



BlackBerry AtHoc

Create and Publish Alerts User Guide

7.9

Contents

- Create and publish alerts..... 6**
- Publish an alert from an existing alert template..... 7**
- Publish a blank alert..... 8**
- Search for an alert..... 9**
 - Filter the alert list..... 9
 - Sort the alert list..... 10
- View a quick summary of an alert..... 11**
- View the details of a sent alert..... 12**
- Change the number of alerts listed on the sent alerts screen..... 14**
- Edit an alert..... 15**
- Define alert template details..... 16**
- Define content for an alert or alert template..... 17**
 - Add attachments to an alert..... 18
 - Add an attachment using Dropbox..... 18
 - Select an alert or event location..... 19
 - View informational layers on a map..... 20
 - Change the map type..... 21
- Writing effective alert messages..... 22**
- Configure a response option as a user attribute..... 24**
- Target users..... 26**
 - Targeting basics..... 26
 - Define fill counts and escalation..... 26

Target groups in alerts or alert templates.....	28
Block groups and distribution lists from receiving a notification.....	28
Target individual users.....	29
Target dependents.....	29
Target subscribed users.....	29
Block a user from receiving a notification.....	30
Target or block users by advanced query.....	30
Target users by role.....	31
Target by location.....	31
Review the targeting summary.....	31
Select personal devices for an alert or alert template.....	32
Specify personal device options for an alert or alert template.....	32
Preview a desktop alert template.....	38
Target AtHoc Connect organizations.....	40
Select and configure mass devices for an alert or alert template.....	41
Review an alert.....	42
Test an alert.....	43
Set an alert to draft mode.....	44
Publish a draft alert.....	45
Quick publish an alert.....	46
Resend an alert.....	47
Track alerts with advanced reports.....	48
View advanced reports.....	48
Advanced report types.....	48
View alert lifecycle results.....	49
Export alert tracking reports.....	51
Message termination.....	52
Message consolidation.....	53
End an alert.....	54

Export an alert as a PDF.....	55
Export sent alerts.....	56
Delete an alert.....	57
Duplicate an alert.....	58
Hosted SMS text messaging tracking codes.....	59
Pager carrier IDs and names.....	60
Phone number validation.....	65
Email format validation.....	67
Email address syntax.....	67
Local-part.....	67
Domain.....	67
Valid email address examples.....	67
Invalid email address examples.....	68
BlackBerry AtHoc Customer Support Portal.....	69
Legal notice.....	70

Create and publish alerts

Alerts are communications sent to your organization, to mobile users, or to outside organizations. A BlackBerry AtHoc operator creates alerts and targets users, distribution lists, mobile users, and organizations through IPAWS or AtHoc Connect. Operators publish alerts from the Alerts menu.

Incoming alerts are alerts received from mobile users, outside organizations, or IPAWS.

Publish an alert from an existing alert template

Important: Before you create and publish a new alert, go to the BlackBerry AtHoc home page and check the list of all alerts that are currently live, scheduled, and recurring in the system. This will help you avoid creating a duplicate alert.

1. In the navigation bar, click **Alerts**.
2. Click **New Alert**.

The Select from Alert Templates screen opens, and displays all alert templates that you have access to in the system.

3. To view details about any of the alert templates in the list, hover your cursor over an alert template name.
4. Do one of the following:
 - Quick Publish: Click **Publish** beside an alert template in the **Ready to Publish** column.
 - Modify and publish: Click **Edit Alert** to modify the contents of any alert template. Click **Publish**.

See [Define alert template details](#), [Define content for an alert or alert template](#) and [Target users](#) for detailed instructions on how to fill in the content and target users.

Publish a blank alert

Important: Before you create a new alert, go to the default BlackBerry AtHoc screen and check the list of all alerts that are currently live, scheduled, and recurring in the system. This will help you avoid creating a duplicate alert.

If you have operator permissions, you can create a new alert without any predefined content or targeted users.

1. In the navigation bar, click **Alerts**.
2. Click **New Alert**.
3. On the **Select from Alert Templates** screen, click **Create a Blank Alert**.

See [Define alert template details](#), [Define content for an alert or alert template](#) and [Target users](#) for detailed instructions on how to fill in the content and target users.

Search for an alert

The alert search engine matches any set of letters or numbers anywhere in an alert title, folder name, or publisher name and is not case-sensitive.

Wildcards are not supported in searches.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. In the search field, type or paste a word or phrase found in the alert title.
4. Click **Search**.

Filter the alert list

You can filter the alert list by any combination of the following attributes: status, folder, date range, and publisher.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click **Advanced** to open the advanced filtering options.
4. Optionally, in the **Severity** drop-down list, select the severity you want to use as a filter: **High, Moderate, Low, Informational, or Unknown**.
5. Optionally, in the **Type** drop-down list, select the type of alert you want to use as a filter. The options displayed in the list are configurable and vary depending on the setup of your organization.
6. Optionally, in the **Status** drop-down list, select the status you want to use as a filter. The following options appear in the list: **Select All, Ended, Draft, Scheduled, Live**.
7. Optionally, in the **Publisher** drop-down list, select the name of the alert publisher you want to use as a filter.
8. Optionally, in the **Folder** drop-down list, select the name of a folder to limit the search to only alerts within that folder.
9. Optionally, in the **Start Date** and **to** fields, select the beginning and end dates of the date range that you want to use as a filter. The alert list then displays only those alerts that have a start date that falls within the range you specified.
10. Click **Search**.

The alert list displays all alerts that match the filter criteria.

Remove filters from the alert list

After you have filtered the alert list, you can do any of the following to filters:

- To remove all filters and return to the default alert list, click **Clear all** below the **Search** button.
- To remove a **Severity** filter, select the **Select All** option in the **Severity** drop-down list then deselect it to remove all selected options.
- To remove a **Type** filter, select the **Select All** option in the **Type** drop-down list then deselect it to remove all selected options.
- To remove a **Status** filter, select the **Select All** option in the **Status** drop-down list then deselect it to remove all selected options.
- To remove a **Publisher** filter, select the **Any Publisher** option in the **Publisher** drop-down list then deselect it to remove all selected options.
- To remove a **Folder** filter, select the **All Folders** option in the **Folder** drop-down list then deselect it to remove all selected options.
- To remove a **Date** filter, click in either or both of the date fields, then click the **X** next to the date.

Sort the alert list

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click the column heading that you want to sort by.

The alerts display in descending order of the values in the selected column.

4. Optionally, click the same column header again to sort in the opposite direction.

View a quick summary of an alert

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. On the **Sent Alerts** screen, use the search field or scroll down in the alerts table to locate the alert that you want to view.
4. Hover your cursor over the title of the alert. A tooltip is displayed, providing the following information:
 - **Alert Title**
 - **Body**
 - **Severity**
 - **Type**
 - **Time Left:** This field appears only if the alert has a status of Live.
 - **Response Options:** If the alert has a status of Scheduled or Draft, the response options appear by themselves. If the status is either Live or Ended, each response option is followed by a number that indicates how many respondents have chosen that option.
5. Click anywhere in an alert line to open the **Users** screen for the alert. The Users screen provides information about the targeted users and response details for the alert. Hover over the **Sent Details** or **Response Details** sections to display a tool tip that shows the number of users with each status. If dependents are enabled for your organization and in the alert template, the number of users displayed in the tool tip includes the number of sponsors and dependents.
6. Click the **Details** tab to view details of the content of the alert, including response options, severity, type, location, and alert time.

If attachments are included in the alert, they are displayed. Click the attachment to open a preview window. In the preview window, click **Download** to download the attachment.

The details screen is identical for both Live and Ended alerts except that the **Scheduled** section of a Live alert is editable, allowing you to change the end time.

- If the alert has a status of **Draft** or **Scheduled**, you can edit any of the details of the alert.
- If the alert has a status of **Live**, you can end the alert. You can edit the end time of the alert if there are five or more minutes remaining before the alert end time.
- If the alert has a status of **Ended**, you cannot make any changes to it.

View the details of a sent alert


After you click the **Publish** button to send an alert, you can click the **Alert Summary** button at the bottom of the **Review and Publish** screen.

If you are not on the Review and Publish screen, you can view the alert summary for any live or ended alert by completing the following steps:

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. On the **Sent Alerts** screen, use the search field or scroll down in the alerts table to locate the alert whose details you want to view.
4. Click anywhere in an alert line to open the details screen for the alert.

The **Alert Summary** screen that appears contains a Details tab and tabs for targeted Users, Organizations, and Mass Devices, when applicable.

If the alert is live, there is an **End Alert** button that you can use to end the alert immediately.

The Alert Summary screen lists the current status of the alert: Live or Ended. For live alerts, the information on the page updates automatically every minute. You can click  to update the screen manually.

Users tab

The Users tab provides statistics on the number of users who were targeted by the alert and the kinds of responses that were recorded from users who received the alert.

The **Sent Details** section contains statistics on the number of users targeted by the alert, the number of users the alert was sent to, and the number of users the system is still trying to contact, or the system failed to contact. For each of these options, a menu next to the number contains the following options:

- **Export Delivery Summary (CSV):** Click this option to create an exportable .csv file that contains the names of all users belong to the category you clicked: Targeted, Sent , or In Progress or Failed. Where applicable, the .csv file also contains the alert sent time, responded time, user response, and error time recorded for each user in the list.
- **Send alert to these users:** Click this option to open a duplicate of the original alert that you can modify and send out again. For the "In Progress or Failed" category, this option is a quick way of adding more personal devices and delivery methods to the alert to try to contact alert targets who were unaware of or unable to respond to the original alert.
- **User List:** Click this option to open a User Tracking Report. The report opens in a new browser window.

The **Response Details** section of the Summary tab displays a list of all of the possible alert response options, each assigned a different color. Next to each option the total number of alert recipients who have selected that option is displayed. This information is also represented in a pie chart.

The menu next to each response number contains the following options:

- **Export Delivery Summary (CSV) for sent alert:** Click this option to create an exportable .csv file containing the names of all recipients who chose the corresponding response option. Where applicable, the .csv file also contains the alert sent time, responded time, user response, and work related details for each recipient.
- **Send Alert to These Users:** Click this option to open a duplicate of the original alert that you can modify and send out again. For the Not Responded category, this option is a quick way of adding more personal devices and delivery methods to the alert to try to contact alert targets who were unaware of or unable to respond to the original alert. For other options, it is a way to provide specific additional instructions to a highly targeted group.
- **User List:** Click this option to open a User Tracking Report. The report opens in a new browser window.

Hover over the Sent Details or Response Details sections to display a tool tip that shows the number of users for each category. If dependents are enabled for your organization and in the alert template, the number of sponsors and dependents is displayed.

Organizations tab

The Organizations tab provides statistics on the number of organizations that were targeted by the alert and the types of responses that were recorded from those organizations.

Each list on the Organizations tab contains an **Export Delivery Summary** option. There is no option to send the alert again to the selected organizations.

Mass Devices tab

Note: Mass devices are not available for non-English alert templates.

