BlackBerry AtHoc

Create and Publish Alerts

7.20

Contents

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 in the BlackBerry AtHoc management system or from the mobile app.

Enterprise Administrators can send alerts to users in their suborganizations. Enterprise Administrators, Organization Administrators, and any operator that has alert publishing permissions in a super enterprise organization can send alerts to users in their sub enterprises and suborganizations.

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

View the following quick action guides for simple steps to complete key tasks.

View all Quick Action Guides

- Create and publish an alert
- Send an alert with fill count
- Send an alert with escalation
- End a sent alert
- View alerts in the Inbox
- Create an alert template
- Organize your alert templates

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, recurring, or require approval in the system. This will help you avoid creating a duplicate alert.

1. Log in to the BlackBerry AtHoc management system as an operator with alert publishing permissions.
2. In the navigation bar, click **Alerts** > **New Alert**.
3. On the **Select from Alert Templates** screen, hover your cursor over an alert template name to view details about an alert template.
4. Do one of the following:
   - Quick Publish: In the **Ready to Publish** column, click **Publish...** beside an alert template.
   - Modify and publish: To modify the contents of any alert template, click **Edit**. On the alert details page, review and update the alert content. Click **Review and Publish**.
   - Approve and publish: To send an alert that requires approval, click **Edit**. Update the alert content and add target approvers. Click **Review**. For more information, see Publish an alert that requires approval.
5. Optionally, on the **Review and Publish** screen, do any of the following:
   - In the **Content** section, click ✎ to edit the Title or Body text. For more information, see Quick publish an alert
   - Click **Export to PDF** to export the content of the alert template to a PDF file. For more information, see Export an alert as a PDF.
   - Click **Preview and Publish** to preview how the alert will appear to end users. For more information, see Preview and publish an alert. This option is not available for bilingual alerts.
6. Click **Publish**.

Publish an alert that requires approval

Use the alert approval publishing flow when you need to have a second operator review, approve, and publish an alert. As an alert creator, select an alert template that is configured to require alert approval. Alert templates that require approval are indicated by a  . The alert creator enters the details of the alert, selects approvers, targeted users, targeted devices, and the timeframe for when the approval is required. A notification is sent to the alert approvers via email or the BlackBerry AtHoc desktop app. The alert approver notification includes a link that alert approvers can use to log in to the BlackBerry AtHoc management system and approve and publish the alert.

The alert approval publishing flow can only be used for alerts that are published manually by an operator. The following types of alerts do not support alert approval: External events, weather events, mobile app, IPAWS, and WEA.

Alert approval cannot be used to publish an alert that is being used in a Connect or weather alert rule, or in mobile alert settings.

The alert creator cannot also be an alert approver.

Alert approvers with userbase restrictions can publish alerts to a targeted userbase that is outside of their userbase.

An entry is added to the operator audit trail when a notification is sent to the alert approvers and when an alert approver approves and publishes the alert.

The following out-of-the-box templates cannot be used with an alert approval workflow:

Template type	Common name
Integrated Weather Alerts (IWS)	Weather Alert
Connect Invitation	INBOUND_CONNECT
External Events	Feed_Service_Template
Incoming Connect Alert	Inbound Standard
IPAWS COG-to-COG	IPAWS-Cog-Cog
Send Alert from SSA Map	SSA-END-USER-NOTIFICATION
New Alert Template	[NEW-ALERT-TEMPLATE]

Before you begin:

- IsAlertApprovalSupported must be enabled in Feature Enablement.
- The Alert Approval option must be selected in the Alert Template section of the alert template.
- Alert approvers must have an operator role that has alert publishing privileges, such as Alert Manager, Advanced Alert Manager, Alert Publisher, Advanced Alert Publisher, Enterprise Administrator or Organization Administrator.

Alert creator

To create an alert that requires approval and send a notification to the alert approvers, complete the following steps:

1. Log in to the BlackBerry AtHoc management system as an operator with alert publishing permissions.
2. In the navigation bar, click **Alerts** > **New Alert**.
3. On the **Select from Alert Templates** screen, select an alert template that has the **Alert Approval** option selected. Alert templates that require approval are indicated by a  .
4. Click **Edit**.
5. In the **Content** section, define the key parts of the alert: Severity, Type, Title, Body, Response Options, More Info Link, Location, and Attachments as needed. For details, see Define content for an alert or alert template.

   If placeholders are used in the **Title** or **Body** fields, the data is pulled from the initial alert from the creator, and not from when the approver publishes the alert. The alert approver can reapply the placeholders when approving and publishing the alert.
6. In the **Target Approvers** section, on the **By Individual Approvers** tab, click **Add/Remove Approvers**.
7. On the **Approvers** dialog, select between one and four approvers. Any operator who has a role with publishing permissions can be selected as an approver.
8. Click **Apply**.

   Devices listed on the Targeted Devices tab are used to contact the selected approvers. Only Desktop and Email devices are included. Any Desktop or Email devices that are enabled in your organization are automatically included.
9. In the **Approver Request** section, click **Edit**.
10. On the **Edit Message** dialog, update the **Title** and **Body** fields with information that your alert approvers should consider when approving and publishing the alert.
11. On the **Edit Message** dialog, in the **Time to Approve** field, enter the number of minutes, hours, or days that alert approval message is valid. The default is 30 minutes. The minimum time to approve is 15 minutes. The maximum time is 7 days. If the time to approve lapses before any approvers review and publish the alert, the alert remains in Sent Alerts with a Lapsed Approval status and a notification is sent to the alert creator and approvers.
12. Click **Apply**.
13. Click **Review**.
14. On the **Review before Approval** dialog, review the content of the alert.
15. Click **Send to Approver**.

The alert appears in Sent Alerts with an Approval Required status. An approver request message is sent to the selected approvers. The request message contains a link that opens the alert in the BlackBerry AtHoc management system. The alert approver can view the alert and make changes to the Title and Body, and add or remove targeted devices, but cannot make changes to any other sections before publishing.

Alert approver

When you receive a notification that an alert requires your approval, complete the following steps to approve, review, and publish the alert.

If you are logged in to the BlackBerry AtHoc management system, click the **Approval Required** link in the **Live Alerts** section of the home page to open the Sent Alerts page and view all alerts that require approval.

1. Click the **For more info** link in the email or BlackBerry AtHoc desktop app notification.
2. Log in to the BlackBerry AtHoc management system.
3. On the **Publish Alert** screen, review the information in the **Content** section and make any required changes.
4. Optionally, in the **Target Users** section, click the **Select Personal Devices** tab to add or remove devices.
5. Click **Review**.
6. On the **Approve and Publish** screen, click **Approve and Publish**.

The approved alert is published. The alert appears in Sent Alerts with a Live status. A notification is automatically sent out to the alert creator and all approvers notifying them that the alert has been published and no further action is needed.

Publish a blank alert

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.

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** > **New Alert**.
2. On the **Select from Alert Templates** screen, click **Create a Blank Alert**.
3. Define alert template details.
4. Define content for an alert or alert template.
5. Target users.
6. Click **Review and Publish**.
7. On the **Review and Publish** screen, review the content of the alert.
8. Optionally, click **Export to PDF** to export the content of the alert template to a PDF file.
9. Optionally, click **Preview and Publish** to preview how the alert content appears to end users.

   Note: This option is not available for bilingual alerts.
10. Click **Publish**.

Publish a geofence alert

Geofence targeting enables operators to target users who are part of a defined geo perimeter on the map. When geofence targeting is enabled, BlackBerry AtHoc looks for updates made to users' locations that match the geo perimeter selected in the alert. BlackBerry AtHoc sends an alert to users who are added to the targeted users for the alert.

User locations are updated when a user manually updates their address, performs a check-in on the mobile app, or when their location is updated by scheduled location access to the location defined in the geofence alert.

Geofence alerts are not limited to location-based targeting. Geofence alerts can also include other targeting methods such as targeting by user, by groups, or by advanced query. If there are updates made to users that match the targeting criteria in the geofence alert for other conditions except location, the new user still receives the alert.

In the alert summary, or in alert reports, there is no distinction between users targeted initially and new users who receive the alert when they enter the geo perimeter.

Limitation: Operator and distribution list user base restrictions apply for alerts that use geofence targeting. If a user enters the defined alert perimeter, and that user is outside the operator's user base, that user is not targeted.

For more information, see Enable geofence targeting.

Preview and publish an alert

On the Review and Publish page, you can access the preview screen to view how the alert will appear to end users. For Email devices, you can also modify the appearance of the alert.

1. On the **Review and Publish** screen, click **Preview and Publish**.
2. On the preview screen, in the **Original Content** section, review the title, body, response options, location, more info links, attachments, and targeted users, groups, and organizations in the original alert template content.
3. In the **Device Summary** section, review the selected devices. This section displays the percentage of targeted users that are reachable by each selected device. This section also displays any selected device delivery preferences and mass devices.
4. If Email is a targeted device, in the **Email Preview** section, review and edit how the email alert will appear to end users.
   - Optionally, select the **Include Map** option to include the selected location as a map in the alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map. This option is available only when a location is selected in the Content section.
   - Optionally, select a custom delivery template from the **Custom Template** pull-down menu. BlackBerry AtHoc provides default templates for each alert severity: High, Moderate, Low, Informational, and Unknown. By default, the custom delivery template associated with the selected alert severity is used.

     Note: If you select a custom template that your email delivery system does not support, the default template is used.
   - Optionally, click **Edit & Format**. On the **Edit & Format** dialog, use the text editing tools to modify the formatting of the title and body text. Click **Apply**.

   Your formatting updates are displayed in the **Email Preview** section.
5. Click **Publish**.

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** > **Sent Alerts**.
2. In the search field, type or paste a word or phrase found in the alert title.
3. Optionally, filter the alert list or sort the alert list.
4. Click **Search**.

Filter the alert list

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

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, click **Advanced** to open the advanced filtering options.
3. Select any of the following filters:
   - **Severity**: Select one or more severity levels: **High**, **Moderate**, **Low**, **Informational**, or **Unknown**.
   - **Publisher**: Select the name of an alert publisher.
   - **Start Date**: Select the beginning and end dates of a date range. The alert list then displays only those alerts that have a start date that falls within the specified range.
   - **Type**: Select types of alerts.
   - **Folder**: Select the name of a folder to limit the search to only alerts within that folder.
   - **Organization**: (Enterprise and super enterprise organizations only): Select one or more organizations. Organizations are displayed hierarchically, with suborganizations displayed beneath their enterprise organizations and sub enterprise organizations displayed beneath their super enterprise organizations. The Organization search filter is available only to Enterprise Administrators and System Administrators.
   - **Status**: Select from the following status options: **Select All**, **Ended**, **Draft**, **Scheduled**, **Live**, **Approval Required**, and **Lapsed Approval**. You can select multiple status values.
4. Optionally, to remove filters from the search, select and then deselect the **All** or **Any** option from the pull-down lists. To remove a **Date** filter, highlight the date in the field, then press **Delete**.
5. Click **Search**. The alert list displays all alerts that match the filter criteria.
6. Optionally, to remove a search filter, click the in the search pill.
7. Optionally, to remove all filters and return to the default alert list, click **Clear All** under the **Search** button.

Sort the alert list

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Click the column heading that you want to sort by. The alerts display in descending order of the values in the selected column.
3. Optionally, click the same column header again to sort in the opposite direction.

View a quick summary of an alert

The Sent Alert screen provides the following information about sent alerts:

- Alert title
- Alert ID
- Status: Live, Approval Required, Draft, Scheduled, Approval Lapsed, or Ended.
- Start time
- Publisher: The operator who published the alert.
- Targeted: The number of targeted users for the alert.
- Sent: The number of users the alert was sent to.
- Responded: The number of users who responded to the alert.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert that you want to view. You can also click a column header to sort the sent alerts list.
3. Hover your cursor over the title of the alert. A tooltip is displayed, providing the following information:
   - **Alert Title**
   - **Alert ID**
   - **Body**
   - **Severity**
   - **Type**
   - **Time Left**: This field appears only if the alert has a Live status.
   - **Response Options**: If the alert has a Scheduled or Draft status, 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.
   - **Time to Approve**: This field appears only if the alert requires approval. This field provides a countdown of the time remaining for an alert to be approved and published.
4. 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. The **Sent Details** section displays the number of targeted users. The **Response Details** section displays 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.

   Note: For an alert that is in an Approval Required status, the alert details page opens. You can edit the Content section, add or remove alert approvers, or resend the alert approver message.
5. Click the **Details** tab to view details of the content of the alert, including response options, severity, type, location, alert time and targeted users.

   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 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 edit 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.

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. Click to update the screen manually.

User responses are tracked every 30 seconds for the first 10 minutes of an alert. For the next 50 minutes, responses are tracked every 60 seconds. After one hour and until the alert ends, responses are tracked once every five minutes.

If you are not on the Review and Publish screen, you can view the alert summary for any live or ended alert from the Sent Alerts screen.

If you are logged in as an Enterprise Administrator to an enterprise or super enterprise organization, sent alerts from your sub enterprises and suborganizations are displayed.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert you want to view.
3. Optionally, click the name of an organization in the **Organization** column to view the organization hierarchy.
4. Click anywhere in an alert line to open the details screen for the alert.

The Alert Summary screen contains Details and Users tabs. When applicable, tabs for organizations and mass devices are displayed.

If the alert is live, there is an **End Alert** button on the Users tab that you can use to end the alert immediately. Click **Save** on the Details tab to save changes to the alert schedule.

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 belonging 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.

  Tip: To view phone error codes, see "Unified telephony tracking codes" in the *BlackBerry AtHoc Alert Tracking* guide.
- **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. If you are logged in to an enterprise organization as an Enterprise Administrator, you can send alerts to users targeted in alerts from your suborganizations. If you are logged in to a super enterprise organization as an Enterprise Administrator, you can send alerts to users targeted in alerts from your sub enterprise organizations and suborganizations.

  Note: This option is not available for alerts that are sent as part of an accountability event.
- **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 Users tab displays the possible alert response options, each assigned a different color. The total number of alert recipients who have selected that option is displayed beside each option. This information is also represented in a pie chart. Hover over the pie chart to display a tool tip that shows the number of users in each category. If dependents are enabled for your organization and in the alert template, the number of sponsors and dependents is displayed.

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

- **Export Delivery Summary (CSV)** : 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.

  Note: This option is not available for alerts that are sent as part of an accountability event.
- **User List**: Click this option to open a User Tracking Report. The report opens in a new browser window.

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 resend the alert 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 resend the alert.

Advanced Reports button

The Advanced Reports button takes you to the Report 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. Click the number to open a Users screen that displays the names and user details of each of the targeted users. The Target Users section also displays the Fill Count, if enabled, response options, targeted personal devices, and the device delivery preference (System defined, Organization defined, or User preferred.)

