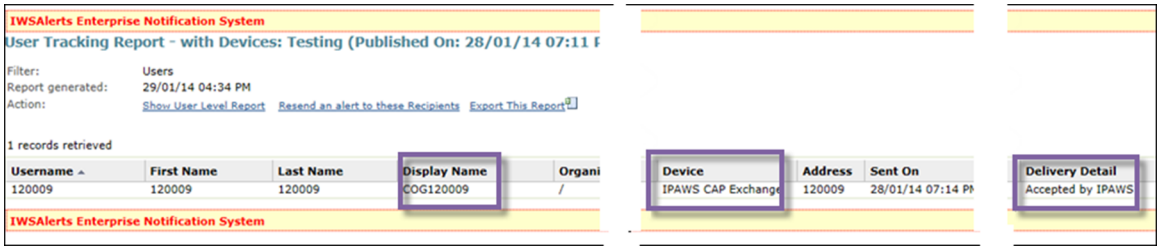
4. Compare the number of alerts sent with the number of responses by the intended audience. The report also displays the number of user responses received for each response option. The response values are based on the number of sent alerts.
5. In the **Publishing Lifecycle** section, check if there were delivery errors. Click **Show Details** to see the batch log.

   The Ending Lifecycle section displays the end time of the alert.

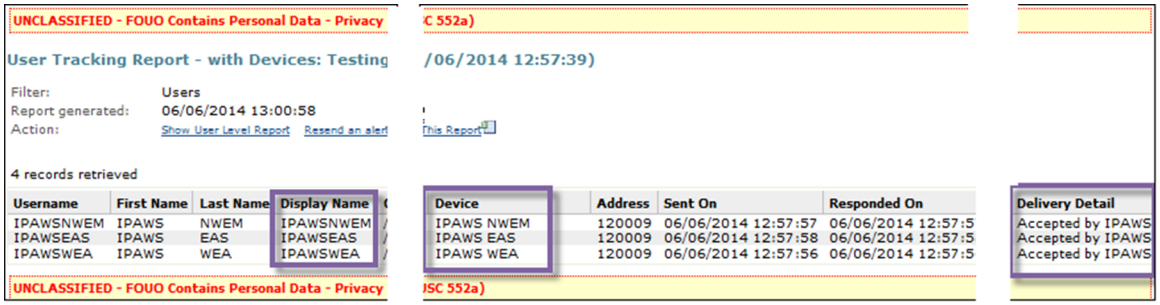


6. Click **Select a Report** to view different types of reports.

   For COG to COG alerts, the **User Tracking Report - with Devices** provides details by COG and shows the delivery status. For example, the following image highlights the target COG name, the IPAWS CAP Exchange device, and the delivery detail status "Accepted by IPAWS".



For public alerts, the **User Tracking Report - with Devices** provides similar details by device type. For example, the following image highlights the device name, the IPAWS public devices (EAS, NWEM, and WEA), and the delivery detail status "Accepted by IPAWS".



Export report data

To manipulate the report data for data mining or format the report before printing, use the export feature to create a Comma Separated Values (.csv) format file. Use an application such as Microsoft Excel to open the .csv file and for editing or formatting purposes. For each report, there is an option to export only the data shown in the report or to export data for all targeted recipients of the selected alert.

1. Send an alert.
2. Click **Alert Summary** from the completed alert or double-click to open the alert from the **Sent Alerts** list.
3. On the **Alert Summary** screen, click **Advanced Reports**.
4. Hover over **Export** in the top corner of the report.
5. Do one of the following from the **Export** list:
   - Select **Export Full Report** to view the list of all the targeted recipients.
   - Select **Export Current Report** to view information for only the recipients who received the alerts successfully.

The report is exported to a .csv file. You can see the status of each user.

When an export option is selected, a dialog provides the option to open the .csv file in Microsoft Excel or save it.

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

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 Settings and 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 Settings and 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 ⚙.

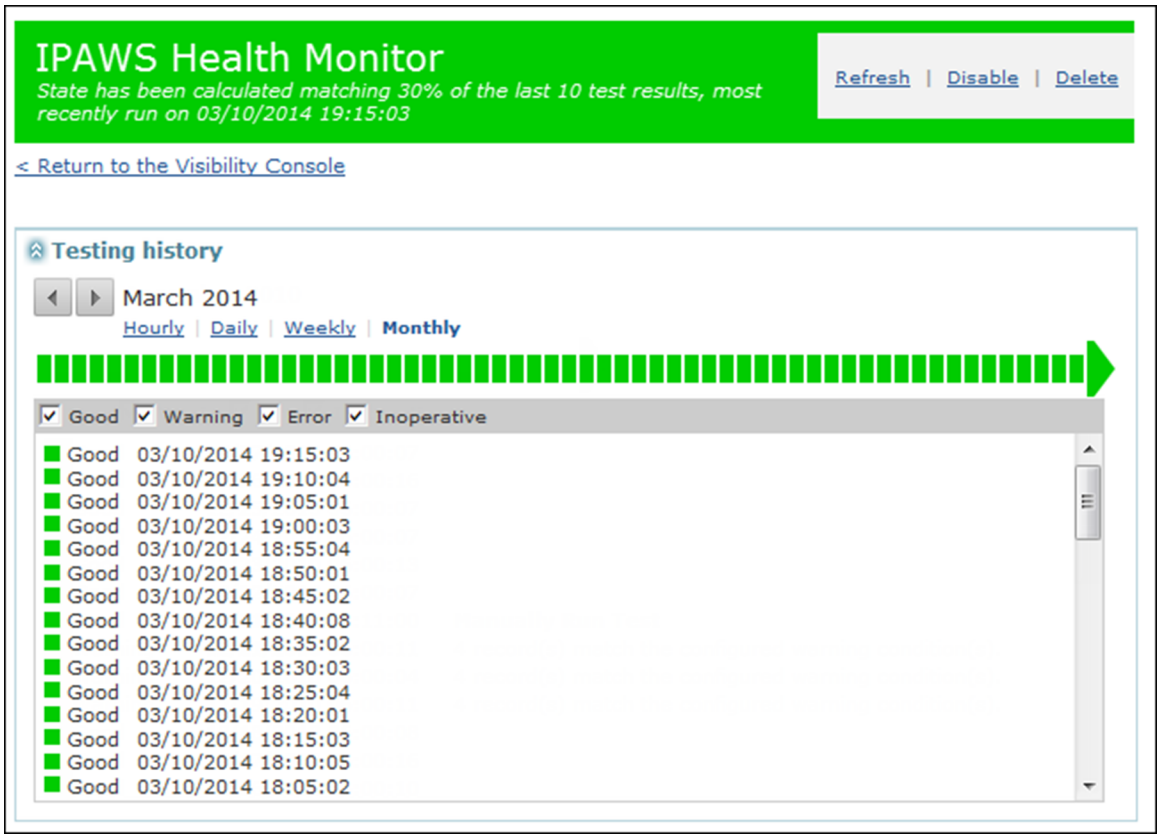
3. In the **System Setup** section, select the system health option that corresponds to your login access: **Global System Health** or **System Health**.