The Mass Devices Targeted tab provides statistics on the number of mass devices that were targeted by the alert and the responses that were received from the devices. Because mass devices broadcast alerts rather than sending them to specific people or organizations, tracking mass device responses involves noting whether a delivered alert was accepted or not. The two response options used for mass devices are Responded, meaning the device broadcast the alert, and Not Responded, which means the device did not broadcast the alert.

The drop-down lists in the Targeted, Sent, and In Progress or Failed sections contain only an **Export Delivery Summary** option, which creates a downloadable .csv file that lists the mass devices that were targeted, that were sent the alert, or that did not or could not receive the alert. There is no option to send the alert again.

Advanced Reports button

The Advanced Reports button takes you to the Reports screen, where you can view a range of different reports. For more information, see [View advanced reports](#).

Note: Unlike the Report Summary screen, the Advanced Reports screen is not localized. The screen appears in U.S. English for all BlackBerry AtHoc users, regardless of their default system or organization locale.

Details tab

The Details tab displays all fields that were included in the alert.

The Total Users field in the Target Users section displays the total number of users targeted in the alert. Clicking the number opens a Users screen that displays the names and user details of each of the targeted users.

If attachments were included in the alert, you can click the image of the attachment to view or download it.

For live alerts, you can change the Alert End Time in the Alert Timing section of the Schedule section if there are five or more minutes remaining before the alert end time.

Change the number of alerts listed on the sent alerts screen

To make it easier to locate alerts on the Sent Alerts screen, you can change the number of alerts that appear on each page.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Scroll to the bottom of the alert list.
4. Click the list that appears next to the phrase **items per page**.
5. Select the number of alerts you want to display per page.

The screen refreshes and displays the total number of results you specified.

Edit an alert

The amount of editing that you can do to an alert depends on its current status:

- If the alert has a status of **Draft** or **Scheduled**, you can edit any of the details.
- If the alert has a status of **Live**, you can edit the End Time for the alert if there are five or more minutes remaining before the alert end time.
- If the alert has a status of **Ended**, you cannot make any changes to it.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the alert you want to edit.
4. Select the check box next to the alert name.
5. At the top of the screen, click the **More Actions > Edit**.
6. Make any changes you want to the unlocked fields.
7. Click **Save**.

Define alert template details

The Alert Template section is used to establish the identifying characteristics of the alert template in the system.

1. In the navigation bar, click **Alerts**.
2. Click **Alert Templates**.
3. Click **New**.
4. On the **New Alert Template** screen, in the **Name** field of the **Alert Template** section, enter a name and description for the alert template. The name and description display in BlackBerry AtHoc only; they are not displayed to end users. The name and description should make it easy to help publishers identify the alert template (for example, Tornado Warning).
5. In the **Description** field, provide details about the alert template purpose or content. For example, "Send out when there has been a tornado sighted within 5 miles of the facility." This description is not seen by end users; it is only visible within the application.
6. In the **Folder** field, click the down arrow and select the alert folder that you want to add the alert template to.
7. Optionally, select **Available for quick publish** if you want to make the new alert template available through all quick publish links in the application.
8. Optionally, select **Available for mobile publishing** if you want to make the new alert template available for publishing from the mobile app.
9. When you are done, configure the [Content](#) section.

Define content for an alert or alert template

The Content section is used to define the key parts of an alert or alert template in the system: the title, the body, the type, and any response options, website links, attachments, or location details that are relevant.

1. If you are creating an alert or alert template in a language other than default language displayed on the screen, click the button next to the Severity field and select the language from the list that appears. This does not change the language displayed on the screen. Instead, it changes the language that the message is delivered in. If text-to-speech is enabled, the audio portion of the sent alert will be in the language you selected.

2. In the **Severity** field, select the severity level from the list.

Important: High severity is reserved for extreme emergencies. On the Mobile application, it overrides the device sound settings to emit any sounds associated with the alert or alert template.

3. In the **Title** field, enter a one-line summary that communicates the purpose of the alert or alert template. There is a 100 character maximum in this field. The title is required and displays at the top of the recipients' screen when the alert is sent out.

4. Optionally, if you want to insert a placeholder into the alert or alert template title, click **+** and select the placeholder in the list that appears.

5. In the **Body** field, enter up to 4000 characters of text that communicate why the alert has been sent and provide instructions to the target audience.

For more details on what to include in the Body field, see [Writing effective alert messages](#).

6. In the **Type** field, select the type that fits with the alert or alert template you are creating.

7. In the **Response Options** field, do one of the following:

- Click the **Custom Response Options** list to view a list of pre-set responses you can add to the alert or alert template.
- Click the **Add Response Option** link to define one or more responses that alert recipients can send to let you know that they have received the message. If the response involves a call bridge, select the Call Bridge check box, then, in the two fields that appear below the check box, enter the call bridge number and passcode users will need in order to respond. For specific details about what call bridges are and how they are used, refer to the text box below.
- **Note:** Targeted users within countries that have a provisioned SMS country code can respond to SMS alerts. Users within countries that do not have a provisioned country code cannot respond to SMS alerts. For more information, including a list of countries with a provisioned code, see "[How does AtHoc SMS support sending text messages to countries abroad?](#)" on the BlackBerry AtHoc Support site.

8. Optionally, in the **More Info Link** field, enter one of the following:

- A URL that opens a webpage where users can go to get more details about the alert when it is sent out. When users receive the alert, a **For Further Information** link within it will take them to the webpage.
- A URL that opens an attachment (media or documents) stored on Dropbox. For details on how to store an attachment on Dropbox, see [Add an attachment using Dropbox](#).

Note: To include the URL in SMS alerts, the SMS alert template must contain a [TargetUrl] placeholder. For more information, see "Configure the hosted gateway for cloud services" in the *BlackBerry AtHoc System Administrator Configuration Guide*.

9. If you entered a URL in the previous step, click **Test URL** to verify that the link works correctly.

10. Optionally, in the **Location** field, click **Add** to access a map on which you can designate a geographic area for the alert or alert template.

For a detailed description of how to specify a geographic location for an alert or alert template, see [Select an alert location](#).

11. Optionally, in the **Attachments** field, drag and drop or click **Browse** to select files to include as attachments in the alert. For more information, see [Add attachments to an alert](#).
12. When you are done, configure the [Target individual users](#) section.

What Is a Call Bridge?

A call bridge is a type of alert response option for telephony devices consisting of a text response accompanied by either a phone number or a URL address. If you set up a Call Bridge phone option, end users must type the full phone number plus the passcode (if required) preceded by an 'x' delimiter: for example, (321)987-6543x98127.

If you set up a Call Bridge URL, the URL address must begin with one of the following:

- http:// – for standard web addresses
- https:// – for secured web addresses
- sip:// – for conference device addresses

Add attachments to an alert

If attachments are enabled for your organization and in the alert template, you can include text, audio, and video files as attachments in your alerts.

In the **Content** section of an alert, in the **Attachments** field, drag and drop files or click **Browse** to select files to include in the alert. Users who receive the alert can view the attachments from the BlackBerry AtHoc mobile app or email.

The following file types are supported:

- Adobe Acrobat document (.pdf)
- Microsoft Word document (.doc, .docx)
- Microsoft Excel document (.xls, .xlsx)
- Text document (.txt)
- Image files (.jpeg, .jpg, .tiff, .tif, .bmp, .png, .gif)
- Video files (.mp4, .mpeg, .mov, .wmv)

Note: File types that are not supported on all mobile platforms (.wma, .wmv, .mov, .tif, and .tiff) are converted to universally supported file types (.mp3, .mp4, and .jpeg) when uploaded.

Note: If you include attachments in an alert template, alerts created from that template include the attachments. The attachments can be removed and additional attachments can be added.

If you export the alert as a .pdf, any included attachments are displayed as images.

Add an attachment using Dropbox

Note: Visibility of the **Choose from Dropbox** button is controlled by an organization setting so it might not be active for your organization. If it is active, you must first register with Dropbox and then sign in before you can attach files. Details on how to register and sign in are presented below.

If you want to include an attachment in an alert, alert template, event, or event template, you can upload media or documents on Dropbox and then include a link to that attachment within the alert, event, or template you are creating. To add a link to an attachment stored in Dropbox, complete the following steps:

1. In the **Content** section of the alert, event, or template, click **Choose from Dropbox**.

2. Enter your Dropbox **username** and **password**. If you do not have a Dropbox account, click the **create an account** link under the **Sign In** button to create one.

Note: Although you need to set up an account in order to access Dropbox, you can use the **Choose from Dropbox** button to select files stored in the cloud or add files from your local drive without having to install the full Dropbox application on your computer.

3. Click **Upload**.
4. Click **Choose files**.
5. Navigate to the file you want to upload, then click **Open**.
6. Click **Done**.
7. Click the filename in your Dropbox homepage, then click the **Share** link that appears in the same row.
8. Copy the link location that appears in the **Link to file** field.
9. Paste the link location into the **More Info Link** field in the **Content** section of the alert, event, or template you are creating.

Select an alert or event location

There are two ways to add locations to an alert or event using the map feature: by defining custom locations using the drawing tools available on the map and by selecting geographic areas from a list of locations that were predefined by a BlackBerry AtHoc administrator.

Note: When Operators and Administrators create an alert or accountability template, they have the option to make Location a mandatory component by clicking the Settings button and selecting the **Is Location Mandatory** check box. When an operator creates an alert or event from the template, if a location is not added, the alert or event is assigned a status of "Not Ready."

Note: When you select **Email** or **Desktop Popup** in the **Select Personal Devices** section of an alert, an image of the map is included in the alert if this capability has been enabled for your organization.

To access a map where you can select one or more geographic location for an alert or event, complete the following steps:

1. In the **Content** section, click **Add** in the **Location** field.

A separate screen appears, displaying an interactive map.

Note: If you have the necessary permissions, you can set the default map area through the Map Settings screen.

2. Optionally, if the location you want to target is not displayed on the current map, enter the address, point of interest, or longitude/latitude value pair in the search field. Press **Enter** on your keyboard to refresh the map location.
3. To use a predefined location on the map as a targeting criteria, click **Select Predefined Locations** to access a drop-down menu from which you can select any of the layers that have been created for you. When you select a layer, the map updates automatically to display the layer location on the screen.

Note: Uploading multiple layers with different set of predefined locations is recommended to improve usability and system performance. Map layers are configured on the Map Settings screen. Administrators can access them at **Settings > Basic > Map Settings**.


4. Select one or more predefined locations within the layer by clicking them on the map or selecting the check box next to their names in the drop-down menu.

As you make selections, the locations are highlighted on the map.

5. To create a custom location, click **Create Custom Locations** to display the drawing tools for creating shapes.
6. Click one of the shape buttons in the Map Tools bar and click and drag on the screen to cover the location you want to use in the alert or event.

7. To view the size of a custom location, click the shape on the map. A black box appears next to the Create Custom Locations button, listing the total area of the custom location in square miles or square kilometers, depending on which unit of measurement your system uses.
8. To edit a custom location, click the shape and then click and drag on any of the circles that appear around the edge of the shape.
9. To scale new shapes up and down while preserving their dimensions, complete the following steps:
 - a. Press and hold the SHIFT key on your keyboard.
 - b. Click and release the shape to select it.
 - c. Move your cursor over one of the white squares around the shape.
 - d. Click and hold on the white box while dragging the mouse to increase or decrease the shape size.