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. Click **Save** to save your changes.

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** > **Sent Alerts**.
2. Scroll to the bottom of the alert list.
3. Click the list that appears next to the phrase **items per page**.
4. 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 **Draft** or **Scheduled** status, you can edit any of the details.
- If the alert has a **Live** status, 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 an **Ended** status, you cannot make any changes to it.
- If the alert has an **Approval Required** status, you can edit the Content section, add or remove alert approvers, and resend the alert approver message.
- If the alert has an **Approval Lapsed** status, you can edit all sections in the alert. You can enter a new Time to Approve and resend the alert to be approved and published.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Use the search field or scroll down in the alerts table to locate the alert you want to edit.
3. Select the check box next to the alert name.
4. At the top of the screen, click the **More Actions** > **Edit**.
5. Make any changes you want to the unlocked fields.
6. 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** > **Alert Templates**.
2. On the **Alert Templates** screen, click **New**.
3. On the alert template details screen, in the **Alert Template** section, enter a name in the **Name** field.
4. Optionally, enter a description in the **Description** field.

   Note: 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. Select the alert folder that you want to add the alert template to from the **Folder** pull-down list.
7. (For enterprise and super enterprise organizations only.) Optionally, select the **Inheritable** option to make the alert template available to sub enterprises and suborganizations. For more information about alert template inheritance, see "Inherited content and settings in the enterprise or super enterprise" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.
8. Optionally, select **Available for Quick Publish** if you want to make the new alert template available through all quick publish links in the application.
9. Optionally, select **Available for mobile publishing** if you want to make the new alert template available for publishing from the mobile app.
10. Optionally, select **Alert Approval** to require that an operator who has been designated as an approver reviews and publishes any alert created from this template. For more information, see Target approvers.

    Note:

    - An alert template that is used in an alert rule cannot be used for alerts that require approval. Selecting the Alert Approval option on an alert template that is used in an alert rule will cause the alert template to not be in a ready state and the template will not be triggered when the alert rule conditions are met.
    - When Alert Approval is selected, the Available for Mobile Publishing option is not available.
11. When you are done, configure the Content section.

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 “Test” 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 that 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** field 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 that you can establish a delivery order for. 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 be published at a later date and time.
- 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 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.

Preview and publish (for email devices only)

- Use the Preview and Publish screen to preview how your alert will appear to end users.
- Use the text editing tools to customize the look and feel of your alert.

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: title, body, type, response options, website links, locations, and attachments.

1. To create an alert or alert template in a language other than the default language displayed on the screen, click the button beside the Type field and select a language. 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 a severity level from the list.

   Important: High severity is reserved for extreme emergencies. On the mobile app, it overrides the device sound settings to play 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. The maximum number of characters is 100. The title is required and displays at the top of the recipients' screen when the alert is sent out.
4. Optionally, to insert a placeholder into the alert or alert template title, click and select the placeholder from the list.

   Note: A space is automatically inserted before the placeholder to prevent text from running together when the alert is published.
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 **Custom Response Options** to view and select from a list of pre-set responses.
   - Click **Add Response Option** to define up to nine responses that alert recipients can send to let you know that they have received the message. To add a call bridge to a response option, see Configure a call bridge for a response option.

     Note: Targeted users in countries that have a provisioned SMS country code can respond to SMS alerts. Users in countries that do not have a provisioned country code cannot respond to SMS alerts.
8. Optionally, in the **Add Bilingual** section, click **Add**.

   a. On the **Translation Language** dialog, click **Change Language**.
   b. Select a language from the **Select Language** pull-down menu. The Title, Body, and Response Options are displayed in the original language on the left and in the selected language on the right.
   c. Review the translated text and make any necessary edits.
   d. Click **Apply**.

   For more information, see Add a bilingual alert.
9. Optionally, in the **More Info Link** field, enter a URL. For more information, see Use the More Info Link field.
10. If you entered a URL in the previous step, click **Test URL** to verify that the link works correctly.
11. Optionally, in the **Location** section, click **Add** to access a map where you can select a geographic area for the alert or alert template. For more information, see Select an alert or event location. This location can also be used to target users by location. For more information, see Target users by location.
12. Optionally, in the **Location** section, if you have selected a location, select **Enable Geofence Targeting** to target users who enter the location after the alert is sent. For more information, see Enable geofence targeting.
13. Optionally, in the **Attachments** section, drag and drop or click **Browse** to select files to include as attachments in the alert. For more information, see Add attachments.
14. Configure the Target users section.

Configure a call bridge for a response option

A call bridge is a type of alert response option for telephony devices consisting of a text response accompanied by a phone number. 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.

1. In the **Response Options** section, select the **Call Bridge** option beside a response option.
2. In the **Call Bridge #** field, enter the conference call number.
3. In the **Pass Code** field, enter the pass code users will use to dial in to the conference call. To add pauses before or in the middle of the code (for the operator to speak), add a comma for each second of pause time.

Use the More Info Link field

Use the **More Info Link** field in the Content section of an alert or alert template to include a URL in an alert.

The URL address must begin with one of the following:

- http:// – for standard web addresses
- https:// – for secured web addresses

You can include any of the following types of URLs:

- A URL that opens a webpage where users can get more details about the alert. When users receive the alert, a **For more info** link in 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.
- A URL that opens a webinar. The following delivery devices can connect with webinar URLs provided in the More Info Link field:
  - Desktop app
  - Mobile app
  - Email
  - SMS with Short URL
  - Connected organization alert template
  - Connected organization from the Inbox. The More Info link appears in the Inbox of the receiving Connect organization.
  - Forwarded alert from a receiving Connect organization. The More Info link is provided when forwarding the alert.

  Note: Phone devices and SMS devices without a short URL cannot connect to a webinar through a URL in the More Info Link field.

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 Settings and Configuration* guide.

After you enter a URL in the **More Info Link** field, click **Test URL** to verify that the link works correctly.

Add a bilingual alert

Operators can send an alert in two languages. The Bilingual Alert feature enables operators to send an alert in both an original language, and in a second language. Users can then choose a preferred language to receive alerts in.

The Bilingual Alerts feature does not support the following types of alerts:

- Connect rules
- Mobile events
- WAM
- BlackBerry Feed Service (BFS)
- IPAWS

Before you begin:

- The IsBilingualAlertSupported feature must be enabled by a System Administrator in **Settings** > **System Setup** > **Feature Enablement** for the super enterprise, enterprise, or suborganization.
- The **Add Bilingual** option must be enabled in the alert template in **Alert Template Settings** > **Content**.

1. In the **Content** section of an alert, in the **Add Bilingual** field, click **Add**.
2. On the **Translation Language** dialog, click **Change Language**.
3. Select a language from the **Select Language** pull-down menu. The title, body, and response options are displayed in the original language on the left and in the selected language on the right.
4. Review the translated text and make any necessary edits.
5. Click **Apply**.

After you finish: If you make any changes to the alert title, body, or response options, click **Edit** in the **Add Bilingual** field. On the **Translation Language** dialog, click **Refresh Translation** and then click **Apply**.

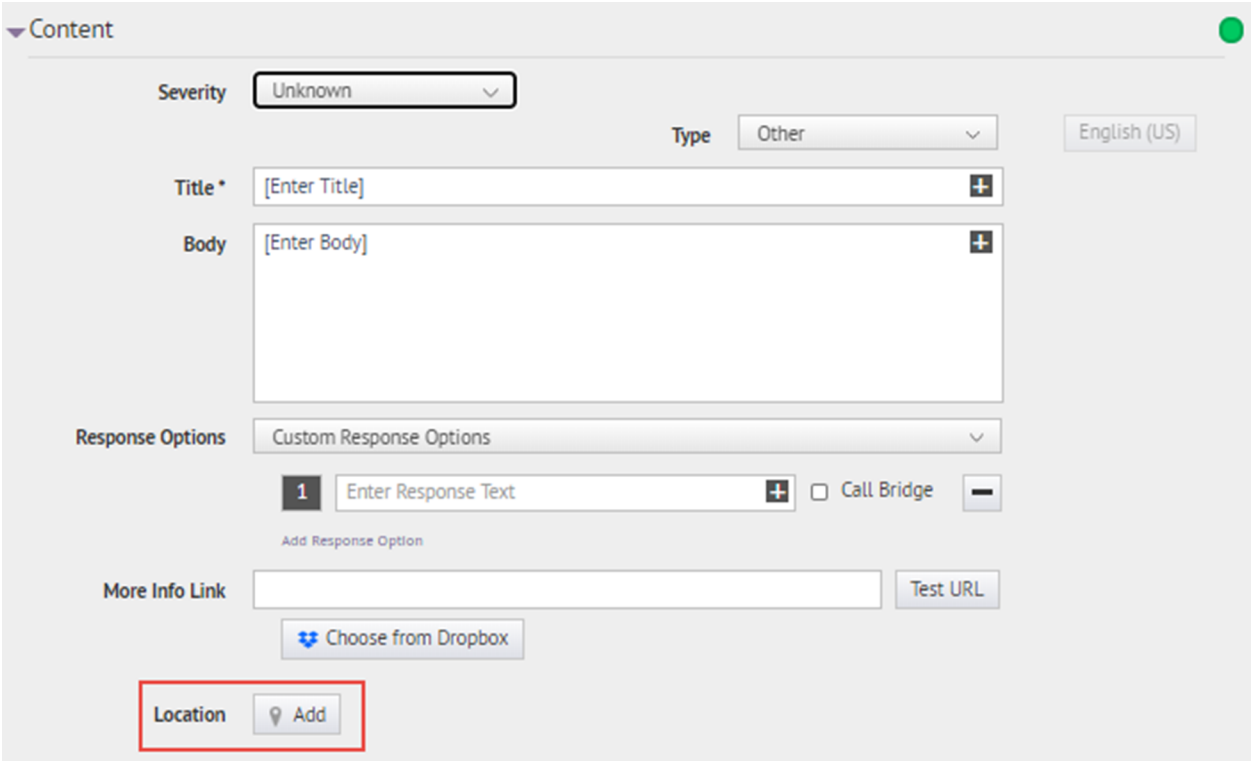
Select an alert or event location

There are two ways to add locations to an alert or event on the publisher map:

- Define custom locations using the drawing tools available on the map.
- Select geographic areas from a list of locations that were predefined by a BlackBerry AtHoc administrator.

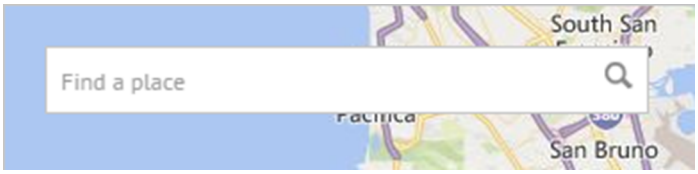
Users with any geolocation attribute in the selected location are targeted in the alert or event. In addition, any users with a Last Known Location attribute that was updated within the configured timeframe are also targeted.

1. In the **Content** section of an alert template, or in the **Event Details** section of an event template, click **Add** in the **Location** section. The publisher map opens.



Note: If you have the necessary permissions, you can set the default map area in the Map Settings screen. For more information, see Configuration and Setup.

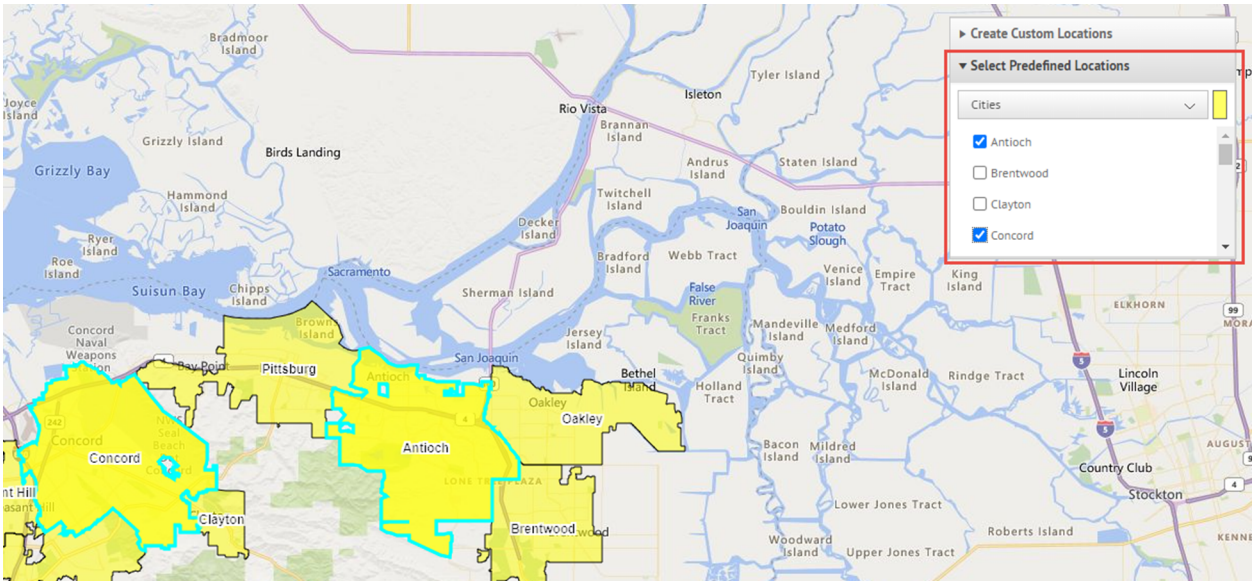
2. Optionally, if the location you want to target is not displayed on the current map, enter the address, point of interest, or longitude/latitude value pair in the **Find a place** field. Press **Enter** on your keyboard to refresh the map location.



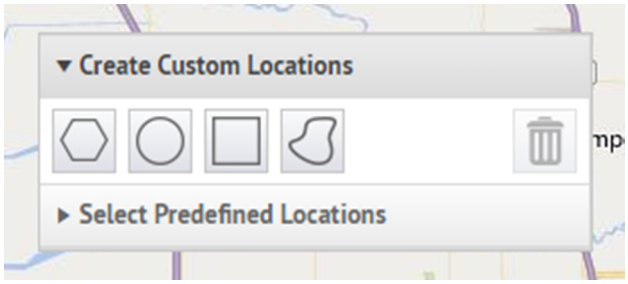
3. To use a predefined location on the map as a targeting criterion, click **Select Predefined Locations** to access a drop-down menu where you can select any predefined layers. When you select a layer, the map updates automatically to display the layer location on the map.

   Shape layers must be made selectable in the Map Settings. For more information, see Shape layers.