   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.

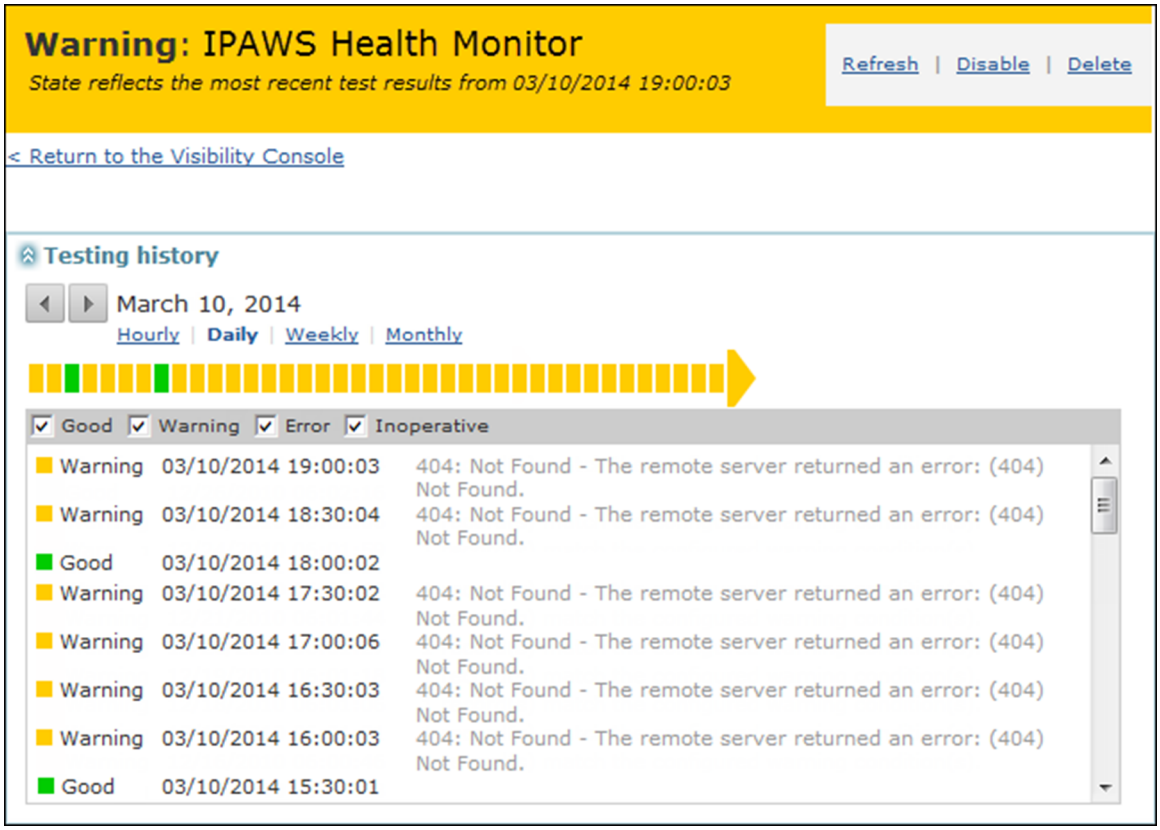
Icon	Description
	Error status. Indicates that the monitor test results meet the defined criteria for an error status.
	Warning status. Indicates that the monitor test results meet the defined criteria for a warning status.
	Good status. Indicates that the monitor test results meet the defined criteria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

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 3.0.

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://www.blackberry.com/us/en/support/enterpriseapps/athoc

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

Documentation feedback

The BlackBerry AtHoc documentation team strives to provide accurate, useful, and up-to-date technical documentation. If you have any feedback or comments about BlackBerry AtHoc documentation, email athocdocfeedback@blackberry.com. Please include the name and version number of the document in your email.

To view additional BlackBerry AtHoc documentation, visit https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc. To view the BlackBerry AtHoc Quick Action Guides, see https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/Quick-action-guides/latest.

For more information about BlackBerry AtHoc products or if you need answers to questions about your BlackBerry AtHoc system, visit the Customer Support Portal at https://www.blackberry.com/us/en/support/enterpriseapps/athoc.

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