As you create shapes and select predefined locations on the map, the **Location Summary** field in the bottom-right corner updates to provide you with an overview of the total number of locations that are displayed on the map and the locations that will be included in the alert or event.

10. To delete one of the custom locations you created, do one of the following:
 - In the Location Summary field, click the **X** button next to each location you want to remove. Note that if you have created more than one custom location, they are combined in the list and cannot be deleted individually. To delete individual custom locations, use the method described below.
 - Click the border of the location shape on the map to select it, then click  to remove it.
11. To see the total number of users and organizations that are located within the selected map locations, click **Calculate** next to the **Target By Location** field.

Important: Users and organizations listed in the Target By Location field are not *automatically* added to the alert or event target list. To add them as targets, you must select **Target Users** and **Target Organizations**.



12. When you are done adding locations and targeting users and organizations, click **Apply**.


View informational layers on a map


Informational layers are created in the Map Settings page within the BlackBerry AtHoc system and are not specific to the current alert. The same layers can be viewed in every alert template.

To enable operators to view multiple layers simultaneously, the Map screen includes a Layers icon. Selecting layers from this list adds them to the map for informational purposes: they can be seen, but not clicked. In contrast, the Select Predefined Location button allows operators to select a location from a single layer at any given time.

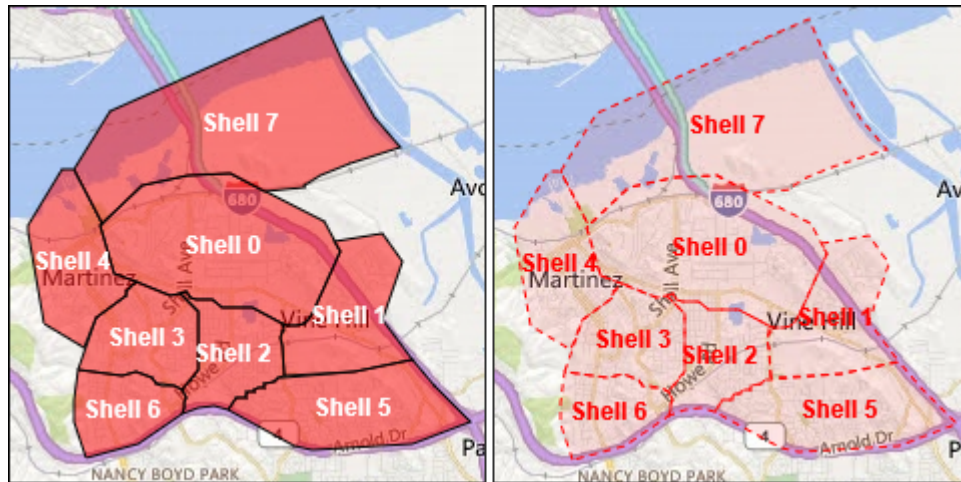
An alert map contains multiple map layers, each of which provides information about the location and target audience for the alert.

1. Open the alert map.
2. In the bottom left corner of the screen, click .
3. Select **Organizations** in the **Layers** list to view all of your connected organizations within the current map area. To view organization details, click the corresponding .

Note: If more than one object exists at or very close to the same geo-location coordinates, click  to see the details of the other organization.


4. Select **Live Incoming Alerts** in the **Layers** list to view all of the incoming alerts that fall within the current map area and include location information. To view incoming alert details, click the corresponding .
5. Click the check box next to any of the Layers check boxes to see it displayed on the map. The difference between selecting a predefined location in the **Select Predefined Locations** drop-down list and doing so in the **Layers** panel is that the location is not interactive when selected in the Layers panel. This non-clickable

status is indicated by the use of lighter shading and dotted lines around the edges of the locations, as shown on the right in the following image:



Note: Custom locations are not listed on the Layers panel.

Change the map type

To change the map style in an alert or alert template, click  in the bottom left corner of the screen and then click to select the map you want to use. The following options are available:

- **Bing Road:** Microsoft's standard drawing map with streets and major landmarks labeled.
- **Bing Aerial:** Microsoft's standard aerial photograph of the map area.
- **Imagery:** Aerial photograph of the map area.
- **Imagery with Labels:** Aerial photograph of the map area with major landmarks labeled.
- **Streets:** Traditional drawing map with streets and major landmarks labeled.
- **Topographic:** Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Dark Gray Canvas:** Dark drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.
- **Light Gray Canvas:** Light drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.
- **National Geographic:** Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Oceans:** Traditional drawing map with topographical land features displayed and underwater topography labeled.
- **Terrain with Labels:** Traditional drawing map with topographical features displayed and cities and major roads labeled.
- **OpenStreetMap:** Traditional drawing map with streets and major landmarks labeled.

Note: OpenStreetMap is provided by OpenStreetMap (www.openstreetmap.org.) All other map types, except for Bing maps, are provided by ESRI (www.esri.com.)

Writing effective alert messages

Use the following hints and best practices to publish successful alerts.

Content and message

- Keep the title and body brief and simple.
- If the alert is an Exercise or Test; clearly put the text “Exercise” or “Text” in the title and message. This practice ensures that everyone responds appropriately and no one mistakenly takes your exercise message for a real-world event.
- Use the five W’s: who, what, when, where, why, and how if needed.
- If you use acronyms or unique words, remember the text to speech may mispronounce your message or make it hard to understand. Add spaces or periods after each letter of the acronym.
- If you include a phone number, remember that the text to speech reads the number in this order: nation number, regional number, telephone exchange number, subscriber number, and extension number. Phone numbers are read digit by digit. If you include a regional number (area code) in parentheses, text to speech will not read the number correctly. For example: (xxx)-xxx-xxxx. To ensure that text to speech reads the regional number correctly, use one of the following formats:
 - xxx-xxx-xxxx
 - xxx xxx xxxx
 - xxx.xxx.xxxx

The following table lists supported phone number formats:

Example phone number	Text to speech expansion
1 800 123 4567	one, eight hundred, one two three, four five six seven
01.1234.5678	zero one, one two three four, five six seven eight
01.1234.5678 Ext. 15	zero one, one two three four, five six seven eight, extension one five
Call me at 123-4567	Call me at one two three, four five six seven

- Placeholders can be very useful when using alert templates. Don’t forget to select the values if they are included.
- Use the **More info** link to add a Web page or Dropbox attachment URL.
- Include Response Options. They are a powerful tool to see who has responded to your alert and can provide valuable accountability information from your users.

Devices and coverage

- Use the devices that will most likely reach your users at the time of the alert.
- Target your Connect Organizations if you want them to receive your alert
- When sending a Desktop Pop-up, ensure that you choose the template and audio that best corresponds to your alert.
- The Phone is the only device for which you can establish a delivery order. When selecting multiple telephony devices, prioritize the devices your recipients are most likely to use.
- Use the device Options to ensure your message is effectively communicated. For example, some devices have shorter message requirements. Or, a message that goes to the phones of individuals might be different than a message that goes to the general public over a loudspeaker.

- Use the Options for (SMS) text messages to shorten the content to 160 characters or less. If you exceed the 160 characters allocated for the title, body and response options, your message may be broken into several messages.
- When you use Twitter, use discretion because the message appears on social media, outside of your user base.

Publishing schedule

- Alerts can be scheduled to publish at a date and time in the future.
- Set the 'live' time for the time you want your users to be able to respond to your alert. You can estimate how long that they will receive the message and respond if they are away from their devices.

Review and publish

- If you have time, always test your messages before sending.
- Use Alert Folders (formerly called Channels) to organize your alerts.
- Use spell checking for your Title and Content before publishing.
- Verify in the Targeting Summary that the correct individuals are receiving your alert.

Configure a response option as a user attribute

Response options can be either of the following types:

- **Custom:** Defined during the creation of an alert or alert template. This is the most common type.
- **Preset:** Defined in advance as user attributes. The preset options have a feature that is not available in custom responses. When a user responds to the alert using a preset option, the response value is copied to their user record as a user attribute that can later be the subject of a query. The user attribute must be a single-select picklist, status attribute, or checkbox type. Use the single-select picklist type when you want to customize the response options. Use the checkbox attribute type if you require only a "Yes" or "No" response. Status attributes are used primarily as a single-select picklist for accountability events, but are also available as preset response options.

Note: Do not use a single-select picklist attribute that has more than 9 values as responses may not accurately update the values.

When a user responds to an alert on multiple devices, only the response on the first device updates the alert summary. A user can update the user attribute from the response options one time for each device that received the alert. For example, if email is used to update a response option, and more than one email address is targeted, only the first email address the user responds from will update the attribute. Each subsequent response is ignored in alert reports. The user can update the attribute value by using another device, such as Phone or SMS, each device can update one time per alert.

If an attribute is used as a response option in an alert, the last response from a single device is the response that updates the user attribute value. If the attribute needs to be updated again after the alert, the user must access Self Service to make the update. Additionally, operators and administrators can update the attribute in the BlackBerry AtHoc management system.

If an attribute is used as a response option in an accountability event, each device can update the event if there are changes to the user's status. Only a single device can be used to update the status attribute value.

Benefits of using a preset response option

Preset response options created as user attributes are appropriate in the following situations:

- As a way to efficiently gather data about users for use later in alert targeting. The response an alert recipient gives to an alert asking if they have medical training, for example, could be added to each respondent's personnel record. During a subsequent emergency, the user database could be searched and an alert immediately sent out to all users whose user attribute value for Medical Training is set to "Yes."
- When there is a need to send out multiple versions of the same alert but view the results in a single, aggregated report. The responses from each version of the alert are added to each respondent's user record. At any time, operators can generate a single personnel report that shows the aggregate totals for all response options across the multiple versions of the alert.

1. In the navigation bar, click .
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, click **New > Single-select Picklist**.

Note: If you require only a "Yes" or "No" response, select **New > Checkbox**.

Note: Do not use a single-select picklist attribute that has more than 9 values as responses may not accurately update the values.

4. In the **Basic** section, in the **Name** field, enter a name for the attribute.

5. For a single-select picklist attribute, in the **Value** section, add the response options for each picklist option. The recommended number of response options is 3 to 5. Do not use more than 9 response options.
6. In the **Page Layout** section, leave all drop-down lists set to **Do not show**.
7. Optionally, to track the responses:
 - a. In the **Personnel Reports** section, select the Enabled **Yes** option.
 - b. In the **Name** field, enter the same name you entered in Step 4.
8. Click **Save**.

The response option user attribute appears in the **Response Options** section of the alert details screen.

If you selected the **Enable** check box in Step 7, each time an operator publishes an alert with the response options you created, the option value each respondent selects is added to their user record. To view a summary of responses to each option, go to **Reports > Personnel Reports** and click **Summary** beside the name you gave the report in Step 7. A list of attributes and users who have selected the values are listed. A pie chart of the selected values is displayed.

For the attribute to show as a response option at least one user must make a selection in the attribute. You may need to log out and log in to see the new attribute as a response option.

Target users

The Target Users section allows you to identify the users you want to send an alert to or block from receiving the alert. As you create an alert or alert template, users can be identified based on their names, attributes, roles, group memberships, distribution list memberships, or physical locations.