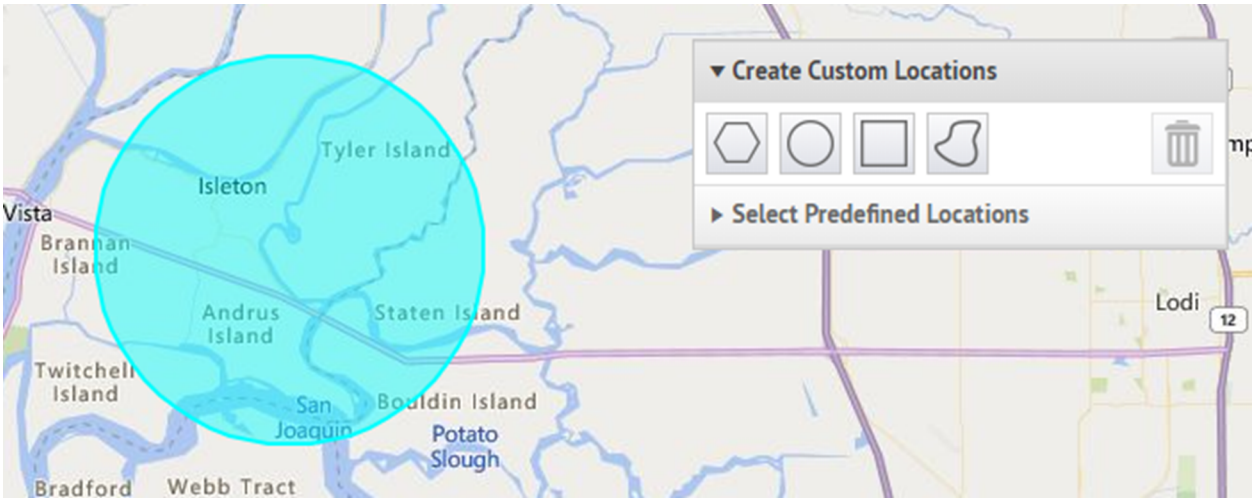
   Note: Uploading multiple layers with different sets of predefined locations is recommended to improve usability and system performance. Shape layers are configured on the Map Settings screen. Administrators can access them at **Settings** > **Basic** > **Map Settings**. For more information, see Shape layers.
4. Select one or more predefined locations within the layer by clicking them on the map or selecting them in the drop-down menu. As you make selections, the locations are highlighted on the map.



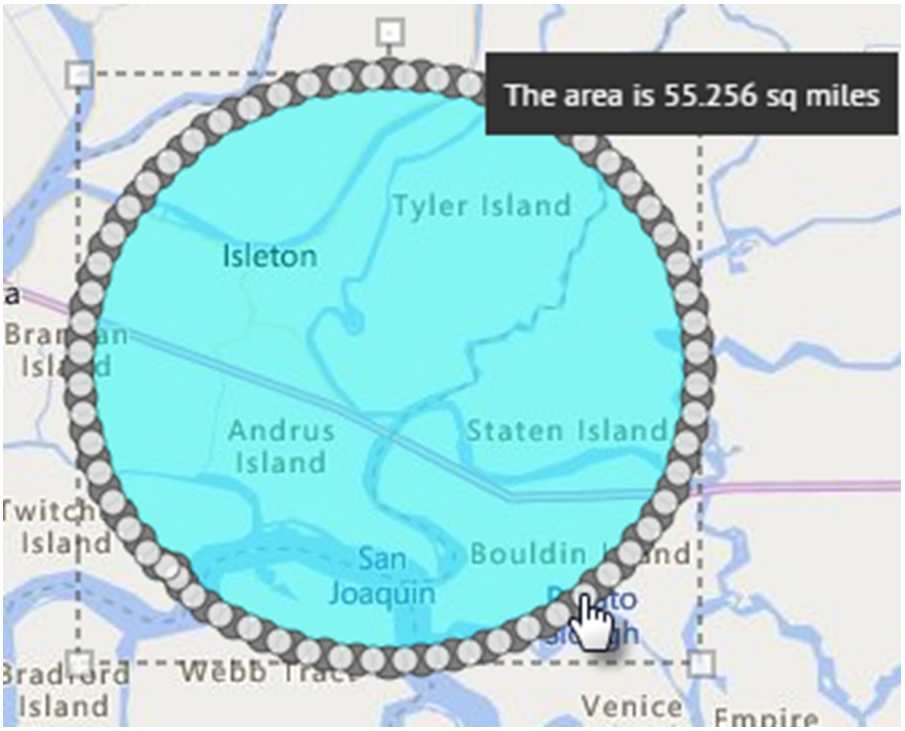
5. To create a custom location, click **Create Custom Locations** to display the drawing tools for creating shapes.



6. In the **Create Custom Locations** toolbar, select a shape and click and drag on the screen to select the location you want to use in the alert or event.

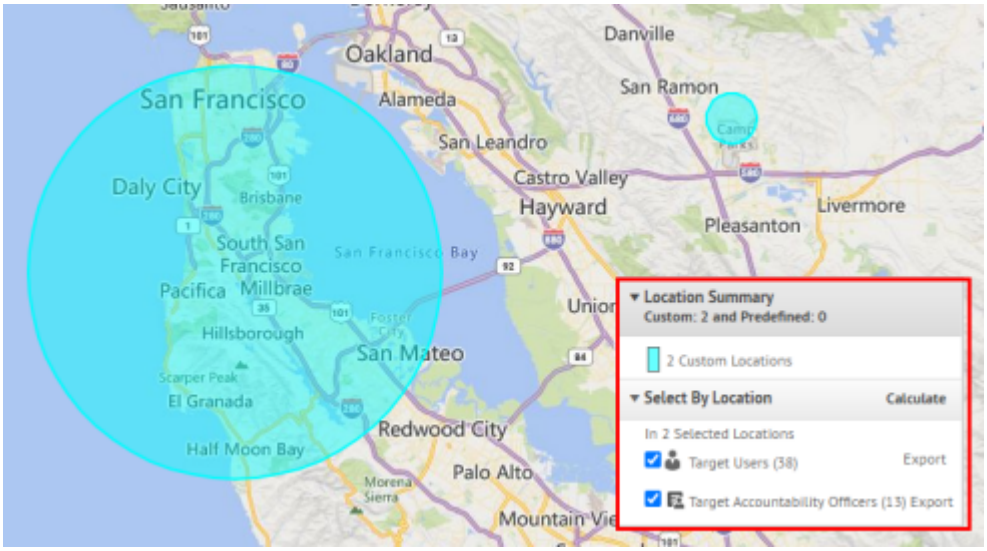


7. To view the size of a custom location, click the shape on the map. A black box appears beside the Create Custom Locations button, listing the total area of the custom location in square miles or square kilometers.



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.

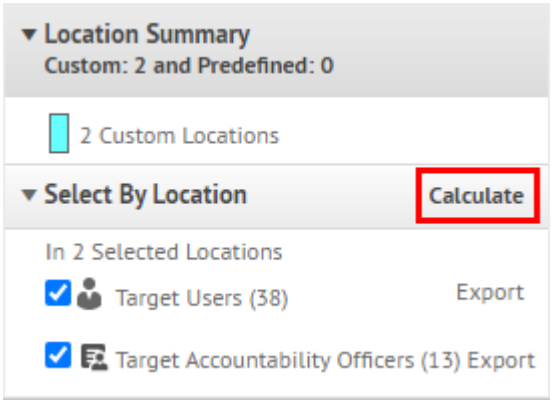
   As you create shapes and select predefined locations on the map, the **Location Summary** field in the bottom-right corner updates to provide you with an overview of the total number of locations that are displayed on the map and the locations that will be included in the alert or event.



10. To delete the custom locations you created, in the **Location Summary** section, click the **X** beside the custom locations. If you have created more than one custom location, they are combined in the list and cannot be

deleted individually. To delete a single custom location, click the border of the location shape on the map to select it, then click on the Create Custom Locations toolbar.

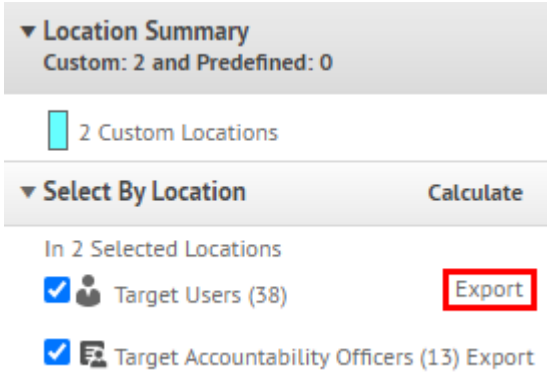
11. To view the total number of users, organizations, and Accountability Officers that are located within the selected map locations, click **Calculate** beside the **Select By Location** field.



Note:

- Users, Accountability Officers, and organizations listed in the Select By Location field are automatically added to the alert or event target list. To remove them as targets, deselect **Target Users**, **Target Organizations**, and **Target Accountability Officers**. For more information, see Target users by location.
- Accountability Officers are displayed on the map for accountability events only.

12. Optionally, in the **Select by Location** section, click **Export** to export the targeted users, organizations, or Accountability Officers.



   a. On the **Export Options** window, select the columns to export in the left column and click **Add**.
   b. Optionally, use the control buttons on the right to order the selected columns.
   c. Click **Export PDF** or **Export CSV**.

      Note: You can export up to 1000 users to a PDF file. You can export up to 25,000 users to a CSV file in a single export. If you are exporting more than 25,000 users to a CSV file, select a grouping of 25,000 users to export.

      The PDF or CSV file downloads to your system.
   d. Click **Cancel** to close the **Export Options** window.

13. Click **Apply**.

To target users with geofence targeting, see Enable geofence targeting.

For more information about the publisher map, see Manage the publisher map.

Add attachments

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. You can add a maximum of 5 files totaling up to 5 MB.

Important: Always use caution when including attachments in events and alerts. Alerts and events with a large number of targeted users and attachments will experience a significant delay in the expected delivery time. (The delivery time is the total time from when the operator sends the alert to when the last targeted user receives the alert). For example, if an alert with a 5 MB attachment is sent to 20,000 users, the expected delivery time is 2 hours. If additional alerts with attachments are also in the BlackBerry AtHoc system, the expected delivery time can increase significantly.

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, email, or in the Self Service inbox. Alerts received through the desktop app do not include attachments.

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, .bmp, .png, .gif)
- Audio and video files (.mp3, .mp4)
- Markup language files (.html, .xml, .kml)

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.

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

Enable geofence targeting

For more information about geofence alerts, see Publish a geofence alert.

Before you begin:

- The IsGeoFenceSupported feature must be enabled in **Settings** > **System Setup** > **Feature Enablement**.
- At least one predefined or custom perimeter must be selected on the map.
- The Location option must be selected on the Content tab of the alert template settings.
- The By Location option must be selected on the Target Users tab of the alert template settings.

1. In the **Content** section of an alert or alert template, in the **Location** section, click **Add**. The publisher map opens.
2. Do one of the following:
   a) Click **Create Custom Locations** to display the drawing tools for creating shapes. Click a shape button and then click and drag on the map to select the location you want to use in the alert or event. You can add multiple custom locations.
   b) Click **Select Predefined Locations**, and select any of the layers that have been created for you. When you select a layer, the map updates to display the layer location on the screen. Select one or more predefined locations in the layer by clicking them on the map or selecting them from the drop-down menu. As you make selections, the locations are highlighted on the map.

For more information, see Select an alert or event location.

3. Click **Apply**. The Targeting Summary section updates to display the total number of locations on the map that will be used to target recipients.
4. In the **Location** section, select the **Enable Geofence Targeting** option.
5. In the **Target Users** section, click **By Advanced Query**. By default, users who have a location attribute in the selected locations and who have a Last Known Location attribute updated within the last 4 hours are targeted.
6. Optionally, click **map selection(s)** to change the selected locations.
7. Optionally, enter a number and select **Minute(s)**, **Hour(s)**, or **Day(s)** to change the timeframe for the Last Known Location attribute.
8. Optionally, in the **Targeting Summary** section, click the number beside **By Location** to open a map that shows the targeted locations.
9. Select personal devices for an alert or alert template.
10. Click **Review and Publish**. The following message is displayed: You have selected geofence targeting. All users entering the selected locations will be added to the targeted user base.

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 **create an account** 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.

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 check box type. Use the single-select picklist type when you want to customize the response options. Use the check box 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: Single-select picklist, and status attributes can have a maximum of 9 values when used as response options.

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. Click **Users** > **User Attributes**.
3. On the **User Attributes** screen, click **New** > **Single-select Picklist**. If you require only a "Yes" or "No" response, select **New** > **Checkbox**.

   Note: Single-select Picklist attributes can have a maximum of 9 values when used as response options.
4. In the **Basic** section, in the **Name** field, enter a name for the attribute.
5. In the **Basic** section, select **Use as a Response Option**.
6. For a Single-select Picklist attribute, in the **Values** section, add the response options for each picklist option. The recommended number of response options is 3 to 5. The maximum number of response options is nine.
7. In the **Page Layout** section, leave all drop-down lists set to **Do not show**.

8. 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.
9. 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 8, 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 8. 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 approvers

Select target approvers when you require an approval workflow before sending out an alert. When the Alert Approval option is selected in an alert template, a target approver must review and publish the alert. Alert approvers with userbase restrictions can publish alerts to a targeted userbase that is outside of their userbase.

The alert creator cannot also be an alert approver.

1. In the **Target Approvers** section, on the **By Individual Approvers** tab, click **Add/Remove Approvers**.
2. On the **Approvers** dialog, select between one and four approvers. Any operator who has a role with publishing permissions can be selected as an approver.
3. Click **Apply**.

   Devices listed on the Targeted Devices tab are used to contact the selected approvers. Only Desktop and Email devices are included. Any Desktop or Email devices that are enabled in the organization are automatically included.
4. In the **Approver Request** section, click **Edit**.
5. On the **Edit Message** dialog, update the **Title** and **Body** fields with information that your alert approvers should consider when approving and publishing the alert.
6. On the **Edit Message** dialog, in the **Time to Approve** field, enter the number of minutes, hours, or days that alert approval message is valid. The default is 30 minutes. The minimum time to approve is 15 minutes. The maximum time is 7 days. If the time to approve ends before any approvers review and publish the alert, the alert remains in Sent Alerts in a Lapsed Approval state and a notification is sent to the alert creator and approvers.
7. Click **Apply**.
8. Click **Review**.
9. On the **Review before Approval** dialog, review the content of the alert.
10. Click **Send to Approver**.

The alert appears in Sent Alerts with an Approval Required status. An approver request message is sent to the selected approvers. The request message contains a link that opens the alert in the BlackBerry AtHoc management system. The alert approver can view the alert and make changes to the Title and Body, and add or remove targeted devices, but cannot make changes to any other sections before publishing.

Target users

Use the Target Users section to identify the users you want to send an alert to or block from receiving an 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.