Targeting basics

The following general targeting information can be used to plan how you target recipients for different types of alerts.

- User-based targeting provides one or a combination of ways to select users:
 - **By Groups:** Target users who belong to one or more groups selected by the operator. Groups can be defined as organizations, shared attributes, or distribution lists. For more information, refer to [Target groups in alerts or alert templates](#). Also enables the operator to block groups from receiving the alert. For more information, refer to [Block groups and distribution lists from receiving a notification](#).
 - **By Users:** Target individual users. Also enables the operator to block specific individuals within a group from receiving the alert. For more information, refer to [Block a user from receiving a notification](#). Also enables targeting dependents of sponsor users.
 - **By Advanced Query:** Target users based on standard or user attributes or delivery devices. Select this option to perform customized, on-the-fly targeting for an alert. For more information, refer to [Target or block users by advanced query](#).
 - **By Location:** Target users based on their geographical location. For more information, refer to [Target by location](#).

The administrator can restrict the organizational nodes and distribution lists that each publisher can access. As a result, a publisher might be able to target only a fraction of the total available organizations and distribution lists.

- Use [Fill Count](#) to specify a certain number of responses before ending an alert. This option is useful when you need confirmation that the alert has been received by a certain number of users.
- Additionally, you can enable [Escalation](#) to control the order in which users are contacted. Use escalation options to control the delivery order by groups or specific individuals.
- You can add a group escalation path based on user attribute values and priority. Another option is to specify a sequence that targets individuals, one-by-one, until enough users respond. After the fill count is met, the alert is ended.
- Blocking a recipient always takes priority during targeting. If a user is excluded, they *will not* receive an alert, even if they belong to a group, organization, geographical area, or distribution list that has been targeted to receive the alert.

Define fill counts and escalation

Use Fill Count to specify a certain number of responses before ending an alert. This option is useful when you need confirmation that the alert has been received by a certain number of users. For example, if you need ten emergency responders to report to an event, you can request this many responses before the alert ends.

Additionally, you can enable Escalation to control the order in which groups or individuals are contacted. For example, you might want a high priority group of users to be contacted before another group of users. To control the order, you use an attribute to target groups or users.

Note: If dependents are targeted in the alert template, Fill Count is not available. If Fill Count is enabled in the alert template, dependents cannot be enabled.

Example: Emergency notification with fill count and escalation

You need to set up an alert template to contact the appropriate teams during a chemical spill. You select a user attribute named EC_ChemSpill. The values of EC_ChemSpill include Chemical Facility, Supervisors, and Executives.

The creation and execution of this hypothetical alert would take place in the following stages:

1. You specify the number of "I can help" responses that must be sent before the alert can end. In this example, that number is 10.
2. You enable alert escalation by choosing a user attribute with groups that are contacted one at a time until the fill count is satisfied.
3. You set the sort order from lowest to highest to ensure that if 10 Chemical Facility team members do not select the "I can help" response option within the time frame, the alert escalates to the Supervisors team.
4. You enter an interval of 6 minutes for each team to respond before the alert escalates to the next team.
5. The first group, the Chemical Facility team, gets the alert immediately.
6. Only seven members respond within the six-minute interval for that part of the alert.
7. The alert then escalates automatically to the next team: the Supervisors.
8. Three members of the Supervisors team respond within the next six-minute interval. The fill count is met so the alert ends.
9. The Executive team is not contacted because the alert ended before it escalated to them.

Prerequisites

- The alert template must have the Fill Count setting enabled. See "Manage visibility options for Target Users fields in an alert template" in the *Manage Alert Templates Guide*
- The user attribute that will be used to target groups and users must be created:
 - It can be any attribute type other than memo or geo location.
 - (Recommended) For escalations, it is recommended to use a single- or multi-select picklist that targets the groups of users needed to meet the fill count.
- Users must have the selected user attribute as part of their profile.
- Response options must be defined in the Content section of the alert.

1. In the **Target Users** section, click **Fill Count and Escalation**.
2. In the **Required Response(s)** field, enter the number of responses needed to end the alert. This number can be changed when the alert is actually published.
3. Select a **Response Option** for the fill count, such as "I can help."
4. Optionally, elect **Enable Escalation** to define the order in which groups of users are contacted.
5. In the **Escalate By** list, select any user attribute with a type other than *memo* or *geo location*.

The attribute should target the users to which you want to deliver the alert. If the attribute is a picklist, ensure that the sort order is correct.

6. Specify the **Escalate By** method for the escalation or delivery method.

Select **Top to Bottom** to start with the first value in the attribute list or **Bottom to Top** to start with the last value in the list. For example, in planning for a chemical spill, you could select top to bottom to ensure that HazMat personnel are sent the notification before it is escalated to higher levels of authority.

7. Optionally, to enable controlled delivery, select **One User at a Time** as a Delivery Method.
8. In the **Interval** field, specify how much time will be given to a group to respond before the next group or user is contacted. If the first group does not send enough responses to meet the fill count during the interval, alerts go out to the next group in the sort order.
9. Click **Apply**.

Your choices are displayed at the top of the Target Users section. These choices can be edited before publishing.

10. To view the order in which users will be alerted, click the number next to Total Users. The list of users is displayed in the order of escalation priority.
11. Publish the alert.
12. Monitor the status of the fill count with the Alert Summary Report. As the users respond, the fill count increases.

Target groups in alerts or alert templates

Using the By Groups tab, publishers can target groups of users based on their memberships in organizational hierarchical nodes and in distribution lists. The alert is sent to users within the selected groups. Users who belong to multiple targeted groups receive a single alert.

The publisher can also block recipient groups (exclude them from alert delivery).

The Group target categories displayed are:

- **Organizational Hierarchy**—If your system is set up for them
- **Distribution Lists**—Static and dynamic
- **Targetable Attributes**—Any attributes that have been selected as targeting criteria

Note: The Administrator can restrict the contents of these categories for each publisher. For example, a publisher might have permission to view only one of four organizational hierarchies.

1. In the **Target Users** section, click **By Groups** if it is not already selected.
2. In the **Groups** field, select the check box next to each group or distribution list that you want to target.

If you select a group or distribution list that contains sub-groups or sub-distribution lists, those are automatically selected, too. However, any of them can be manually deselected by clicking the check box next to its name. If you select all of the sub-groups or sub-distribution lists manually, the parent group or distribution list is not selected automatically.


Note: The presence of a black square (or a black hyphen if you are using Google Chrome) in a check box indicates that some of its sub-groups or sub-distribution lists have been selected and some have not.

Block groups and distribution lists from receiving a notification

Blocking groups (which can be either organizations or distribution lists) can be done through the By Groups tab in the Target Users section by completing the following steps.

1. In the **Target Users** section, click the **By Groups** tab if it is not already selected.
2. In the **Groups** field, click **Block** next to each group or distribution list that you want to block from receiving any alert generated from the alert template.

Note: Even if a top-level group or distribution list is selected for inclusion, you still have the option of blocking any of the sub-groups or sub-distribution lists underneath it. Blocking takes precedence over inclusion, so blocked sub-groups and sub-distribution lists will not be targeted even if their parent groups or distribution lists are targeted.

As soon as you block a group or distribution list, the Block link in their row changes to an Unblock link and a  appears next to its name, preventing you from adding it to the alert recipients list.

3. If you want to unblock a group or distribution list, click **Unblock** next to its name.

Note: If you block a group or distribution list that contains sub-groups or sub-distribution lists, those are automatically blocked, too. In order to unblock any of the sub-groups or sub-distribution lists, you must

manually unblock the parent group or distribution list first. Note that if you manually block all sub-groups or sub-distribution lists, the parent group or distribution list will not display a blocked icon.

Target individual users

Targeting users can be done through the By Users tab in the Targeting section.

Note: If dependents are enabled for your organization and enabled in the alert template settings, the Target Users section displays separate tabs for sponsors and dependents.

1. In the **Target Users** section, click **By Users**.
2. In the **Users** field, click **Add/Block Users**.
3. On the **Add/Block Users** screen, select the check box next to each user that you want to target in the alert and then click **Block** next to any user you want to block from receiving the alert.

Note: If the name of the user does not appear on the screen, enter the name in the search field, and then click **Search**.

As you select (and block) users, the total number selected updates automatically at the top of the screen and the total number targeted and blocked appears below the search field.

4. After you have selected all users you want to include in the alert, click **Apply**

The Users screen then reappears, displaying the names of the users you added with a ✓ next to their name. If you blocked any users, a ⛔ appears next to their name.

Note: If you change your mind and want to remove a targeted user from the alert recipient list, click ✕ next to their name.

5. Optionally, to target dependents, click the **Dependents** tab and then select **Include all dependents of targeted sponsors**.

Target dependents

If dependents are enabled for your organization, you can target them on the Dependents tab in the Targeting section.

1. In the **Target Users** section, click **Sponsors**.
2. Select one or more sponsor users.
3. In the **Target Users** section, click **Dependents**.
4. Select **Include all dependents of targeted sponsors**.

Target subscribed users

When the organization subscription feature is enabled, organizations are enabled for subscription, and users subscribed to those enabled organizations, subscribed users can be targeted in alerts on their subscribed organization.

Subscribed users can be targeted on their subscribed organization using email, SMS, phone, and mobile app devices and can be targeted using any criteria such as location, groups, or attributes. Targeted devices must be enabled on both the home and subscribed organizations. When targeting subscribed users by attributes, those attributes must be enterprise-level attributes.

1. In the **Target Users** section, click **By Advanced Query**.


2. Click the **Select Attribute** list, and then scroll down and click **Subscribed Organizations** in the **Attribute** section.
3. In the **Select Operation** field that appears, select the **equals** operator. In the field that appears, select your organization.
4. Optionally, click the number in the **Advanced Query** field to view a pop-up screen that displays the attributes you have selected as targeting criteria for the alert.

Block a user from receiving a notification



In some situations, you might want to block (exclude) specific users from receiving an alert. Individual alert settings take precedence over group settings, so if a user is blocked, they will not receive an alert even if a group they belong to is included in the alert.

1. In the **Target Users** section, click **By Users**.
2. In the **Users** field, click **Add/Block Users**.
3. On the **Add/Block Users** screen, click **Block** next to each user you want to block from receiving the alert.

Note: If the user's name does not appear on the screen, enter the name in the search field, then click **Search**.

When you block a user, the Block link becomes an Unblock link and a  appears next to their name, preventing you from adding them to the alert recipients list.

4. After you have selected all of the users you want to block (and all users you want to add to the alert), click **Apply**.

The Users screen then reappears, displaying the names of the users you blocked with  next to their name and the users you added with a  next to their name.

Target or block users by advanced query

You can perform ad hoc targeting or blocking of users based on general attributes, organization hierarchies, geolocation, operator attributes, or device types.

1. In the **Target Users** section, click **By Advanced Query**.
2. Click **Add Condition**.
3. In the **Select Attribute** list, select the first attribute, organization hierarchy, geolocation, operator attribute, or device you want to use as targeting criteria.
4. In the **Select Operation** field, select the operation that you want to assign to the attribute. To block users who have specific attributes, select a negative operator such as **not equals** or **does not contain**.