If you are an Enterprise Administrator, you can target users in your suborganizations. If you are an Enterprise Administrator logged in to a super enterprise organization, you can target users in your sub enterprises and suborganizations.

Targeting basics

The following general targeting information can be used to plan how to 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, see Target groups in alerts or alert templates. You can also block groups from receiving the alert. For more information, see Block groups and distribution lists from receiving a notification.
  - **By Users**: Target individual users. You can also target dependents of sponsor users. Operators can also block specific individuals within a group from receiving the alert. For more information, see Block a user from receiving a notification.
  - **By Advanced Query**: Target users based on standard or user attributes or delivery devices. Select this option to perform customized targeting for an alert. For more information, see Target or block users by advanced query.
  - **By Location**: Target users based on their geographical location. For more information, see 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.
- 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. You can also 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.
- Enterprise Administrators can target users in the enterprise or any suborganization. Enterprise Administrators logged in to a super enterprise organization can target users in their sub enterprises and suborganizations.

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 targeted.

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 *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 Geolocation.
  - (Recommended) For escalations, you should 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. On the **Fill Count and Escalation** window, 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.
4. Optionally, select the **Enable Escalation** option 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 you want to deliver the alert to. If the attribute is a picklist, ensure that the sort order is correct.
6. Specify the **Escalate Priority** 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 users will be alerted in, click the number next to Total Users in the **Targeting Summary** section. 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 or 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 also automatically selected. Click the check box next to a selected sub group or sub distribution list name to deselect it. If you select all 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 are selected and some are not.

Block groups and distribution lists from receiving an alert

You can block groups (organizations or distribution lists) from receiving an alert on the By Groups tab in the Target Users section.

1. In the **Target Users** section, click **By Groups**.
2. In the **Groups** field, click **Block** beside each group or distribution list that you want to block.

   Note: Even if a top-level group or distribution list is selected for inclusion, you can still block a sub group or sub distribution list 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.

   When you block a group or distribution list, the Block link changes to an Unblock link and a  appears beside its name.
3. To unblock a group or distribution list, click **Unblock** beside its name.

Note: If you block a group or distribution list that contains sub groups or sub distribution lists, those are also automatically blocked. To unblock any of the sub groups or sub distribution lists, you must manually unblock the parent group or distribution list first. 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

Use the By Users tab in the Target Users section to target individual users.

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. Click **Block** in the row for any user you want to block from receiving the alert.

   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. The total number of targeted and blocked users appears below the search field.

   Tip: Click the name of an organization in the Organization column to view a user's organization hierarchy.
4. Click **Apply**. The users you added are displayed in the Users field with a ✔ beside their name. Blocked users appear with a ⊘.

   Note: To remove a targeted user from the alert recipient list, click ✖ beside 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 Target Users 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

Subscribed users can be targeted in alerts on their subscribed organization when:

- The organization subscription feature is enabled
- Organizations are enabled for subscription
- Users are subscribed to enabled organizations

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.

When the organization subscription feature is enabled on a super enterprise organization, Enterprise Administrators can target subscribed users in their sub enterprises and suborganizations.

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, select the **equals** operator. In the field that appears, select your organization.
4. Optionally, in the **Targeting Summary** section, click the number beside 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 an alert

You can 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 targeted 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** beside 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 beside their name.
4. Click **Apply**.

The Users screen reappears, displaying the names of the users you blocked with ⊘ beside their name.

Target or block users by advanced query

You can target or block users based on general attributes, organization hierarchies, geolocation, operator attributes, or device types.

Prerequisite: The **By Advanced Query** option must be enabled on the **Target Users** tab in the alert template settings.

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

   Note: If you have added a location in the Content section, the **All geolocations inside map selection(s) plus Last Known Location update** option is selected by default.
2. Select the AND/OR operator. When AND is selected, users must meet all conditions to be targeted in the alert. When OR is selected, users that match any of the search conditions are targeted. The default is AND.
3. Click **Add Condition**.
4. In the **Select Attribute** list, select the first attribute, organization hierarchy, geolocation, operator attribute, or device you want to use as targeting criteria.
5. 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 operation such as **not equals** or **does not contain**.

   Note: The list of operations varies depending on the type of attribute selected.
6. If the operation you selected in Step 5 requires additional query values, a third field appears. Enter or select a value for the attribute.

Tip: For multi-select picklist, single-select picklist, geo-aware multi-select picklist, and status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.

7. Optionally, click **Add Condition** and then repeat steps 3 through 6 for each additional condition you want to add.

   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.

   Tip: You can target or block users based on the User Last Updated Source attribute. For details, see Target or block users with the User Last Updated Source attribute.
8. Optionally, click the number in the **By Advanced Query** field in the **Targeting Summary** section to view the advanced query criteria.
9. 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 ⛔ beside a condition to remove it.

Target or block users with the User Last Updated Source attribute

Operators can target or block users based on the source that last updated the users' profiles. The following table lists the possible sources and the search terms required to target users by source.

Source	Search term
Mobile app	• Check-in • Check-out • Report • Emergency • User Tracking - Mobile App • Mobile
Self Service	SelfService
BlackBerry AtHoc Management System	ManagementSystem
User Sync Client	UserSyncClient
API	API
CSV Import	UserImport
Targeted Device	• Alert Tracking - Desktop Popup • Alert Tracking - Email • Alert Tracking - Mobile App • Alert Tracking - Phone • Alert Tracking - Text Messaging

1. In the **Target Users** section, click **By Advanced Query**.
2. Select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
3. Click **Add Condition**.

4. From the **Select Attribute** list, select **User Last Updated Source**.
5. Select an operation from the **Select Operation** list.
6. In the blank field that appears, enter the source that you want to target users by. The text you enter in this field must match one of the search terms listed in the table above. You can add more than one source, separated by a comma. For example, API, UserSyncClient.

Target users by role

1. In the **Target Users** section, click **By Advanced Query**.
2. Optionally, select the AND/OR operator. When AND is selected, users must meet all conditions to be targeted in the alert. When OR is selected, users that match any of the search conditions are targeted. The default is AND.
3. Click **Add Condition**.
4. In the **Select Attribute** list, scroll down to the **Operator Attribute** section and select **Roles**.
5. In the **Select Operation** field, select a query operation.
6. In the third field that appears, select the role or roles that you want to use as search criteria.

   Note: Roles associated with features that are not enabled in the organization do not appear. For more information, see "BlackBerry AtHoc roles" in the *BlackBerry AtHoc Operator Roles and Permissions* guide.

   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 **By Advanced Query** field to view a pop-up screen that lists the operator roles you have selected as targeting criteria for the alert.

Target users by location

You can target users by selecting locations on a map. Users with any geolocation attribute in the selected locations are targeted in the alert or event. In addition, any users with a Last Known Location attribute that was updated within the selected timeframe are also targeted by default.

1. In the **Content** section of an alert or alert template, in the **Location** section, click **Add**. The publisher map opens.
2. On the map, do one of the following:

   - Click **Create Custom Locations** to display the drawing tools for creating shapes. Click a shape button and then click and drag on the map to select the location you want to use in the alert or event. You can add multiple custom locations.
   - Click **Select Predefined Locations**, and select any of the layers that have been created for you. When you select a layer, the map updates to display the layer location on the screen. Select one or more predefined locations in the layer by clicking them on the map or selecting them from the drop-down menu. As you make selections, the locations are highlighted on the map.

   For more information, see Select an alert or event location.
3. Click **Apply**. The Targeting Summary section updates to display the total number of locations on the map that will be used to target recipients.
4. In the **Target Users** section, click **By Advanced Query**. By default, users who have a location attribute in the selected locations and who have a Last Known Location attribute updated within the last 4 hours are targeted.
5. Optionally, select an AND/OR operator. AND is selected by default.
6. Optionally, click **map selection(s)** to change the selected locations.

7. Optionally, enter a number and select **Minute(s)**, **Hour(s)**, or **Day(s)** to change the timeframe for the Last Known Location attribute.
8. Optionally, in the **Targeting Summary** section, click the number beside **By Location** to open a map that shows the targeted locations.

Note: To target users with geofence targeting, see Enable geofence targeting.

For more information about the publisher map, see Manage the publisher map.

Review the targeting summary

The Targeting Summary section of the Target Users section displays 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.

Click the numbered links in the Targeting Summary field to open a pop-up 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 the organizational hierarchies and 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 the organizational hierarchies and distribution lists that have been excluded from the alert. If all sub groups or sub distribution lists of a parent have been blocked manually, the parent is not also blocked by default. The parent can only be blocked by manually selecting it for blocking.

By Users

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

By Users-Blocked

The By Users-Blocked screen lists 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 are 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 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 beside 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 available personal devices appears, including the percentage of selected users who can be reached by each device type.
2. Select the check box beside each personal device you want to include. As you select devices, the pie chart in the Targeting Summary section updates to show the number of reachable and unreachable users based on your current selections.
3. Optionally, click the number beside the **Total Users** field to view a screen that displays the username and organizational hierarchy for the users in the target group.
4. Optionally, click the numbers in the **Reachable Users** and **Unreachable Users** fields to view separate pop-up screens that provide user details for those groups.

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.

1. In the **Target Users** field, click **Select Personal Devices**.
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 device 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	Description
Desktop Popup	App Template	• 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 severity: High, Moderate, Low, Informational, and 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 **Preview** to preview the custom template. **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.
	App Audio	• 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	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 (for non-bilingual alerts)	—	The device options for Email devices are set on the preview screen. For more information, see Preview and publish an alert.
Email (for bilingual alerts)	Email Template	Specify the email template, either the default template or a custom template. BlackBerry AtHoc provides default templates for each severity: High, Moderate, Low, Informational, and Forgot Password. **Note:** If you select a custom template and your email delivery system does not support it, the default template is used.
	Email Message Content	• 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.

Device Type	Options	Description
	Map Image in Alert	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.
Text Messaging	Content Sent Via Text	• Select **Alert Title and Body (Short)** to use the first 1250 characters of the alert title and body as the text message content. The text message content is truncated at the first space before the 1250th character. If the content is truncated, the text message includes a link users can click to view the complete alert text. This is the default option. • 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. The maximum is 1250 characters. • 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 *How does AtHoc SMS support sending text messages to countries abroad?* on the BlackBerry AtHoc customer support site.
Pager	Content	• 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	• 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	• 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	Description
	Audio Broadcast	• 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 can specify the number of times to replay the alert. • Select **Audio - Title Only** if you want the alert title to play when the alert is received. If you select this option, you can specify the number of times to replay the alert. • Select **Audio - Body Only** if you want the alert body to play when the alert is received. If you select this option, you can specify the number of times to replay the alert. • Select **Custom** if you want to enter custom text for the alert. If you select this option, you can specify the number of times to replay the alert.
Phone	Phone Message Content	• 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	Select what happens after the recipient answers the call: • Deliver alert without any authentication. • Deliver alert only after the provided PIN is entered. • Deliver alert only after user validation.

Device Type	Options	Description
	Recipient Does Not Answer the Call	Select what happens if the call is not answered: • Deliver alert as voice mail. **Note:** If the Severity of an alert is changed to Moderate or High, this option is removed and the "Leave callback information" option is applied instead. • Leave callback information in the voicemail. **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. • 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	Select the criteria that stop calls from being made to the alert recipient: • Recipient acknowledged the message. • Recipient listened to entire message. • Entire message left on voicemail.
	Call Attempts	Enter the number of attempts the system makes 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	Description

BlackBerry AtHoc Mobile App	Repeat Notification	Each alert is only sent once. This option specifies if and how often notifications about the alert are repeated on a mobile device.
		• **None**: Send the alert notification once.
		• **Default**: Use the default time that has been defined for the selected severity.
		  • For **High** severity alerts, the default is one notification a minute for 10 minutes.
		  • For **Moderate**, **Low**, **Informational**, or **Unknown** severity alerts, the default is one notification a minute for 2 minutes.
		• **Custom** :
		  • Select how long to repeat the notification if the user does not respond.
		  • Select how long to pause between each repetition.
		  Note: Ensure that the pause time is smaller than the repetition timeframe. For example, if you 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.
		Alert notifications repeat until one of the following actions occur:
		• The recipient responds to the alert from any of the mobile apps on which the same recipient is registered. Responses sent from other devices such as email, phone, or SMS, do not stop the notification.
		• The defined timeframe for repeat notifications elapses.
		• The alert ends.

	Deliver Alert with Sound	• 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 check boxes beside the phone devices to use as targeting methods.
3. Click **Options**.
4. On the **Personal Devices Options** screen, 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 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 beside the phone devices to use as targeting methods.
3. Click **Options**.
4. On the **Personal Devices 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** section, click **Select Personal Devices**.
2. In the **Personal Devices** field, select **Desktop App**.

3. Click **Options**.
4. On the **Personal Devices Options** screen, click **Desktop Popup**.
5. In the **App Template** field, select **Use Custom Template**.
6. Select the desktop template you want to use for the alert.
7. Click **Preview**.

   Note: A preview of the template appears on the screen.
8. To preview the audio component of the alert, in the **App Audio** field, select **Use Custom Audio**. Select an audio file from the list and then click ▶.

Select the device delivery preference

Device delivery preference must be enabled in **Settings** > **Feature Enablement**. When device delivery preference is enabled, devices selected in the order configured by the organization or in the default order and default interval are used. If the desktop app is an enabled device in the organization, it is first in priority.

After selecting the personal devices to use to contact users, the operator selects the delivery method and can choose between organization-defined, system-defined, or user-preferred device delivery preference to use to contact users. This selection applies to personal devices only. The default selection is system-defined.

When the device delivery preference is system-defined, all devices are targeted almost simultaneously. The alert is sent to the users targeted in the alert on all of their enabled devices at the same time. Phones can be set in a delivery order.

When the device delivery preference is user-preferred, the user defined sequence, configured in either the BlackBerry AtHoc management system or in Self Service, is applied.

When device delivery preference is enabled, and the alert publisher selects Device Delivery Preference as organization-defined or user-preferred, on the Alert Publish page, BlackBerry AtHoc performs redundant message stop. End users targeted in the alert receive the alert on their enabled devices in the specified sequence and interval. Once a user responds to the alert on a higher priority device, they should not receive the alert on any additional enabled devices. The alert must contain response options for redundant message stop to work. Messages do not stop until the user responds with a response option.

Note: Users may receive an alert on their next device if BlackBerry AtHoc did not receive their response before sending the alert to the user's next device. Users will also receive alerts on additional devices when an alert does not have a response option that the user can respond to.

Note: If a high severity alert is received on the mobile app and audio tones are used, only a response from the mobile app will stop the mobile app audio. Responding on another device does stop the audio once the alert has been received on the mobile app.

Before you begin:

- Device delivery preference must be enabled for your organization.
- Device delivery priority and delay must be configured in **Settings** > **Devices**.

1. In the **Target Users** section, click **Device Delivery Preference**.
2. Select **System defined**, **Organization defined**, or **User preferred**. The operator does not see the order or interval when sending the alert.

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 you want to add organizations to.
2. In the **Target Organizations** section, select each organization you want to target 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 beside 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. Click **Apply**.

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, click **Preview and Publish** to preview how the alert will appear to end users. On the preview page, you can review the original content, and a summary of the targeted devices. For Email devices, you can choose a delivery template and use the text editing tools to format the alert title and body text.
3. Optionally, to make changes to any part of the alert, click **Cancel**. The edit alert screen appears. Make and save your changes.
4. When you are satisfied with the alert content, click **Publish** to send the alert.

The Alert Summary screen appears, displaying the alert details and targeting information. Click the **Advanced Reports** button 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. When you test the alert, it is sent only to you.

1. In the navigation bar, click **Alerts** > **New Alert**.
2. On the **Select from Alert Templates** screen, click **Edit** for the alert you want to test.
3. On the alert details screen, click **Test Alert**. The Test Alert window opens with your available enabled devices selected or a test box to add a device. You can deselect any device you don't want to receive the test alert on.
4. In the **Test Alert** window, click **Test Alert**.

The Test Alert screen closes and a confirmation notification appears at the top of the alert details screen. The test alert is sent to your selected devices.

Set an alert to draft mode

Alerts are sometimes created in advance or created by operators 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 the details of the alert. The draft alert is saved in the Sent Alerts screen as a draft.

1. Create the alert.
2. Click **Draft** at the top of the screen.

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

Publish a draft alert

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert to publish.
3. Select the check box beside the alert name.
4. Click **More Actions** > **Publish**.
5. On the **Review and Publish** screen, review all sections of the alert.
6. Optionally, if you need to make any changes:
   a. Click **Edit** at the bottom of the screen.
   b. On the alert details screen, make any needed changes.
   c. Click **Save**.
   d. When you are satisfied with the alert content, click **Review and Publish**.
7. Optionally, on the **Review and Publish** screen, click **Preview and Publish** to preview how the alert will appear to end users.
8. Click **Publish**.
9. Optionally, click **Alert Summary** to go to the alert details page.

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 on the BlackBerry AtHoc management system 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. On the **Review and Publish** page, click .
3. On the **Edit Title and Body** window, update 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 enables an operator to customize the targets when resending an alert. The operator can resend the alert to all original recipients, to recipients who responded to the original alert, or to recipients who did not respond to, or did not receive, the original alert.

If you are logged in to an enterprise organization as an Enterprise Administrator, you can resend alerts that were originally sent by your suborganizations. Alerts resent from an enterprise organization are published from the enterprise.

If you are logged in to a super enterprise organization as an Enterprise Administrator, you can resend alerts that were sent from any sub enterprise or suborganization. Alerts resent from a super enterprise organization are published from the super enterprise. Fill count is not supported for alerts that are resent from a super enterprise organization. Alerts resent from a super enterprise organization can only be targeted to devices that are supported on the super enterprise, the sub enterprise, and suborganization.

The Resend feature is not available for alerts that are sent as part of an accountability event. These alerts are indicated on the Sent Alerts screen with a  .

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, click the alert that you want to resend.
3. On the alert details screen, click the **Users** tab.
4. In the **Sent Details** section, click the drop-down menu in the **Targeted**, **Sent**, or **In Progress or Failed** row.
5. Select **Send Alert to These Users**.
6. Optionally, on the alert details page, update the details of the alert.
7. Click **Review and Publish**.
8. Optionally, on the **Review and Publish** screen, click **Preview and Publish** to preview the alert.
9. 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 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** > **Sent Alerts**.
2. Click a live or ended alert.
3. On the alert details screen, click **Advanced Reports**.
4. In the **Report** section, select a report from the **Select a Report** list.
5. 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** > **Sent Alerts**.
2. Click a live alert or ended alert.
3. Click the **Users** tab.
4. Do one of the following:
   - 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.
   - 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.
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.

Report name	Description
Delivery Distribution by Devices	Displays a tabular report that tracks the number of targeted alerts, the number of alerts sent, and the number of responses received for each device used. The report can include all devices or only the devices used for targeted recipients. You can click any user count in the report, such as the number of targeted users, to open a detailed user tracking report that identifies individual users and provides their names, device addresses, and responses. This information is useful for evaluating the effectiveness of the delivery devices used for the alert. **Note:** If device delivery preference is set to Organization defined, the number in the Sent column of the report is updated incrementally as different personal devices are targeted.
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 an 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** > **Sent Alerts**.
     a. On the **Sent Alerts** screen, click the live or ended alert you want to see lifecycle results for.
     b. Click **Advanced Reports**.
2. On the report screen, 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 a subset of a 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.

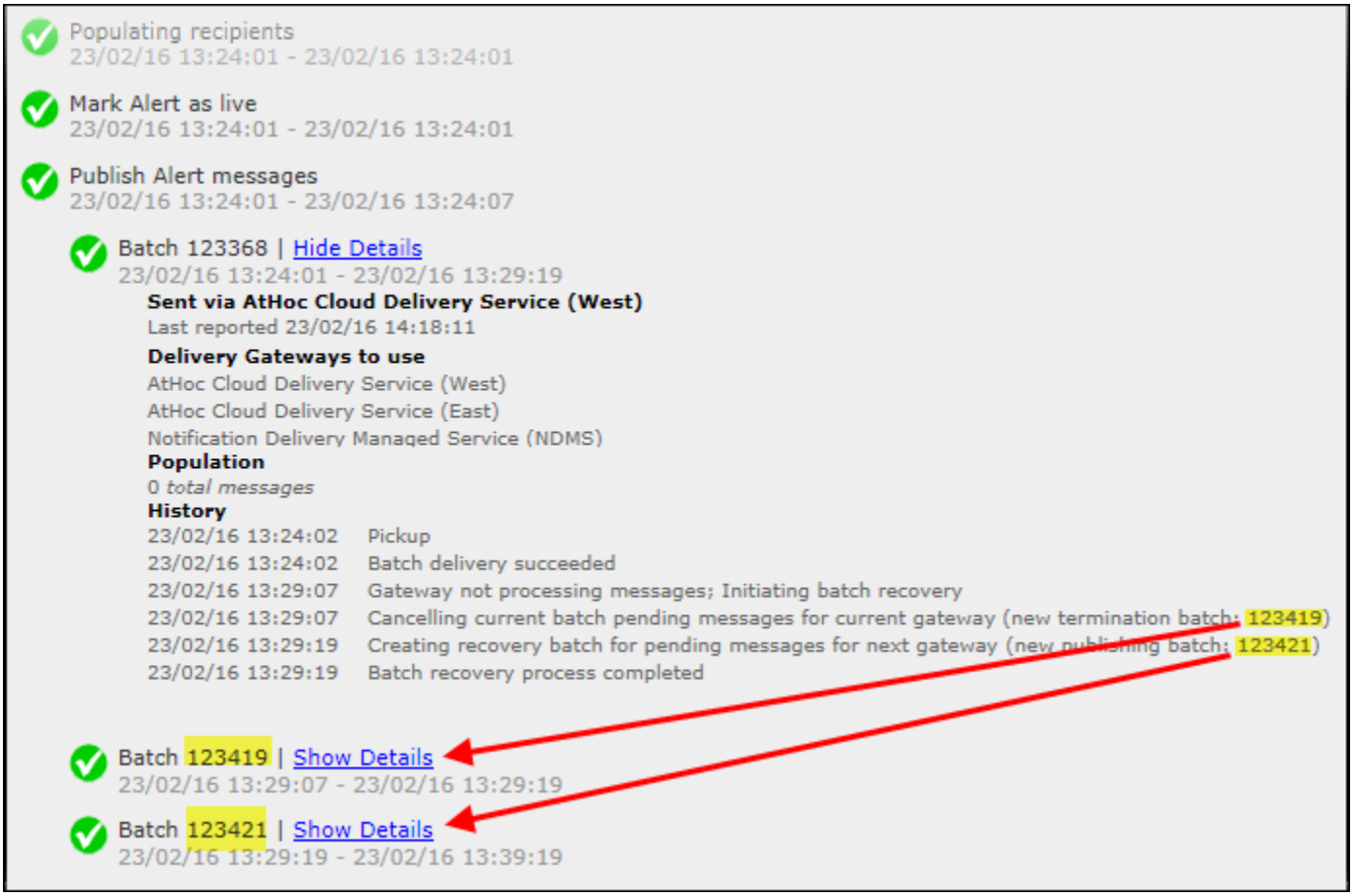
After a specified time (the default is five minutes), BlackBerry AtHoc resends any alert that was not sent or does not have a response. Users that have responded to the alert do not receive another alert.

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. 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.



As you can see, the initial alert batch was 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.

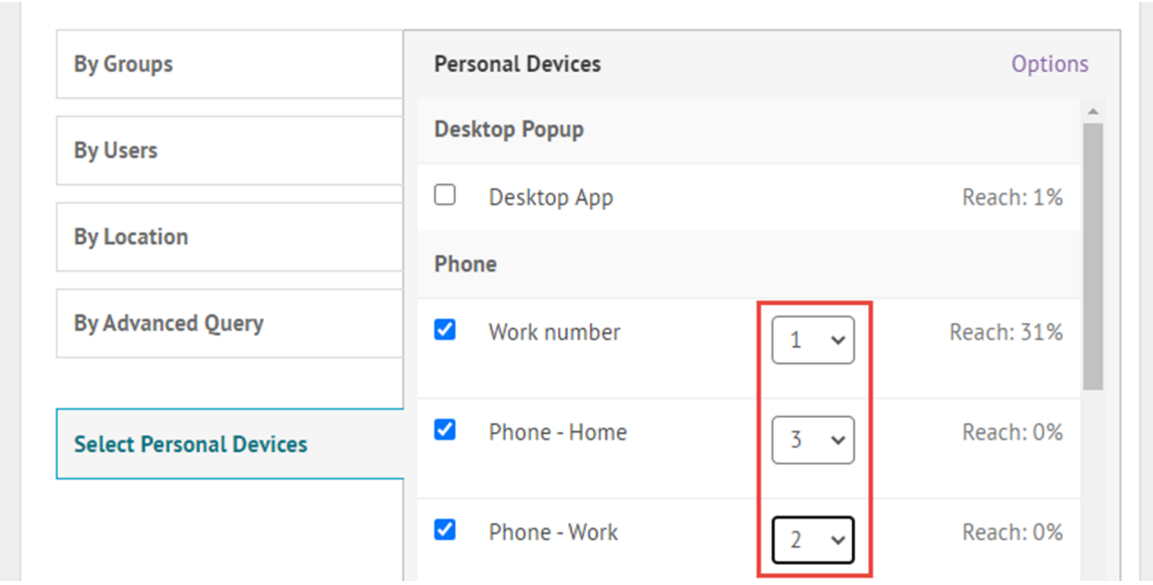
Message termination

The BlackBerry AtHoc management system performs message termination (also known as call termination) on hosted telephone devices for users with multiple targeted phones. Message termination is enabled by default. Message termination is not performed for other devices such as email, SMS, or the mobile app.

When a user has multiple phone numbers in the system, and those numbers are all targeted, when the user responds from one number, they should not receive the alert on any other phone numbers. The operator must select the order of the phones, or they are all listed as priority 1 and the alert is sent to all phones at the same time. The alert must contain response options so that the user can respond and prevent the alert from being sent to their additional phone devices.

The number of users and phone numbers targeted in an alert may impact the user experience of message termination. For example, if an alert is sent to a small group of users, they may not have enough time to respond to the alert on their first targeted phone before the system sends the alert out to the second group of phone numbers.

To specify the call order, operators should set the preference order for phone devices when selecting them for targeting in an alert.



The Stop Calling Options for phones set in the Personal Devices Options in an alert also impact message termination. If an operator selects the “Recipient listened to the entire message” or “Entire Message left on Voicemail” stop calling option, the delivery preference continues until one of the devices is used to respond to an alert. These phone options, designed to stop phone calls if the user listens to the message or has the message left on their voicemail, do not function with device delivery preference. Phone calls continue in the order of the delivery preference, and users continue to receive phone calls, even if the operator selects these options. The user must respond to the alert to stop alerts from being sent to their additional devices. Ensure that the **Requires Acknowledgment** option is selected in the Personal Devices Options for phone devices.

Message termination applies only to multiple phone device types. Message termination is not redundant message stop, which applies to other targeted device types and is enabled when a system administrator enables device delivery preference. For more information, see Redundant message stop.

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.

Redundant message stop

Redundant message stop prevents users from receiving the same alert on multiple devices after they have responded to the alert on one device. When redundant message stop is enabled, when a user is targeted in an alert on multiple devices, when they respond to the alert from a higher priority device, including email, SMS, mobile app, or mobile device, they do not receive the alert on any additional targeted devices.

Redundant message stop is enabled when:

- Device delivery preference is enabled by a system administrator in **Settings** > **Feature Enablement**.
- An administrator sets the delivery order and interval in **Settings** > **Devices** > **Personal Devices**.
- The Device Delivery Preference is set to Organization defined or User preferred on the alert details page when publishing an alert.

If the device delivery preference is set to the default (System defined) all alerts are sent in a single batch (broadcasted) and redundant message stop is not performed.

Redundant message stop is not supported on the desktop app.

For alerts targeted to the mobile app, if the Repeat Notification setting is enabled, redundant message stop is not performed for mobile app alerts, and users continue to receive alert notifications on their mobile app once the alert has been received on the mobile app even if they have responded on another device.

Redundant message stop is only performed on devices that have a response option. By default, the desktop app and mobile app have an acknowledge response if the alert does not have response options. Phones have a response by default if the Requires Acknowledgement option in Personal Devices Options for phones is checked. Other devices do not include a response option unless one or more is included in the alert content.

Redundant message stop is not message termination, which is enabled by default and applies only to phones. For more information, see Message termination.

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 Live status.

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

1. In the navigation bar, click **Alerts**> **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert that you want to export.
3. Click anywhere in the alert row.
4. Optionally, on the alert details screen, add or modify information.
5. Click **Review and Publish**.

   Note: If any required information is missing, the Review and Publish button will be inactive, indicated by a ⛔.
6. On the **Review and Publish** screen, click **Export to PDF**.

The alert details are downloaded as a PDF file.

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

If you are logged in to an enterprise or super enterprise organization as an Enterprise Administrator, the Organization column is included.

Note: You must be a Report Manager to export sent alerts.

If the Sent Alerts page is sorted by column, the exported report reflects the sorting.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the sent alerts you want to export.
3. Select the sent alerts you want to export.
4. Select **More Actions** > **Export**.