Note: The list of operations varies depending on the type of attribute selected.

5. If the Operation you selected in Step 3 requires additional query values, a third field appears. Enter or select a value for the attribute.
6. Optionally, click **Add Condition** and then repeat steps 2 through 4 for each additional condition you want to add.

Note: In order to be included in the target group, users must meet all conditions specified by the condition statements.

The Targeting Summary field at the bottom of the Target Users section updates automatically to display the total number of users who match the query conditions you have created.

7. Optionally, click the number in the **Advanced Query** field within the **Targeting Summary** to view a screen that displays the criteria that you created for the advanced query.

8. Optionally, modify the query conditions as needed to isolate the exact user group that you want to send the alert to. Click **Add Condition** to add more conditions. Click  next to the condition to remove the condition.

Target users by role

1. In the **Target Users** section, click **By Advanced Query**.
2. In the **Select Attribute** list, scroll down to the **Operator Attribute** section and select **Roles**.
3. In the **Select Operation** field, select the query operation that you want use.
4. In the third field that appears, select the role or roles that you want to use as search criteria.

The Targeting Summary field at the bottom of the Target Users section updates automatically to display the total number of advanced queries you have created.

5. Optionally, click the number in the **Advanced Query** field to view a pop-up screen listing the operator roles you have selected as targeting criteria for the alert.

Target by location

In order to target users by location, you must first define a location in the Content section of the alert or alert template. For detailed instructions on how to do this, refer to [Select an alert or event location](#).

You can target users based on a geographical location that you select on a map.

1. In the **Target Users** section, click **By Location**.
2. Select the check box next to **Users in the defined location**.

The Targeting Summary field at the bottom of the Target Users section then updates to display the total number of locations on the map that will be used to target recipients when alerts are generated from the alert template.

3. Click the number in the **By Location** field to open a new screen that displays a map showing each of the locations that have been targeted. This is the same map that can be seen in the **Location** field in the **Content** section above.

Review the targeting summary

The bottom section of the Target Users section displays the Targeting Summary, showing the total number of groups and users that have been selected and blocked and the number of targeted locations and personal devices included in the alert. As additional groups, users, and devices are added to or removed from the target group, the section updates automatically.

Clicking any of the numbered links in the Targeting Summary field opens a popup screen that provides a list of the users, devices, or search conditions related to the selected target.

By Groups

The By Groups summary screen lists all of the organizational hierarchies and all distribution lists that are included in the alert. If a group or distribution list has children that have been blocked, the alert will not go out to users within those sub-groups or sub-distribution lists.

By Groups-Blocked

The Groups-Blocked summary screen lists all of the organizational hierarchies and all distribution lists that have been excluded from the alert. If all sub-groups or sub-distribution list of a parent have been blocked manually, the parent is not, by default, blocked as well. The parent can only be blocked by manually selecting it for blocking.

By Users

The By Users screen lists all of the users who have been selected for inclusion in the alert.

By Users-Blocked

The By Users-Blocked screen lists all of the users who have been blocked from receiving the alert.

By Location

The By Location screen displays a map showing each of the locations that have been targeted in the alert. This is the same map that can be seen in the **Location** field within the Content section of the new alert template or new alert screen.

By Advanced Query

The By Advanced Query screen lists the search conditions that have been created to identify the target audience for the alert.

Personal Devices

The Personal Devices screen displays a list of each of the personal devices that will be used to target the alert recipients. The percentage of alert recipients who can be reached using the device is listed next to each device.

Select personal devices for an alert or alert template

After selecting the users or groups you want to include in the alert or alert template, you must select the personal and mass devices to use to contact the target group.

1. In the **Target Users** section, click **Select Personal Devices**.

A list of all available personal devices appears, accompanied by statistics that reveal the total number of selected users who can be reached by each device type.

2. Select the check box next to each personal device you want to include.
3. As you select devices, the pie chart on the side of the screen updates to show the number of reachable and unreachable users based on your current selections.
4. Optionally, click the number next to the **Total Users** field to view a User Listing screen that displays the username and organizational hierarchy for each of the users in the target group.
5. Optionally, click the numbers in the **Reachable Users** and **Unreachable Users** fields to view separate popup screens providing user details for those subgroups.

Note: If no users are reachable based on the targeted users and devices you select, the alert template is not ready for publishing.

Specify personal device options for an alert or alert template

After you select personal devices for an alert or alert template, you can specify options for most of the devices by completing the following steps:

1. In the **Target Users** field, click the **Select Personal Devices** tab.
2. In the **Personal Devices** field, select the check boxes next to each of the personal devices you want to use as targeting methods.
3. Click **Options** in the top corner of the Personal Devices field.

The Personal Devices Options screen opens, displaying separate tabs and separate options for each of the devices you selected in Step 2.

4. After selecting options, click **Apply**.

The following table details the options that are available for the most common device types.

Device Type	Options	Explanation
Desktop Popup	App Template	<ul style="list-style-type: none"> All desktop pop-up alerts display the alert severity and type, and, if available, a link to the alert location. BlackBerry AtHoc provides default templates, one for each type of severity: High, Moderate, Low, Informational, Unknown. Specify the desktop delivery template, either the default template or a custom template. If you choose Use Custom Template, you can pick from any existing templates. Best Practice: Click the Preview button to preview the custom template. <p>Important: If your operating system has been magnified to 150% or higher, reduce the amount of text in the alert. If the alert exceeds the size of the alert dialog, the scroll bars might be unavailable.</p>
	App Audio	<ul style="list-style-type: none"> Select whether to use the default or a custom audio sound. The default audio is predefined by your organization. If you choose Use Custom Audio, you can pick from any existing audio sound. Best Practice: Click ► to preview audio selections.
	Map Image in Alert	<ul style="list-style-type: none"> Select Enable to include the location set in an alert template as a map in an alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map.
Email	Email Template	<ul style="list-style-type: none"> Specify the email template, either the default template or a custom template. BlackBerry AtHoc provides default templates, one for each type of severity: High, Moderate, Low, Informational, Forgot Password. <p>Note: If you select a custom template and your email delivery system does not support it, the default template is used.</p>
	Email Message Content	<ul style="list-style-type: none"> Select Alert Title and Body to use the information in the alert title and body fields as the email message content. Select Custom Text to enter a custom title and message body as the email message content.
	Map Image in Alert	<ul style="list-style-type: none"> Select Enable to include the location set in an alert template as a map in an alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map.

Device Type	Options	Explanation
Text Messaging	Content Sent Via Text	<ul style="list-style-type: none"> • Select Alert Title and Body to use the information in the alert title and body fields as the text message content. • Select Alert Title to use the information in the alert title as the text message content. • Select Custom Text to enter a custom message as the text message content. • Targeted users within countries that have a provisioned SMS country code can respond to SMS alerts. Users within countries that do not have a provisioned country code cannot respond to SMS alerts. For more information, including a list of countries with a provisioned code, refer to <i>How does AtHoc SMS support sending text messages to countries abroad?</i> on the BlackBerry AtHoc customer support site.
Pager	Content	<ul style="list-style-type: none"> • Select Alert Title and Body to use the information in the alert title and body fields as the pager message content. • Select Custom Text to enter a custom message as the pager message content.
Cisco IP Phone Display	Alert Image	<ul style="list-style-type: none"> • Select None if you do not want an image to accompany the alert. • Select Image to select an image from a predefined list. • Select Online Image to enter the URL for an image that you want to accompany the alert.
	Ringtone	<ul style="list-style-type: none"> • Select No Ringtone if you do not want a ringtone to play before the alert • Select Use Ringtone to select a ringtone from a predefined list. The tone will sound before the alert content plays.

Device Type	Options	Explanation
	Audio Broadcast	<ul style="list-style-type: none"> • Select No audio message if you want no audio to play when the alert is received. • Select Audio - Title and Body if you want the alert title and body to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Audio - Title Only if you want the alert title to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Audio - Body Only if you want the alert body to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Custom if you want to enter custom text for the alert. If you select this option, you have the option of setting the alert to replay as many times as you want.
Phone	Phone Message Content	<ul style="list-style-type: none"> • Select Send Alert Title and Body to use the information in the alert title and body fields as the phone message content. • Select Send Custom Text to enter a custom title and message body as the phone message content. • Select Send Recorded Message to create and upload a custom recorded message that will be played for the alert recipients. For complete details on creating a recorded message, see Create a custom recorded message for an alert or alert template. For complete details on uploading a recorded message, see Upload a custom recorded message for an alert or alert template.
	Recipient Answers the Call	<p>Select what you want to happen after the recipient answers the call:</p> <ul style="list-style-type: none"> • Deliver alert without any authentication. • Deliver alert only after the provided PIN is entered. • Deliver alert only after user validation.

Device Type	Options	Explanation
	Recipient Does Not Answer the Call	<p>Select what you want to happen if the call is not answered:</p> <ul style="list-style-type: none"> • Deliver alert as voice mail. • Leave callback information in the voicemail. <p>Note: If this option is selected, the end user must have a PIN associated with their account to retrieve the alert message from a phone number other than the phone number targeted in the alert.</p> <ul style="list-style-type: none"> • No voice mail.
	Requires Acknowledgment	Select if the alert has no response options. The acknowledgment steps are provided at the end of the alert
	Stop Calling Options	<p>Select the criteria you want to use to stop calls from being made to the alert recipient:</p> <ul style="list-style-type: none"> • Recipient acknowledged the message. • Recipient listened to entire message. • Entire message left on voicemail.
	Call Attempts	Enter the number of attempts the system should make to contact each recipient.
	Retry Interval	Enter the amount of time that must elapse before the system tries again to contact the recipient.

Device Type	Options	Explanation
BlackBerry AtHoc Mobile App	Repeat Notification	<p>Each alert is only sent once. This option is used to specify if and how often notifications about the alert are repeated on a mobile device.</p> <ul style="list-style-type: none"> • None: Send the alert notification once. • Default: Use the default time that has been defined for the selected severity. <ul style="list-style-type: none"> • For alerts with a severity level of High, the default is one notification a minute for 10 minutes. • For alerts with a severity of Moderate, Low, Informational, or Unknown, the default is one notification a minute for 2 minutes. • Custom: <ul style="list-style-type: none"> • Select how long to repeat the notification if the user does not respond. • Select how long to pause between each repetition. <p>Note: Ensure that the pause time is smaller than the repetition timeframe. For example, you can set the Stop Repetition After value for 5 minutes, and the Pause between Notifications value to 30 seconds - the notification can be repeated up to 9 times. However, if the Stop Repetition After value is 5 minutes, but the Pause between Notifications value is 6 minutes, the notification is repeated only once.</p> <p>Alert notifications repeat until one of the following actions occur:</p> <ul style="list-style-type: none"> • The recipient responds to the alert from at least one device. • The defined timeframe for repeat notifications elapses. • The alert ends.
	Deliver Alert with Sound	<ul style="list-style-type: none"> • Select Yes if you want the mobile device to play a sound according to the alert severity and device settings. For high severity alerts, this setting overrides the device settings and plays a sound when an alert is delivered. For all non high-severity alerts, the sound setting on the mobile device takes precedence. This is the default. • Select No to prevent the mobile device from playing any sounds. Alerts of any severity are delivered silently.