The .csv file downloads to your computer.

Delete an alert

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

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

The Sent 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** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert that you want to duplicate.
3. Select the check box next to the alert name.
4. Click **Duplicate**.

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

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

Alerts that are sent as part of an accountability event cannot be duplicated. These alerts are indicated on the Sent Alerts screen with a .

Manage the publisher map

The publisher map is the map that appears when creating alerts or events. Use the publisher map to target users in a predefined location and to communicate the affected area for an alert or event.

To view the publisher map, do one of the following:

- Click **Add** in the **Location** field in the Content section of an alert template or alert.
- Click **Add** in the **Location** field in the Event Details section of an accountability template or event.

Manage map settings

As an administrator, you can use the Map Settings screen to set up and configure map defaults, shape layers, external layers, and distribution list layers.

1. In the navigation bar, click .
2. In the **Basic** section, click **Map Settings**.

Shape layers

Important: You must be familiar with Geo Information System tools and know how to create map shapes before attempting to add a shape layer. Contact BlackBerry AtHoc customer support for help with using GIS to add a shape layer.

The Shape Layers section of the Map Settings screen displays details about each of the shape layers that have been configured for maps. Shape layers enable you to:

- View the boundaries of shapes and polygons on the map.
- View users and connected organizations that are in defined shape boundaries by their location attributes.
- Target users and connected organizations that are in shape boundaries in alerts and events based on their last known location, location attribute, or selected geographical area of interest.
- Create custom user attributes.

The locations in the shape file are called Imported Shape Layers on the live map and Predefined Locations on the publisher map.

Only shape files that contain polygons and multipolygons can be imported. If your shape file contains any of the following items, the file cannot be imported:

- Point data
- Polylines (linestrings)
- Polygons and polylines (linestrings)
- Self-intersecting polygons

If you need to display points on a map, you should use an external third party tool to create a polygon buffer around each point, and then import the buffer polygons.

The imported shape file should not exceed 100 Mb and should be saved as a .zip file containing one of each of the following file types: .prj, .dbf, and .shp. BlackBerry AtHoc supports the GCS_WGS_1984 Geographical Coordinate System, with the following data:

- Well-known ID: 4326
- Name: GCS_WGS_1984

- GCS Data

```
GEOGCS["GCS_WGS_1984",DATUM["D_WGS_1984",SPHEROID["WGS_1984",6378137.0,298.257223563]],
PRIMEM["Greenwich",0.0],UNIT["Degree",0.0174532925199433]]
```

Tip: Before adding a shape layer, Validate your shape file using QGIS.

Add a shape layer

1. On the **Map Settings** screen, in the **Shape Layers** section, click **Add Shape Layer**.
2. On the **Add Shape Layer** window, click **Select**.
3. Browse to select the shape file on your system.

   If your shape file cannot be loaded, Validate your shape file using QGIS.
4. Select a shape layer name from the **Shape Display Name** pull-down menu. The values in this menu are attributes in the shape file that can be used as the shape display name when the shape layer is displayed on the map.
5. In the **Name** field, enter a name for the shape layer.
6. Optionally, select the check box to make the new shape selectable.

   When creating an alert or alert template, a shape layer that is marked as selectable appears in the Select Predefined Locations list and in the Show Layers panel on the publisher map. If the layer is not selectable, it appears in the Show Layers pop-up, but does not appear in the Select Predefined Locations. Shapes that are not selectable cannot be selected on the map or used for targeting.
7. Select a color from the list. The default is red.
8. Optionally, select to enable the **Create User Attribute** option. When this option is selected, the **Name** field appears. This field is prepopulated with the name of the shape layer, but can be edited. By default, the new attribute is a multi-select picklist. The values of the attribute match the names of the shapes in the shape file. The name for the attribute must be unique in the organization.

   Once a user attribute is created from a shape layer, it cannot be deleted and no other user attributes can be associated with the shape layer.

   Go to **Settings** > **User Attributes** > **Page Layout** to update the new attribute so that it is visible in user profiles. When the attribute is visible, users can subscribe to it as a location of interest from Self Service or in their user profile in the BlackBerry AtHoc management system. Users who subscribe to a location can be targeted in alerts impacting that location on the live and publisher maps.
9. Click **Add**. You are returned to the Map Settings screen.
10. Optionally, to edit an existing shape layer, click . The Update Shape Layer dialog opens. You can update the shape layer name, display color, and selectability status. Click **Save** to save your changes and return to the Map Settings screen.
11. Optionally, click and drag to define the order in which the shape layers are listed on the live and publisher maps.
12. Click **Save**.

Validate your shape file using QGIS

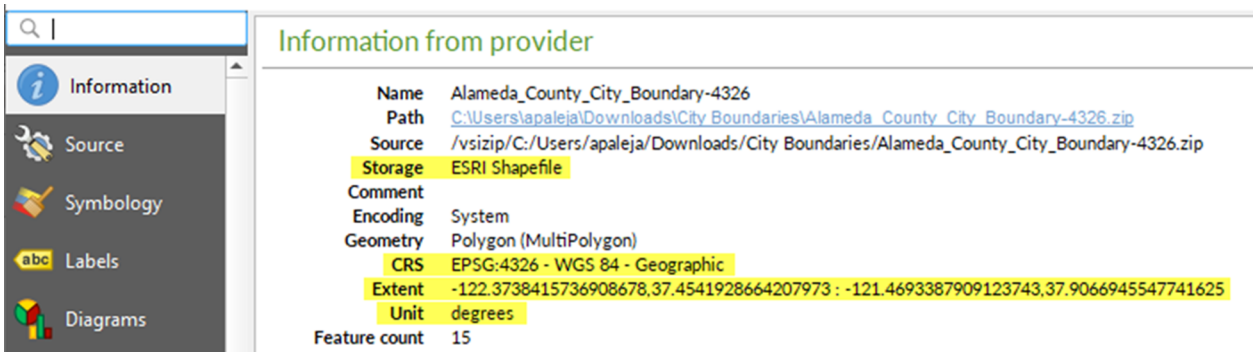
To ensure your shape file is correctly formatted to meet all requirements, you can validate it using desktop software such as ArcGIS, or open source software such as QGIS.

1. Open QGIS.
2. Click **Layers** > **Add Layer** > **Add Vector Layer**.
3. Click **Source** and select the shape file or zipped shape file. The shape .zip file must contain the .shp, .dbf, and .prj files. The shape .zip file can also contain a .shx file that is used to increase the performance of the

shape file, but it is not required. If the shape .zip file does not include the required files, the import stops and an error is displayed.

4. Select **file** for Source Type.
5. Select **UTF-8** for encoding.
6. Click **Add**.
7. Click **Layers**.
8. Right-click the new layer.
9. In the menu that appears, click **Properties**.
10. Click **Information**.
11. In the **Information from provider** section, verify the following values:

    - Storage: ESRI Shapefile
    - CRS: EPSG:4326 - WGS 84 - Geographic
    - Extent: should be within the range of -180.00, -90.00, 180.00, 90.00
    - Unit: degrees



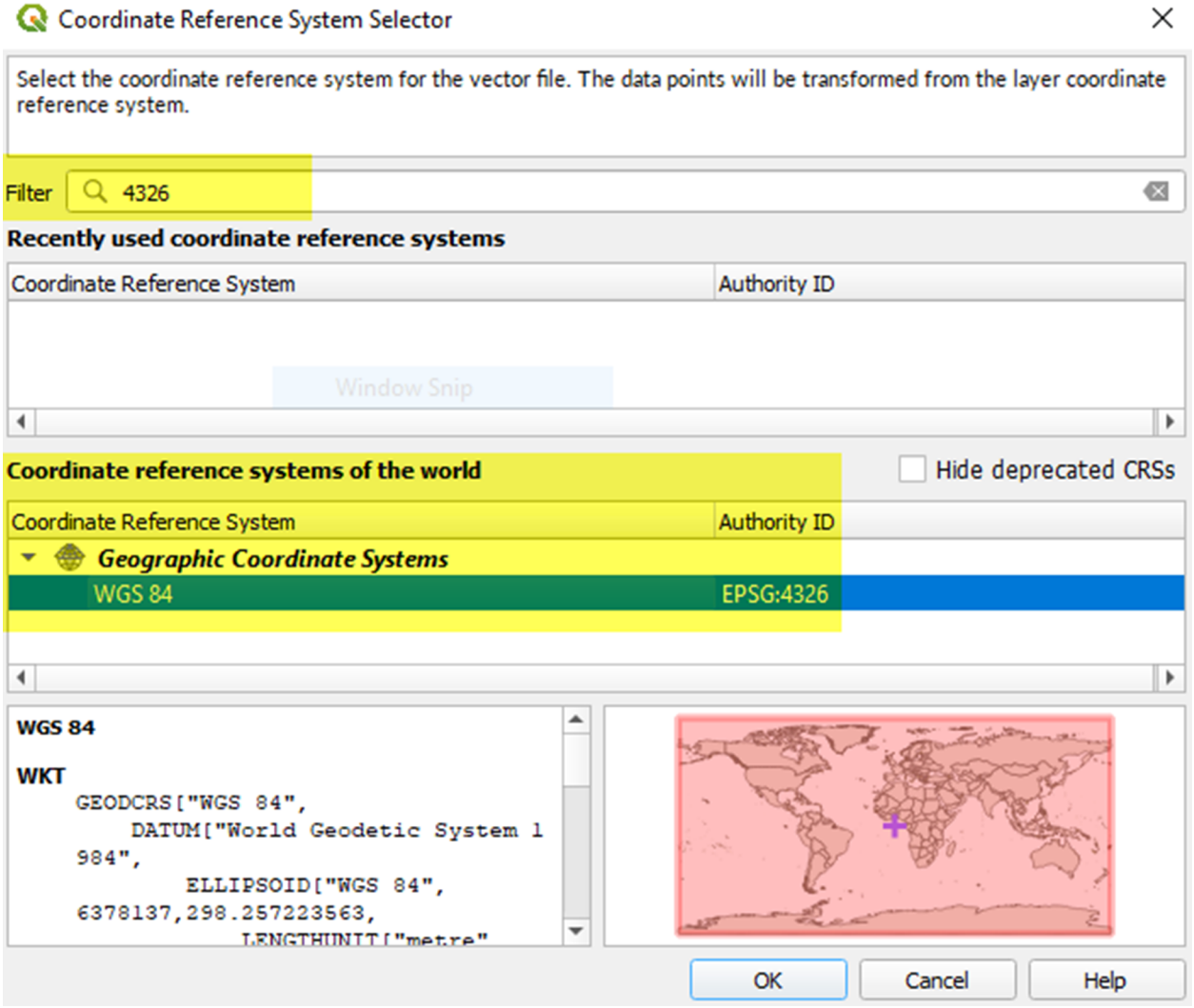
After you finish: If your shape file does not display the correct values in the Information from provider section, Convert projection of shape file using QGIS.

Convert projection of shape file using QGIS

If your shape file is not valid, you can convert a projection of it using QGIS.

1. Open QGIS.
2. Click **Layers** > **Add Layer** > **Add Vector Layer**.
3. Click **Source** and select the shape file or zipped shape file. The shape .zip file must contain the .shp, .dbf, and .prj files. The shape .zip file can also contain a .shx file that is used to increase the performance of the shape file. The .shx file is not required. If the shape .zip file does not include the required files, the import stops and an error is displayed.
4. Select **file** for Source Type.
5. Select **UTF-8** for encoding.
6. Click **Add**.
7. Click **Layers**.
8. Right-click the new layer.
9. Click **Export** > **Save Features As...**.
10. On the **Save Vector Layer as...** window, click **Browse**.
11. Navigate to the correct folder and specify the name of the new layer.
12. In the **Coordinate Reference System** section, click .

13. In the **CRS Selector** window, in the **Filter** field, enter **3426**.
14. From the search results list, select **WGS 84**. The Authority ID is **EPSG:4326**.
15. Click **OK**.
16. Compare the old and new projections of the layer and verify that they are in two different CRS but still overlap.



Distribution list layers

The Distribution List Layers section of the Map Settings screen displays details about each of the distribution list layers that have been configured for maps.

Note: You can create up to ten distribution lists. Each distribution list can include a maximum of 500 users.

1. On the **Map Settings** screen, in the **Distribution List Layers** section, click **Add Distribution List**.
2. On the **Distribution Lists** screen, on the **All Distribution Lists** tab, select the check boxes to display static or dynamic distribution lists. You can also use the search field to narrow the distribution lists that are displayed.
3. Select the check boxes beside the distribution lists you want to add. You can add up to ten distribution lists.
4. Optionally, click the **Selected Distribution Lists** tab and click ✖ to remove a distribution list from the distribution list layers.
5. Click **Apply**. You are returned to the Map Settings screen.
6. Select a color from the palette for each new distribution list. The default color is blue.

7. Optionally, click and drag ⇕ to change the order of distribution lists.
8. Optionally, click ✕ to remove a distribution list from the distribution list layer.
9. Click **Save**.

Configuration and Setup

You can set up the default map view and select your areas of interest for external events in the Configuration and Setup section.

The default map view is the view a user sees when they open the live or publisher map.

Select locations on the map to specify the areas of interest to receive notifications about when external events occur.

Draw shapes or select locations on the map to define your organizational area (areas of interest) to monitor for external events. When an external event impacts a defined organizational area, a notification of the event is sent to the Inbox in the BlackBerry AtHoc management system.

1. On the **Map Settings** screen, in the **Configuration and Setup** section, click ✎ in the **Default Map View and Organizational Areas** section. An editable map screen opens.
2. Optionally, do any of the following:
   - Click 🗺 to select the type of map to display by default.
   - Click 👥 to display users from distribution lists on the map. You can select to display up to ten distribution lists.
   - Click ◈ to choose the layers to display on the map. You can select whether to view:
     - Live accountability events
     - Accountability events from suborganizations
     - Live sent alerts
     - Live incoming alerts
     - Shape layers
     - Organizations
   - In the **Find a place** field, enter an address and press **Enter** on your keyboard to zoom to that location on the map.

     Note: The location on the map you zoom to is configured as the default map view and organizational area. The default map view is displayed on the live and publisher maps and in the Recently Received Alerts section on the BlackBerry AtHoc management system home page.
3. Optionally, to select your organizational area for external events, do the following:
   - Click **Create Custom Locations**, and then select a shape from the shapes panel. Click and drag on the map to draw the shape.
   - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

   Note: You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
4. Click ↻ to refresh the map and review your changes.
5. Click **Apply**.
6. Optionally, on the **Map Settings** screen, in the **Unit of Measure** section, select **Imperial (miles)** or **Metric (kilometers)**. Imperial (miles) is selected by default. The selected unit of measure will display on the live and publisher maps. This setting is applied only to the current organization.
7. Click **Save**.