Create a custom recorded message for an alert or alert template

Note: Audio files are compressed to 8 bits before an alert is delivered. The quality of the recorded voice that is delivered to the end user may be different from the quality of the original audio file.


Note: Recorded messages are supported only on Chrome and Firefox browsers.

1. In the **Target Users** section, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the appropriate check boxes next to the **Phone - Work** and **Phone - Mobile** devices, depending on which you want to use as targeting methods.
3. Click **Options**.
4. Click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Record New Message**.
7. On the **Record New Message** window, click **Record** and then start speaking.

Note: As you speak, the timer on the screen counts down, showing you how many more seconds you can record. By default, the timer is set to 1 minute.

8. When you have finished recording the message, click **Stop**.
9. Optionally, click  to listen to your message.
10. Optionally, if you want to re-record the message, click **Record**.
11. When you are satisfied with the recording, click **Use Recording**.

The Personal Devices Options screen appears, with the Phone tab displayed and the filename field populated with a system-generated name for your recording.

12. Optionally, click  to download your message as a .wav file.
13. Optionally, make selections in the other fields on the **Phone** tab.
14. Click **Apply**.

The recorded message is then added and will be played when the alert is sent.

Upload a custom recorded message for an alert or alert template

Note: Audio files are compressed to 8 bits before an alert is delivered. The quality of the recorded voice that is delivered to the end user may be different from the quality of the original audio file.

Note: Recorded messages are supported only on Chrome and Firefox browsers.

1. In the **Target Users** field of the alert or alert template, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the check boxes next to the **Phone - Work** and/or **Phone - Mobile** devices, depending on which you want to use as targeting methods.
3. Click **Options** in the top corner of the **Personal Devices** section.
4. On the **Personal Device Options** screen, click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Browse** and navigate to the location where the custom recorded message is stored.
7. Click the filename and then click **Open**. The name of the file appears in the filename field.
8. Optionally, click **Play** to hear the message before attaching it to the alert or alert template.
9. Optionally, make selections in the other fields on the Phone tab.
10. Click **Apply**.


The recorded message is added and will be played when the alert is sent.

Preview a desktop alert template

1. In the **Target Users** field of the alert, click **Select Personal Devices**.

2. In the **Personal Devices** field, select the check box next to the **Desktop App** option.
3. Click **Options** in the top corner of the **Personal Devices** field.
4. If it is not already selected, click the **Desktop Popup** tab on the side of the screen.
5. In the **App Template** field, select the desktop template you want to use for the alert.
6. Click **Preview**.

Note: A preview of the template appears on the screen.

7. To preview the audio component of the alert, if you plan to include one, select an audio file from the **App Audio** list and then click .

Target AtHoc Connect organizations

Note: You must have the Connect Publisher, Organization Administrator, or Enterprise Administrator role to target AtHoc Connect organizations in alerts or alert templates or to respond to alerts from these organizations.

1. Create or open the alert or alert template to which you want to add organizations.
2. In the **Target Organizations** section, select each organization you want to target the alert or alert template to or select **Include all connected organizations** at the top of the section to target all organizations that you are connected to.

Select and configure mass devices for an alert or alert template

Note: This feature is not available for non-English alert templates.

Mass devices are designed to alert users in a general location using equipment such as digital signs, loudspeakers, and fire alarms. When using mass devices, there is no need to target individual users or groups.

1. In the **Mass Devices** section, select the check box next to each mass device you want to use to broadcast alerts.
2. Optionally, click **Options** at the top of the **Mass Devices** section.

Each of the mass devices you selected in Step 1 appears as a separate tab on the Mass Devices Options screen that opens. The contents of each tab vary depending on the type of mass device selected.

3. Click each tab on the screen and then configure each mass device by selecting from the range of options that appear.
4. When you have finished configuring all of the mass devices, click **Save**.

Review an alert

When you click **Review and Publish** after creating an alert, the **Review and Publish** screen opens.

1. Review the values in each section.
2. Optionally, to make changes to any part of the alert, click **Cancel**. The edit alert screen appears. Make and save your changes.
3. When you are satisfied with the alert contents, click **Publish** to initiate the alert.

The Alert Summary screen appears, displaying alert detail and targeting information and an **Advanced Reports** button that allows you to view detailed tracking reports for the alert.

Test an alert

The BlackBerry AtHoc system allows you to test any alert from the Edit Alert screen. Note that when you test the alert, it is sent only to you. If you are not included in the targeted users list or if you are not reachable (you do not have any of the devices targeted in the alert enabled for your account), the following error message is displayed when you try to run the test:

No devices are enabled for this operator to test the alert.

1. In the navigation bar, click **Alerts**.
2. Click **New Alert**.

The Select from Alert Templates screen opens, displaying all alert templates that you have access to in the system.

3. Click **Edit Alert** for the alert you want to test.
4. Click **Test Alert** at the top of the screen.

A **Test Alert** pop-up screen opens, letting you see the list of personal devices that will be sent a test alert. If your account is not set up for one or more of the alert devices, the device will appear in the list, but will be grayed out and the phrase **Not Available** will appear next to it.

5. Click **Test Alert** to initiate the test.

The pop-up screen closes and a confirmation notification appears at the top of the Edit Alert screen.

Set an alert to draft mode

Alerts are sometimes created in advance or created by users who do not have the necessary permissions to publish them. BlackBerry AtHoc allows the alert creator to set the alert to Draft mode, which retains all of the details of the alert in edit mode, but does not make it publicly available.

1. [Create the alert.](#)
2. Click **Draft** at the top of the screen.

The Sent Alerts screen appears and the alert is listed with Draft status.

Publish a draft alert

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the alert you want to publish.
4. Select the check box next to the alert name.
5. At the top of the screen, click the **More Actions > Publish**.
6. Review each of the sections of the alert to make sure that all of the settings are correct.
7. Optionally, if you need to make changes to any part of the alert, click **Edit** at the bottom of the screen, then make and save your changes on the edit alert screen.
8. When you are satisfied with the alert contents, click **Publish** to send the alert.

The Alert Summary screen then appears, displaying the current delivery, publishing lifecycle, and draft information for the report.

Quick publish an alert


When time is critical and you want to publish an alert where only the Title and Body content needs to be changed, you can edit only those sections without the need to wait for the entire Review and Publish page to load.

Before you can quick publish an alert, the alert template must be in a Ready state.

1. Access an alert template from any of the following locations:

- The Quick Publish section of the BlackBerry AtHoc management console home page
- The Alert Templates page
- The Sent Alerts page. (Select an alert, and then select **More Actions > Publish.**)

The Review and Publish page opens. The Title and Body fields in the Content section of the alert template appear in a white box at the top of the page.

2. Click . The Edit Title and Body window opens.

3. Edit the title and body text as needed. The title must be between 3 and 100 characters. The body must be fewer than 4000 characters.

4. Click **Apply**. You are returned to the Review and Publish page. If you click **Edit** at the bottom of the **Review and Publish** page to edit other sections of the alert template, any changes you made in the Edit Title and Body window are not retained.

5. Click **Publish**.

Resend an alert

The Resend feature in BlackBerry AtHoc allows an operator to customize the targets when resending an alert. The operator can resend the alert to all original recipients, to only recipients who responded to the original, or to only recipients who did not respond to, or did not receive, the original alert.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click the alert that you want to resend.
4. On the **Alert Summary** screen, click the **Users Targeted** tab if it is not already open.
5. View the **Sent Details** section of the report.
6. To resend the alert to everyone in the original targeting list, for example if you want to make modifications to the original alert, do the following:
 - a. Click the drop-down menu in the **Targeted** row.
 - b. Select **Send alert to these users**.
 - c. Optionally, revise the copy of the alert that opens.
 - d. Click **Review and Publish**.
 - e. Click **Publish**.
7. To resend the alert to everyone to whom the alert was successfully sent (for example, if you want to give them further details or instructions), do the following:
 - a. Click the drop-down menu in the **Sent** row.
 - b. Select **Send alert to these users**.
 - c. Optionally, revise the copy of the alert that opens.
 - d. Click **Review and Publish**.
 - e. Click **Publish**.
8. To resend the alert to everyone whose receipt of the alert is either still in progress or has failed, do the following:
 - a. Click the drop-down menu in the **In Progress or Failed** row.
 - b. Select **Send alert to these users**.
 - c. Optionally, revise the copy of the alert that opens by targeting new or additional personal devices.
 - d. Click **Review and Publish**.
 - e. Click **Publish**.

Track alerts with advanced reports

The following sections describe how to track alerts using advanced reports and how to export and print those reports.

View advanced reports

There are two methods you can use to view an advanced report. You can select a report from the Advanced Reports screen, or go directly to a specific report from the Users Targeted tab of the Alert Report page for a sent alert.

To view advanced reports from the Advanced Reports screen, complete the following steps:

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click a live or ended alert.
4. Click **Advanced Reports** at the top of the screen.
5. Select a report from the **Select a Report** list.

Note: To view a brief description of each report in the list, hover your cursor over the report names.

6. Select a report type to view.

The report opens in a new browser screen.

To view an advanced report for a specific set of users from the Sent Alerts screen, complete the following steps:

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click a live alert or one that has ended.
4. Click **Users Targeted**.
5. In the Sent Details section, select **User List** from the drop-down menu next to **Targeted, Sent, or In Progress or Failed** to go directly to an Advanced Report that lists users in that category.

Or

In the Response Details section, select **User List** from the drop-down menu next to **Responded or Not Responded** to go directly to an Advanced Report that lists users who have responded or have not responded to the alert.

Advanced report types

The following reports provide advanced tracking information about the alert delivery process, including the number of alerts sent compared to the delivery devices used and the responses received.

Report Name	Description
Organizational Report	Displays the alert progress for recipients grouped by Organizational Hierarchy.
Distribution List Report	Displays the alert's progress for recipients divided by targeted distribution lists.

Report Name	Description
Delivery Distribution by Devices (Chart)	Displays a group bar chart that tracks, for each device used, the number of targeted alerts, the number of alerts sent, and the number of responses received.
Delivery Distribution by Devices	Displays a tabular report that tracks, for each device used, the number of targeted alerts, the number of alerts sent, and the number of responses received. The report can include all devices or only the devices used for targeted recipients. An additional feature enables clicking any user count in the report, such as the number of targeted users, to open in a new window a detailed user tracking report that identifies individual users and provides their names, device addresses, and responses. Useful for evaluating the effectiveness of the delivery devices used for the alert.
User Tracking Reports	Displays user tracking information and user response data. The User Tracking with Devices report tracks which users were targeted by device and which device users responded on. The User Tracking with Alerts report tracks the delivery date and delivery status of the alert.

View alert lifecycle results

You can view the publishing lifecycle for the alert to trace the progress of the alert and determine how it was handled during delivery. The lifecycle shows information such as the following:

- When the alert went through the delivery gateway
- If a failure prevented the alert from being delivered
- If the alert needed to be redirected because of a gateway failover

You can also check the batch process to determine if the alert was delivered.