Map controls

The following control options are available on the publisher map:

- **Find a place**: Enter an address and press **Enter** on your keyboard to move the map view to that location.
- : Select the type of map you want to view. For more information, see Change the map type.
- : Select the layers that are displayed on the map. You can select whether to view the following layers:
  - Live accountability events
  - Events from all suborganizations
  - Live sent alerts
  - Live incoming alerts. Live incoming alerts include: Connect alerts and check-in, check-out, emergency and report alerts from the mobile app.
  - Connected organizations
  - Predefined locations. Predefined locations are imported layers and shape files.
- : Display users from distribution lists on the publisher map.
- : Refresh the map. The map updates automatically every sixty seconds.
- : Zoom to fit. Zoom out to display all incoming live Connect and mobile alerts.
- : Zoom in.
- : Move to the default view.
- : Zoom out.

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. Available map types include the following:

- **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.)

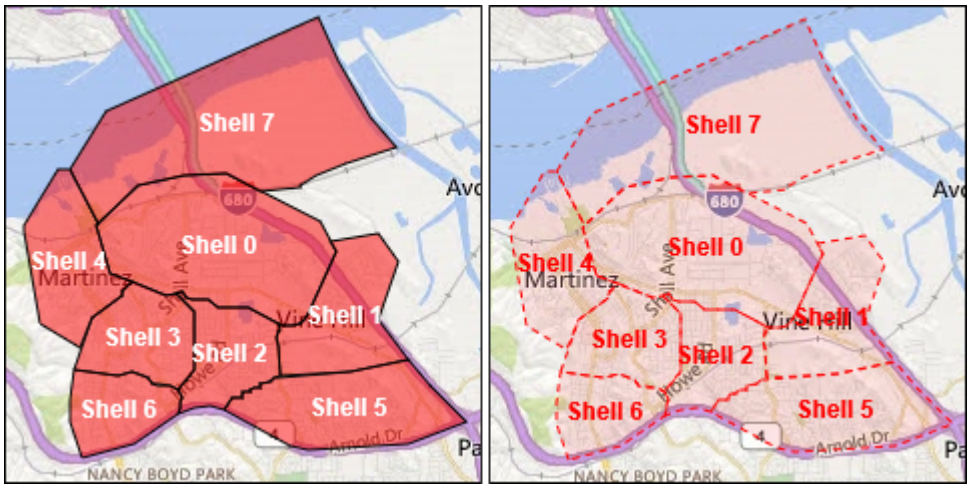
View layers on the publisher map

To view layers on the publisher map, click to open the Show Layers panel and select the layers you want to view. You can view multiple layers simultaneously on the publisher map. Layers selected on the Show Layers panel are displayed for informational purposes and cannot be selected for alert targeting. To select predefined locations for alert targeting on the publisher map, select them from the Select Predefined Locations pull-down menu on the right side of the map. For more information, see Select an alert or event location.

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

Select the check box on the Show Layers panel to view any of the following types of layers:

- **Live Accountability Events**: For more information, see View live alerts and events on the publisher map.
- **Events from all Sub Organizations**: This layer appears only if the map is accessed from a super enterprise or enterprise organization. For more information, see View live alerts and events on the publisher map.
- **Alerts from all Sub Organizations**: This layer appears only if the map is accessed from a super enterprise organization. For more information, see View live alerts and events on the publisher map.
- **Live Sent Alerts**: For more information, see View live alerts and events on the publisher map.
- **Live Incoming Alerts**: This layer displays alerts from the mobile app and Connect alerts. For more information, see View incoming alerts on the publisher map.
- **Organizations**: This layer appears only when the Connect feature is enabled and there are connected organizations. To view organization details in the Organizations layer, click the corresponding icon.
- **Predefined location layers**: Predefined locations are defined in the Map Settings page in the BlackBerry AtHoc management system. Predefined locations selected on the Show Layers panel are not selectable for alert targeting. The non-selectable status is indicated by lighter shading and dotted lines around the edges of the location as shown in the following image:



To select a location from a predefined layer for alert targeting, use the **Select Predefined Locations** panel.

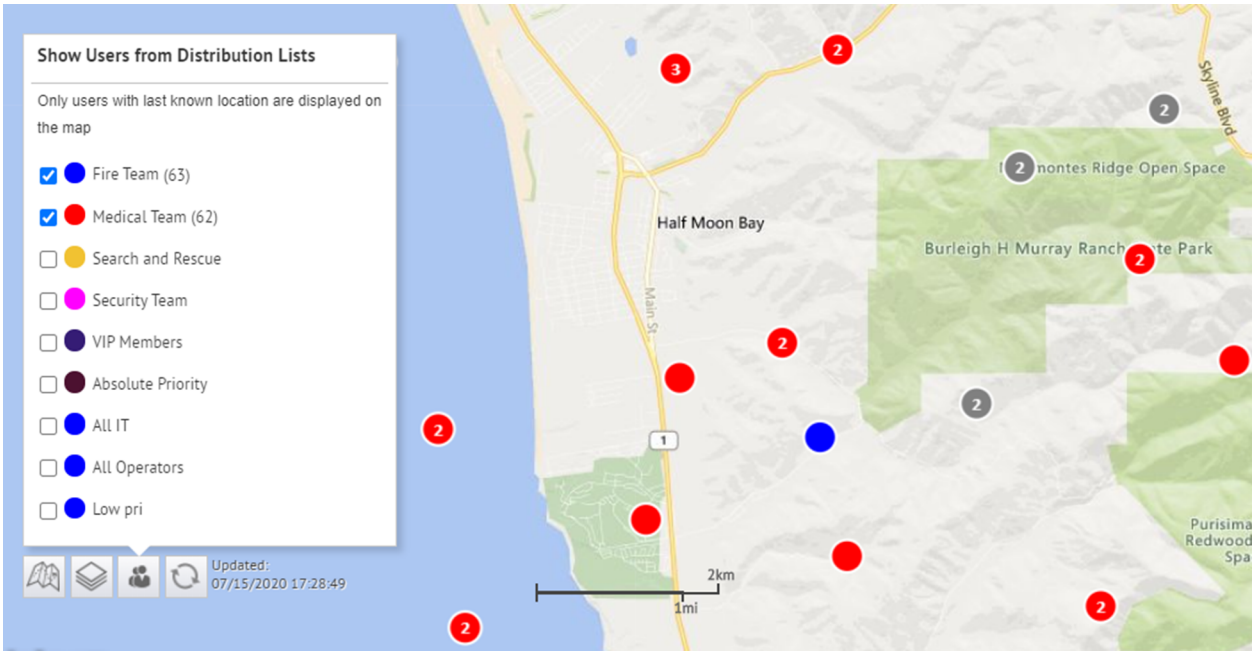
If more than one object exists at or is very close to the same location, click to see the details of the next object.

View users on the publisher map

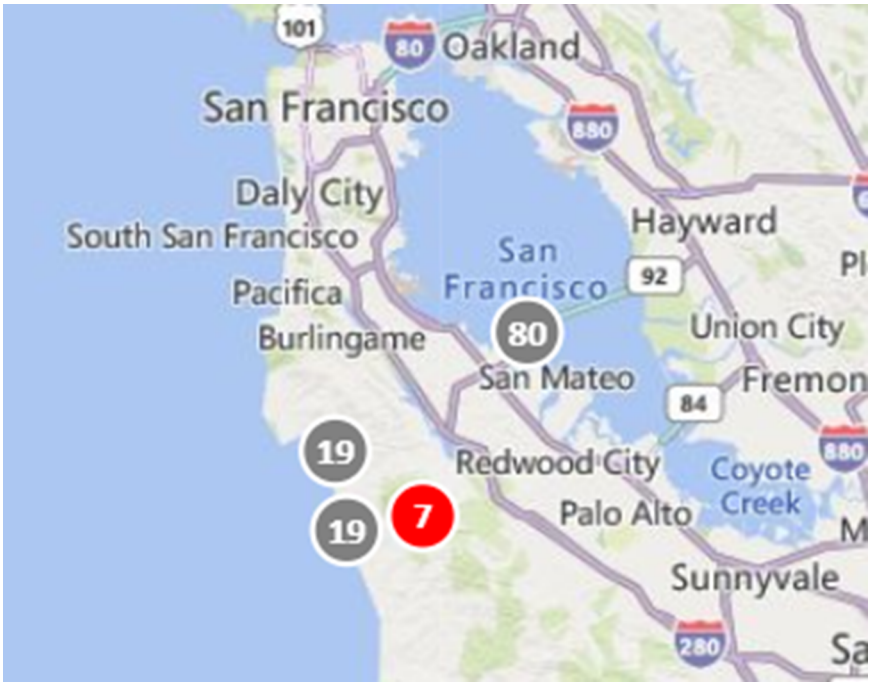
Users last known locations can be displayed on the publisher map. A user's last known location is updated when they do any of the following from the BlackBerry AtHoc mobile app:

- Check-in
- Check-out
- Send a report
- Send an emergency
- Enable the tracking feature
- Enable scheduled location access

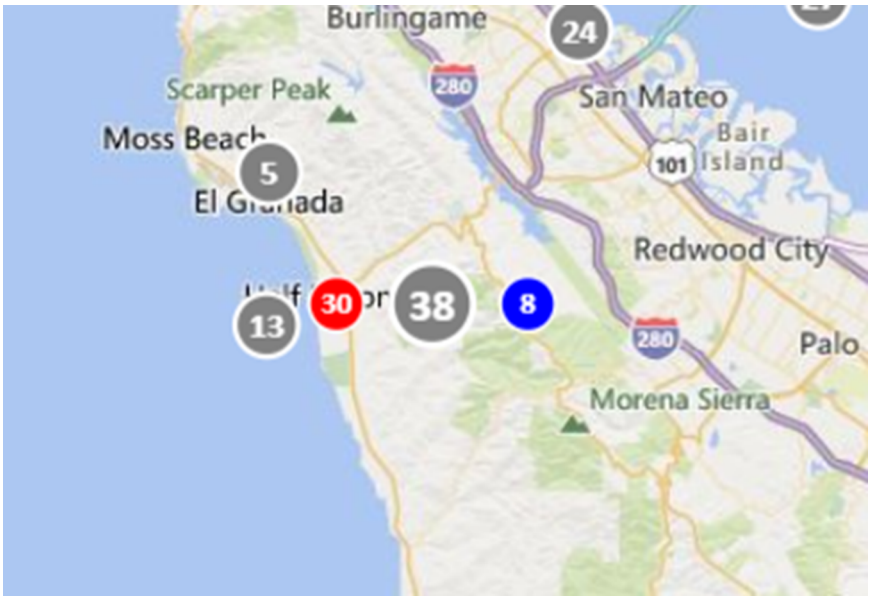
1. On the publisher map, click to open the **Show Users from Distribution Lists** panel. You can select to view users from multiple distribution lists. If multiple users are members of the same distribution list and are in the same location, the number of users is displayed in a circle with a color that matches the color assigned to the distribution list. When users from different selected distribution lists are in the same location, they are displayed in a grey circle.



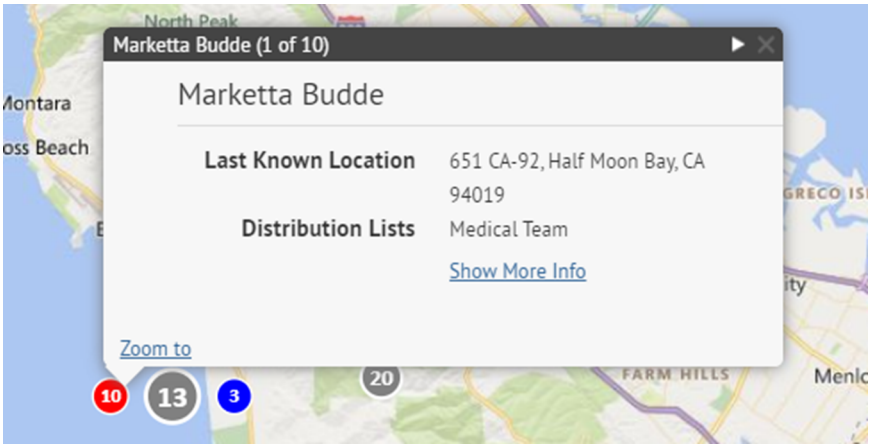
2. Optionally, click to zoom the map out to show all users in the selected distribution lists:



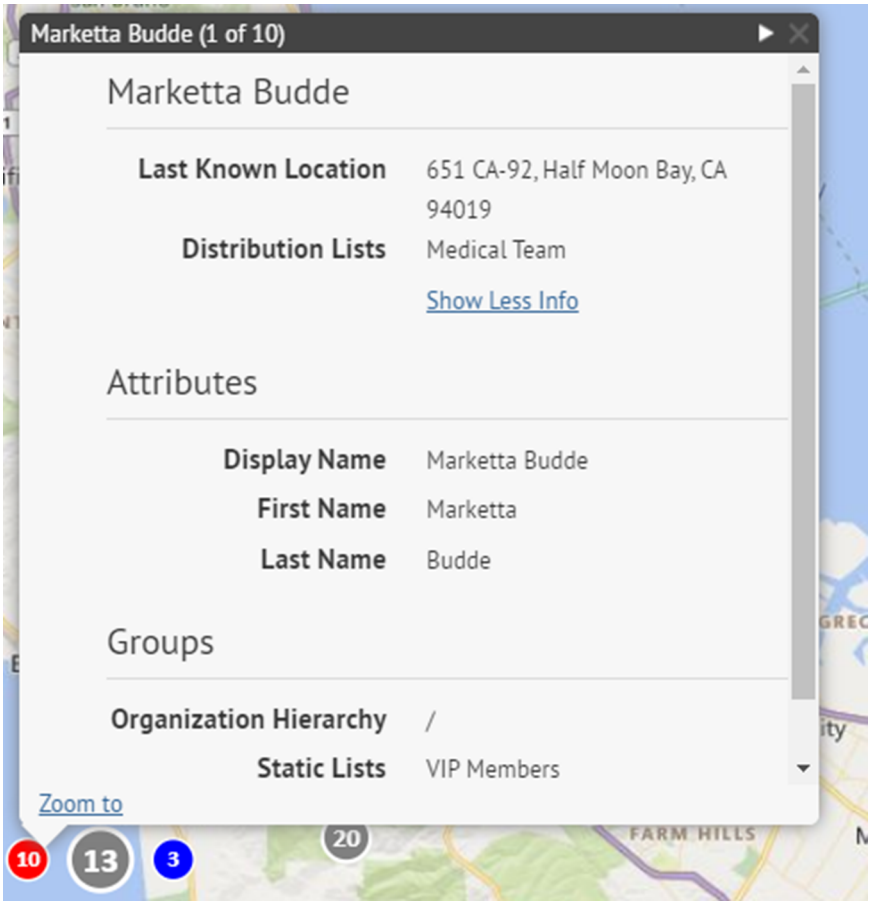
3. Optionally, click a grey circle to display separate circles that have users from the selected distribution lists:



4. Click a circle to open the user details pop-up. The user details pop-up displays the last known location, a timestamp for the last known location, and distribution list membership for a user.