To view the publishing lifecycle events, complete the following steps:

1. Open the alert summary and do one of the following:
 - After sending the alert, click **Alert Summary** in the completed alert, then click **Advanced Reports** at the top of the screen.
 - In the navigation bar, click **Alerts**.
 - a. Click **Sent Alerts**.
The Sent Alerts screen opens, displaying a list of all alerts in the system along with their current status: Live, Ended, or Draft.
 - b. Click the live or ended alert you want to see lifecycle results for.
 - c. Click **Advanced Reports**.
2. Scroll to the **Publishing Lifecycle** section.
3. Check to see that the alert was marked as Live.
4. In the **Publish Alert messages** field, check for batch reports, and then click **Show Details** to see a detailed log.

A batch contains the alerts for each targeted user and is sent to a delivery gateway corresponding to the personal or mass devices targeted in the alert. The batch report tracks the delivery of the batch to the gateway and whether it was successful.

It shows if there was a problem with the batch and whether it had to be sent to another gateway for delivery. This is called batch recovery.

5. Check to see that the recipients were populated.

Note: If you have specified backup delivery gateways for the targeted devices, you might see additional batch reports if messages were redirected to a backup gateway because of a failover.

Alert partial batch recovery

BlackBerry AtHoc Cloud Delivery Services performs partial batch recovery when subset of batch of alerts cannot be successfully delivered to email, SMS, or telephony devices. Batch recovery occurs when delivery errors in the batch reach 20% of users, or more.

If there is a complete batch failure (100%), BlackBerry AtHoc tries to recover immediately.

For example, an operator publishes an alert that targets 50 users. Thirty-five users receive their alerts, however, message error codes were received for the other 15 users, exceeding the 20% recovery threshold. After 5 minutes, BlackBerry AtHoc sends a termination request to the primary gateway. It then creates a recovery batch only for the users that got errors for the next available gateway.

BlackBerry AtHoc cancels the current batch delivery and creates a new batch to be sent to another gateway, if the alert batch meets the following conditions:

- The network is up and BlackBerry AtHoc Cloud Delivery Service is available.
- Gateway reporting succeeds for the batch.
- The percentage of "No activity" plus "Error" messages reaches the recovery threshold within the batch. The default is 20%. Alerts that have received responses are not counted.

After a specified time (default is five minutes), BlackBerry AtHoc re-sends any alert that was not sent or does not have a response. Users that have responded to the alert do not receive another alert.

The new alert batch contains the following information:

- All alert messages that had delivery errors
- All alert messages that had no delivery tracking information (inactivity)
- Relevant phone messages that had MSG-SENT codes, when the contact cycle value is greater than "1"
- Excludes all messages that already have acknowledgments coming from any devices

To view delivery information, check the Publishing Lifecycle section of the Alert Summary, as shown in the previous section. The Batch details show how many alerts, whether the batch was sent successfully, and if it had to be redirected. You can also check user delivery reports for more information.

The following figure shows the history of the alert delivery and the recovery process.

Populating recipients
 23/02/16 13:24:01 - 23/02/16 13:24:01

Mark Alert as live
 23/02/16 13:24:01 - 23/02/16 13:24:01

Publish Alert messages
 23/02/16 13:24:01 - 23/02/16 13:24:07

Batch 123368 | [Hide Details](#)
 23/02/16 13:24:01 - 23/02/16 13:29:19
Sent via AtHoc Cloud Delivery Service (West)
 Last reported 23/02/16 14:18:11
Delivery Gateways to use
 AtHoc Cloud Delivery Service (West)
 AtHoc Cloud Delivery Service (East)
 Notification Delivery Managed Service (NDMS)
Population
 0 total messages
History
 23/02/16 13:24:02 Pickup
 23/02/16 13:24:02 Batch delivery succeeded
 23/02/16 13:29:07 Gateway not processing messages; Initiating batch recovery
 23/02/16 13:29:07 Cancelling current batch pending messages for current gateway (new termination batch: 123419)
 23/02/16 13:29:19 Creating recovery batch for pending messages for next gateway (new publishing batch: 123421)
 23/02/16 13:29:19 Batch recovery process completed

Batch 123419 | [Show Details](#)
 23/02/16 13:29:07 - 23/02/16 13:29:19

Batch 123421 | [Show Details](#)
 23/02/16 13:29:19 - 23/02/16 13:39:19

As you can see, the initial alert batch had to be terminated (Batch:123419) for the current gateway, and a second publishing batch was created (Batch: 123421). You can click on the details for the additional batch reports to see if the batch was successfully sent. The batch can be sent to additional gateways if there are problems with second batch.

Export alert tracking reports

You can export alert tracking reports to a .csv file to view the full detailed report or for other tracking reasons.

1. Send an alert.
2. Click **Alert Summary** from the completed alert or open the alert from the **Sent Alerts** list.
3. On the **Alert Summary** screen, click **Advanced Reports**.
4. Hover over the **Export** link and then select **Export Full Report**.

The report is exported to a .csv file.

Message termination

The BlackBerry AtHoc management system performs message termination on telephony devices for users with multiple targeted devices. When a targeted user for an alert has multiple devices in the system, and responds on one device, for example email, the user does not receive duplicate alerts on their targeted phone. Message termination saves resources and improves alert delivery performance and user experience.

Message termination is performed only on BlackBerry AtHoc hosted telephony. It is not performed on NDMS telephony.

Message termination is enabled by default.

Disable message termination

Message termination is enabled by default.

1. Start **Internet Information Services (IIS.)**
2. In the **Connections** panel, expand the **Sites** folder.
3. Expand **IWS Services**.
4. Click **User Termination Coordinator**.
5. In the **Actions** panel, click **Stop Application**.
6. In the **Connections** panel, click **Application Pools**.
7. In the **Application Pools** pane, click **Athoc User Termination Coordinator Pool**.
8. In the **Actions** panel, in the **Application Pool Tasks** section, click **Stop**.

Note: If the Application Pool task indicates that it is already stopped, you can stop the process using the task manager.

9. Reset IIS.

Message consolidation

Message consolidation applies to phone and text messaging devices only. Consolidation occurs when multiple users have the same phone number. It does not occur when a user has entered the same phone number for multiple device addresses.

For example, an alert targets a work phone, mobile phone, and text messaging. One of the targeted users has entered the same phone number in the address field for each device. The system sends two phone calls and a text message to the same device.

When the same alert targets several users who share a phone, the system sends one phone call to the phone. Note that response options are disabled when message consolidation occurs.

End an alert

You can end alerts that currently have a status of Live.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the alert or alerts you want to end.
4. Select the check box next to the name of each alert you want to end.
5. At the top of the screen, click **More Actions > End**.
6. Click **End**.

The alert status changes from Live to Ended.


Export an alert as a PDF

The BlackBerry AtHoc system allows you to export alerts as .pdf documents by clicking a button on the Review and Publish screen that appears when reviewing a new or draft alert.

Export a draft alert

You can export an alert that is in a Draft state.


1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the alert that you want to export.
4. Click anywhere within the alert row.
5. Optionally, add or modify information on the alert details screen that appears.
6. Click **Review and Publish** at the top of the screen.

Note: If any required information is missing, the Review and Publish button will be inactive, indicated by a  on the side of the button.

7. At the bottom of the **Review and Publish** screen, click **Export to PDF**.
8. The alert details are downloaded as a .pdf file.

To export an alert that has not yet been sent or put into a Draft state, complete the following steps:

1. In the navigation bar, click **Alerts**.
2. Click **New Alert**.
3. Click **Create a Blank Alert**.
4. Complete each of the required sections of the alert.
5. When you are done, click **Review and Publish** at the top of the screen.

Note: If any required information is missing, the Review and Publish button will be inactive, indicated by a  on the side of the button.

6. At the bottom of the **Review and Publish** screen, click **Export to PDF**.
7. Follow the instructions to save or open the alert.

Note: If the alert contains attachments, they are displayed in the .pdf as thumbnail images. The attachments cannot be viewed or downloaded from the export .pdf.

Export sent alerts

The BlackBerry AtHoc system enables you to export the details of sent alerts to a .csv file. The report contains the following columns: Alert ID, Alert Title, Alert Body, Start Time, Publisher, Severity, Type, Status, Targeted, Sent, Responded, and Error.

Note: You must have Report Manager Operator permissions to export sent alerts.

If the sent alert page is sorted by column, the exported report reflects the sorting.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the sent alerts you want to export.
4. Select the sent alerts you want to export.
5. Select **More Actions** > **Export**. A browser confirmation window opens.
6. Select **Save** to download the report or **Open** to open and edit the report.

Delete an alert

You can delete any alert that has a status of Draft or Scheduled. If the alert has a status of Live or Ended, it cannot be deleted from the system.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Locate the alert you want to delete.
4. Select the check box next to the alert name.
5. At the top of the screen, click **More Actions > Delete**.
6. Click **Delete**.

The Alerts screen refreshes and the alert no longer appears in the list.

Duplicate an alert

Important: When you duplicate an alert, the Schedule section of the new alert reverts to the default settings for all new alerts, overriding any date and time parameters that are configured for the alert that you duplicated. For example, if you duplicate an alert that is set to begin at 12:30 PM on August 1, 2015 and your system default is to have all new alerts begin "As soon as I click the "Publish" button," your duplicated alert will begin as soon as you click **Publish** unless you manually change the Alert Timing setting beforehand.

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Use the search field or scroll down in the alerts table to locate the alert that you want to duplicate.
4. Select the check box next to the alert name.
5. At the top of the screen, click **Duplicate**.

The Duplicate Alert screen opens, displaying a copy of the alert.

Note: If the original alert contains attachments, they are included in the duplicate alert. You can remove these attachments, or add additional attachments.

Hosted SMS text messaging tracking codes

The following codes are used to track the status of SMS text messages. They appear in the full delivery report for an alert.

Code	Status	Message
3001	Sent	Invalid destination phone number
3002	Sent	The target user has unsubscribed from BlackBerry AtHoc alerts
3003	Not Sent	The target carrier has blocked BlackBerry AtHoc alerts
3006	Not Sent	Rejected by the SMS aggregator
3007	Not Sent	Rejected by target carrier
3900	Not Sent	Error in sending alert

Pager carrier IDs and names

The following table displays the name and ID of all of the pager carriers that are supported in [BlackBerry AtHoc](#).

Pager Name	ID	Pager Name	ID
AAA	1	MetroCall National TAP (888)	164
Advanced Paging and Wireless	2	MetroCall National2 TAP (800)	165
Advantage Paging	41	MetroCall TAP (757)	166
Airtouch Paging	3	MetroCall TAP (904)	162
Airtouch TAP	84	Metrotel National TAP	167
AllCom	4	Metrotel TAP	100
ALLTEL PCS	42	Midwest Paging	39
Alpha Messaging Center TAP	103	Midwest Paging National TAP	123
AlphaNow	5	Minncomm	57
American Messaging	73	MinnComm National TAP	133
American Messaging National TAP	149	MinnComm TAP (763)	134
American Messaging Network	81	Mobilfone	94
American Messaging TAP	74	MultiComm Paging TAP	97
American Messaging TAP (305)	145	MultiComm SNPP	98
American Messaging TAP (520)	140	MWD TAP	72
American Messaging TAP (586)	146	National Communication TAP	102
American Messaging TAP (618)	139	Network Services	20
American Messaging TAP (714)	147	New SPN National TAP	189

Pager Name	ID	Pager Name	ID
American Messaging TAP (734)	138	New SPN TAP (252)	194
American Messaging TAP (734)	144	New SPN TAP (330)	197
American Messaging TAP (734)	142	New SPN TAP (406)	190
American Messaging TAP (818)	150	New SPN TAP (609)	191
American Messaging TAP (818)	148	New SPN TAP (612)	193
American Messaging TAP (904)	141	New SPN TAP (626)	192
American Page Network	52	New SPN TAP (626)	195
Ameritech	6	Nextel	21
Ameritech 001 TAP	106	Nextel 2 Way	22
Ameritech TAP (314)	108	Northeast Paging	23
Ameritech TAP (573)	107	Omni-com Paging	24
Aquis SNPP	210	Omnicom TAP (406)	110
Aquis TAP (615)	200	One Source	203
Arch National TAP	158	Other	40
Arch Wireless (USA Mobility)	38	Page 1	78
Arch Wireless 1-way (USA Mobility)	61	Page One TAP (304)	187
arch1way (USA Mobility)	18	Page Plus TAP (918)	153
AT&T Wireless	58	PageMart Canada	25
ATS National TAP	161	PageMe Inc	55
ATS Paging	83	PageNet - Canada	53
ATS TAP (402)	160	Pagenet Pro TAP	66

Pager Name	ID	Pager Name	ID
ATT Tap	208	PageOne - TX	215
Bailys Comm.	43	PageOne UK	92
Baystar	7	PagePlus	90
beepers.com	60	Pager People TAP	101
Bell Mobility (US)	8	Personal Page	214
Bell Mobility TAP (416 / Walkerton, ONT)	205	Porta-Phone Paging	26
Bell Mobility TAP (519 / Walkerton, ONT)	206	Priority Communications	27
BELL SNPP	204	ProPage	28
Cap Communications TAP (231)	175	RAM-Page	62
Carolina Wireless TAP	99	Range Paging	196
Carolina Wireless TAP (843)	172	Range Telecommunications	185
CellularPage	88	Range Telecommunications (TAP 512)	211
Central Vermont Comm.	45	Range Telecommunications TAP	209
Chariton Valley National TAP	199	RCS Wireless	77
Cingular	64	Rogers Two Way	48
Comm Special TAP (910)	109	RSC COMM National TAP	151
Communications Specialists	9	Satellink	29
Contact Communications	82	Satellink TAP (615)	111
Contact Paging	10	SBC National TAP (800.250)	129

Pager Name	ID	Pager Name	ID
Contact Wireless	207	SBC National TAP (800.864)	132
Cook Paging	37	SBC National TAP (877.802)	130
DataComm	11	SBC Paging	56
DataPage	12	SBC TAP	85
Dial A Page TAP (479)	186	SBC TAP (313)	131
Digi-Page/ Kansas	13	SBC TAP (573)	127
Edge Wireless	79	SBC TAP (763)	128
Electronic Engineering TAP (319.362)	181	Schuylkill Mobile	93
Electronic Engineering TAP (319.833)	180	Schuylkill TAP (570)	154
Electronic Engineering TAP (515)	179	Schuylkill TAP (717)	155
Extel Mobile	14	Sharp TAP (256)	176
GrayLink	15	Skytel	30
Highland Paging, Inc.	16	SkyTel National TAP	173
Illinois Signal	46	Skytel Talkabout	63
IM Cingular	76	Skytel TAP	67
Indiana Paging SNPP	44	Sprint SNPP	89
Indiana Paging TAP (219.756)	126	Stenocall TAP (806)	174
Indiana Paging TAP (219.928)	124	Teleone TAP	104
Indiana Paging TAP (317)	125	Teleone TAP (903)	178
Infopage Systems	17	Telepage TAP	105
Intelliguard Systems	95	TeleTouch (TeleOne) SNPP	202

Pager Name	ID	Pager Name	ID
Intelliguard Systems (TSU/Raven)	96	Teletouch TAP (501)	171
Island Page	68	Teletouch1 National TAP	168
JSM Comm TAP (414)	137	Teletouch2 National TAP	169
JSM Comm TAP (608)	136	Teletouch3 National TAP	170
JSMCOM 1-way	65	Tele-Trak	31
KP In-House	213	Telus Vancouver TAP	91
KPN TAP	212	Texas Communications	198
Lauttamus 2 TAP (304)	183	TSCNet	32
Lauttamus Communications SNPP	201	TWR TAP (301)	184
Lauttamus TAP (304)	182	UCOM	50
Maximum Communications	54	UCP	33
Metro Communication TAP	87	Unity Comm TAP (304)	135
Metrocall (USA Mobility)	19	Unity Communications	59
Metrocall 1-way (USA Mobility)	51	US Mobility TAP	75
MetroCall National TAP (800)	163	USA Mobility	80

Phone number validation

Overview

An Emergency Mass Notification System is only as effective as the contact information it contains. For this reason, BlackBerry AtHoc provides a phone number validation feature that applies to all phone numbers, no matter which country they belong to. It also enforces clean data wherever data can be entered.

The validation feature gives operators higher confidence before an alert is sent that end users with phone numbers are reachable. One way it does this is by ensuring that end users completing self-service profiles enter actual phone numbers, instead of invalid data such as “No Phone” or “N/A.” Validating phone numbers when they are created in the system makes the alerting process more rapid and efficient by preventing the Telephony Delivery Service from wasting time trying to send telephone notifications to invalid numbers.

BlackBerry AtHoc provides this feature for customers operating outside or calling users who are outside the United States. Validated phone numbers can be stored in the internationally recognized E.164 format, ensuring that alerts sent by delivery services deployed throughout the world will reach their destinations. BlackBerry AtHoc uses a third-party library to validate phone numbers.

BlackBerry AtHoc works with customers to make sure that automated data imports, including Active Directory sync, .csv imports, and direct SDK integrations, will send phone numbers to the server in the correct format. The following sections provide the validation rules and best practices for getting the most out of this feature.

Areas of the system that validate phone numbers

The following inputs will use the same set of phone number validation rules:

- AtHoc SDK
- LDAP/Active Directory Sync module
- CSV Import
- Self Service
- User Details page in the Management System

Validation rules

The following validation rules are delivered by a third-party open source component. For more information, see: <https://github.com/googlei18n/libphonenumber>.

1. E.164 international format is preferred and is always accepted.
 - The number should start with + followed by the country code and then the full number to call. A maximum of 15 digits can be used.
 - For example: +18884628462
2. Numbers can have an extension.
 - The user interface has a separate field for telephone extensions. When importing numbers, an x should be used to separate the main number from the extension.
 - When dialing, the Telephony Delivery Service will wait for the call to connect before dialing the extension.
 - For example: +18884628462x1340
 - Unlike the phone number field, the extension field is not validated.
3. Numbers not in E.164 are interpreted based on the Default Country Code for the Organization.
 - The Default Country Code can be set on the General Settings screen in the Phone Call Settings section.
 - For example, for the Country Code “US,” the following rules apply:
 - If the number starts with 011, which is the international exit code from within US, it will be replaced with +.
 - If the number contains only 10 digits, it will be stored as +1 followed by the number.

- If the number contains 11 digits and starts with 1, it will be stored as +1 followed by the number.
 - For example: (888) 462-8462 will be interpreted as +18884628462
4. Common formatting punctuation is ignored.
 - The following characters are removed: ().-_
 - For example: +1 (888) 462-8462 will be interpreted as +18884628462.
 - If you are using control characters such as , (comma) or # (pound sign), they must be in the extension field.
 5. If the number contains letters, they will be converted to numbers according to a standard keypad.
 - For example: (888) Go AtHoc will be converted to +18884628462.
 6. If the number starts with +, it will be assumed to be an international number.
 - For example: A number starting with +440 will dial the UK, even though 440 is a valid US area code.

Best practices

Send all numbers in E.164 format. Although E.164 format is not required, it is the best way to send a number to the system, especially if user data can contain numbers from different countries.

Make sure you set the correct Default Country Code in the Phone Call Settings section on the General Settings screen. This specifies what country is the default for user-entered phone numbers. This also is used to interpret phone numbers that are not in E.164 format.

If the number contains any special control characters that must be dialed, such as , (comma) ; (semicolon) * (asterisk) or # (pound sign), the characters must be part of the extension. This is especially important for numbers that connect to a conference bridge.

Special note

If you are unable to comply with the new validation rules, fields that do not contain valid phone numbers will not be updated.

For BlackBerry AtHoc versions 6.1.8.88 and earlier, you must continue to use 011 instead of + at the beginning of all international phone numbers.

BlackBerry AtHoc version 6.1.8.89 and later fully support the leading + method. Dialing 011 will continue to be supported after upgrade to 6.1.8.89 for organizations with a US country code since 001 is the US exit code.

Email format validation

An Emergency Mass Notification System is only as effective as the contact information it contains. For this reason, BlackBerry AtHoc validates that email addresses are RFC-5322 compliant in the following areas:

- End User Manager in the management system
- Self Service My Profile page
- Forgot Username
- Forgot Password
- .csv import
- User Sync Client
- AtHoc SDK
- Swagger

Email address syntax

The valid email address syntax is *local-part@domain*.

Local-part

The local-part of an email address can contain any of the following ASCII characters:

- Uppercase and lowercase Latin letters A to Z and a to z
- Digits 0 to 9
- The following printable characters: !#\$%&'*+,-/=/?^_`{|}~

The following guidelines apply to the local-part of a valid email address:

- The dot (.) character is allowed but cannot be the first or last character and cannot appear consecutively.
- Spaces are not allowed.
- The length is not validated.

Domain

The domain of an email address can contain any of the following ASCII characters:

- Uppercase and lowercase Latin letters A to Z and a to z
- Digits 0 to 9

The following guidelines apply to the domain of a valid email address:

- The domain must match the requirements for a hostname, and include a list of dot (.) separated DNS labels.
- The dot (.) character is allowed but cannot be the first or last character and cannot appear consecutively.
- No digits are allowed in the top-level domain (TLD). The TLD is the portion of the domain after the dot (.).
- The TLD must contain a minimum of 2 and a maximum of 9 characters.
- Spaces are not allowed.
- The length is not validated.

Valid email address examples

- simple@example.com

- very.common@example.com
- abc@example.co.uk
- disposable.style.email.with+symbol@example.com
- other.email-with-hyphen@example.com
- fully-qualified-domain@example.com
- user.name+tag+sorting@example.com
- example-indeed@strange-example.com
- example-indeed@strange-example.inininini
- 1234567890123456789012345678901234567890123456789012345678901234+x@example.com

Invalid email address examples

- Abc.example.com (No @ character.)
- A@b@c@example.com (Only one @ is allowed outside quotation marks.)
- a"b(c)d,e:f;g<h>i[j]\k]l@example.com (None of the special characters in the local-part are allowed.)
- just"not"right@example.com (Quoted strings are not supported.)
- this is"not\allowed@example.com (Spaces, quotes, and backslashes are not allowed.)
- this\ still\"notallowed@example.com

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

©2019 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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