5. Optionally, click **Show More Info** to display the attributes, groups, and devices for the user. The details of the user pop-up can be configured in **Settings** > **General Settings** > **Layouts** > **User Details - Popup View**.



6. Optionally, click **Zoom to** to move the map view to the user.
7. Optionally, click ▶ to display the details for the next user.

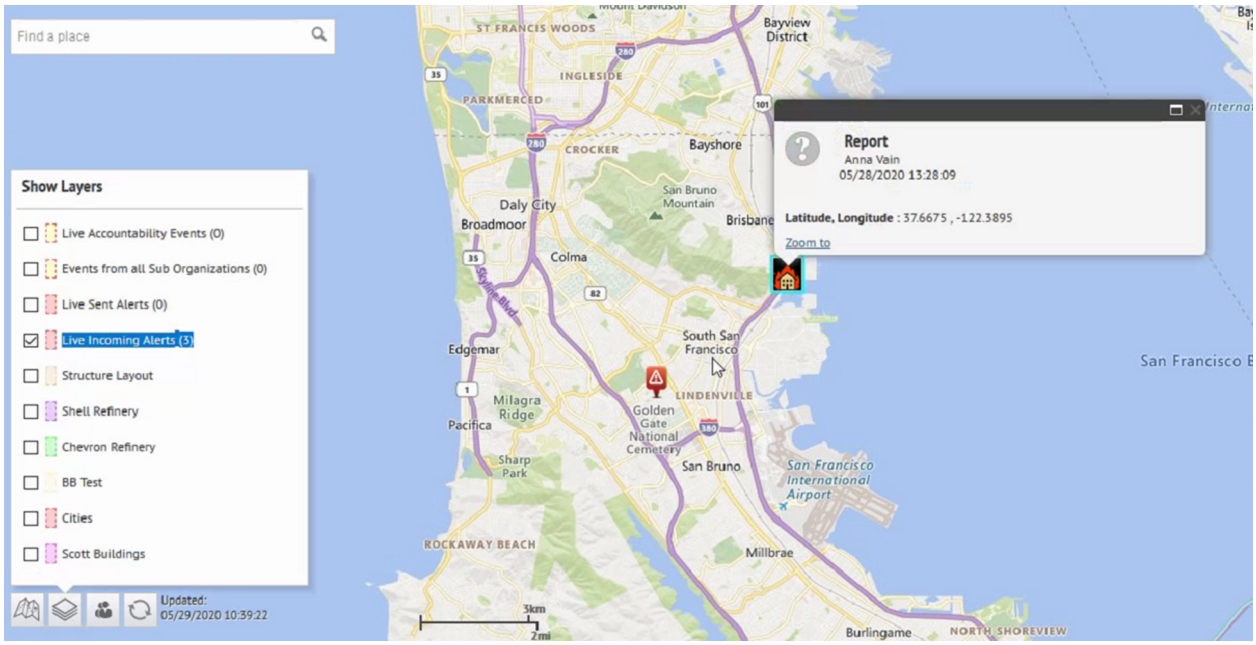
   The ▶ icon appears only when more than one user is displayed in the selected location.

View incoming alerts on the publisher map

Select **Live Incoming Alerts** in the **Show Layers** panel to view all incoming external alerts that fall within the current map area and include location information. External alerts are alerts from the mobile app (check-ins, check-outs, emergencies, and reports) and alerts from connected organizations. To view details about an incoming alert, click the corresponding alert icon on the map.

Note: Alert icons on the map can be customized in BlackBerry AtHoc in the Mobile Alert Settings page. The mobile app Emergency, Check in, and Check out icons cannot be customized.

1. In the bottom left corner of the map, click .
2. On the **Show Layers** panel, select the layers you want to view.
3. On the map, click the icon of the incoming alert you want to view. The following information is displayed in the alert details pop-up:
   - Severity icon
   - Alert type
   - Date and timestamp
   - Location in latitude,longitude
4. Optionally, on the alert details pop-up, click **Zoom to** to move the move the map focus to the alert location.

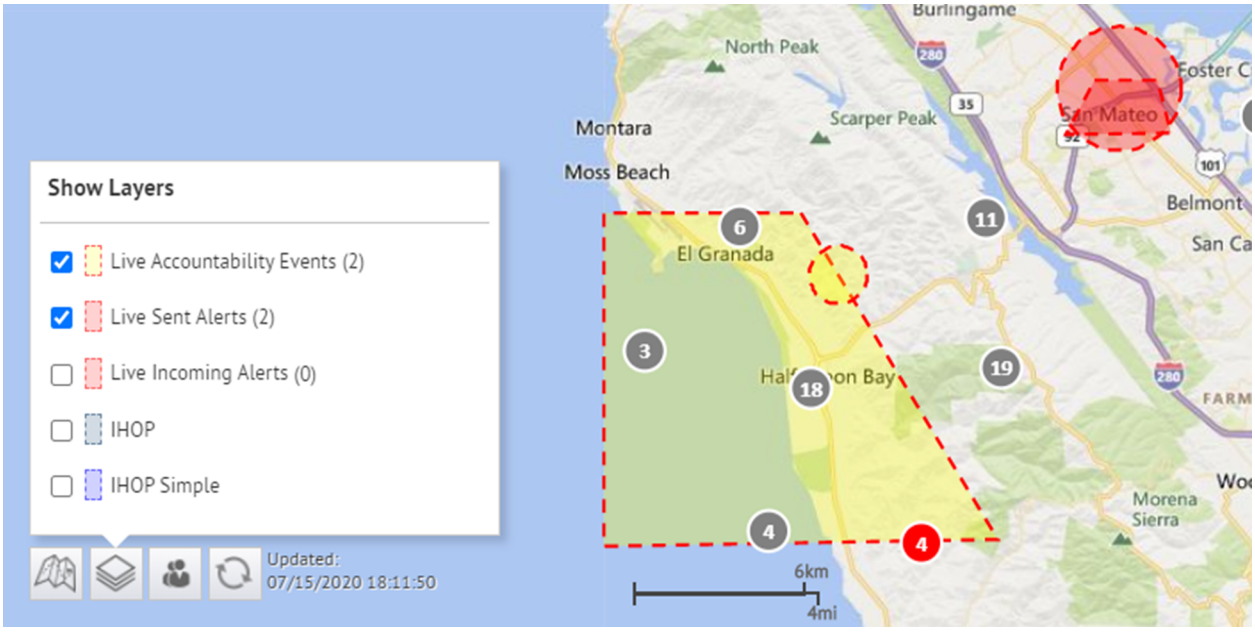


View live alerts and events on the publisher map

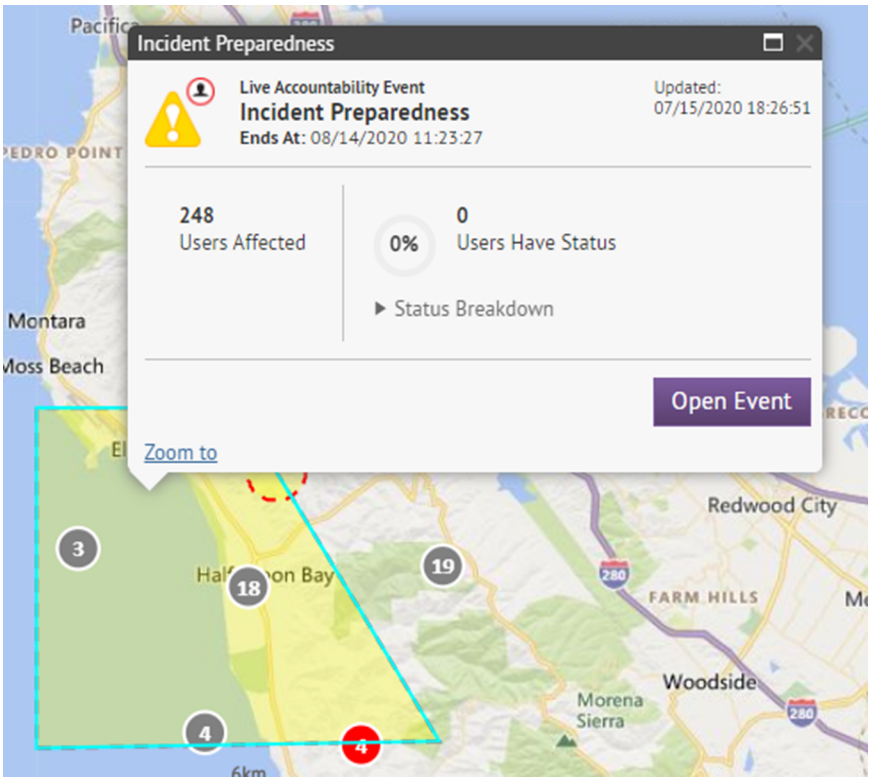
You can view live accountability events and alerts on the publisher map.

The publisher map displays all live accountability events and alerts for your organization. If you are logged in to an enterprise organization, it also displays live alerts from your suborganizations. If you are logged in as an Enterprise Administrator to a super enterprise organization, it also displays live alerts from your sub enterprises and their suborganizations.

1. In the bottom left corner of the publisher map, click .
2. On the **Show Layers** panel, select **Live Sent Alerts** or **Live Accountability Events**.



3. Click an event or alert on the map to open a pop-up window that displays detailed information:

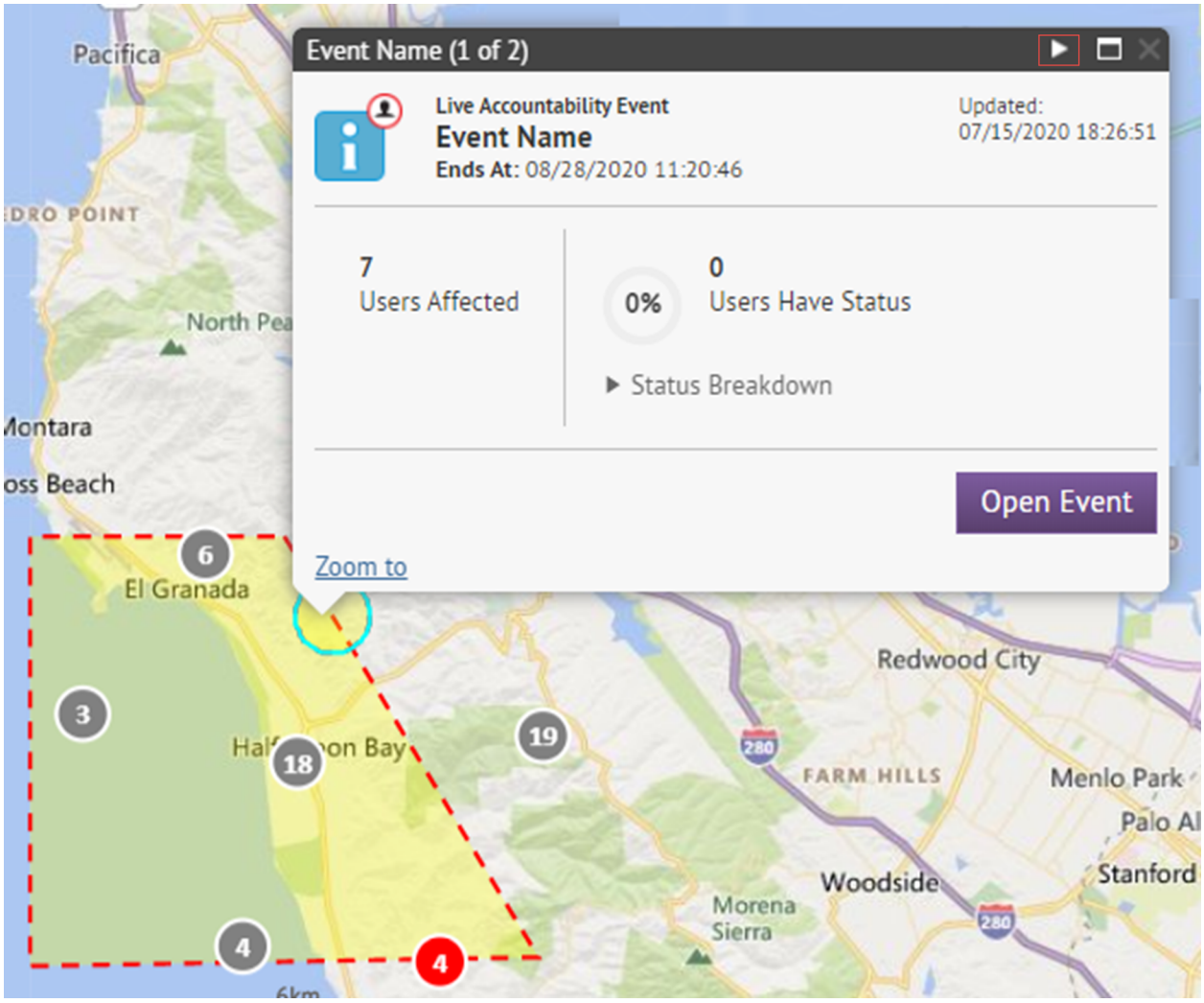


The following information is displayed for the selected event or alert:

- Name of the event or alert
- Type of item: accountability event or alert
- Last updated date and time
- GPS coordinates in latitude,longitude (for incoming mobile alerts only)
- Number of affected users

- Number and percentage of users with a status
- Summary of user statuses by response option

4. Optionally, in an event details pop-up, click **Open Event** to go to the Summary tab of the event in the event manager.
5. Optionally, in an alert details pop-up, click **Open Alert** to go to the Users tab of the alert in the Sent Alerts screen.
6. Optionally, on the pop-up, click **Zoom to** to move the map focus to the alert or event location.
7. If there are multiple events or alerts in the same location on the map, click ▶ to scroll through the details for each alert or event:



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	Omnicomm 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

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.

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

BlackBerry AtHoc fully supports the leading + method. Dialing 011 will continue to be supported for organizations with a U.S. country code since 001 is the U.S. exit code.

Areas of the system that validate phone numbers

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

- BlackBerry AtHoc SDK
- User Sync module
- CSV Import
- Self Service
- User Details page in the BlackBerry AtHoc 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.

- 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.
- 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.
- 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
- 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.
- 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.
- 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.

Email format validation

A critical event management 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
- 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 15 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://www.blackberry.com/us/en/support/enterpriseapps/athoc

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

Documentation feedback

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

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

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

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada