BlackBerry AtHoc

Mobile App Administrator Guide

4.6.1

Contents

What is the BlackBerry AtHoc mobile app?

The BlackBerry AtHoc mobile app leverages the latest mobile technologies for rapid mass notification and personnel accountability. The BlackBerry AtHoc mobile app provides significant advantages to mobile operators, first responders, and alert recipients. This innovative application activates mass alerts and personnel tracking. The BlackBerry AtHoc mobile app is available on most popular devices, including Android and iOS smart phones and tablets. The BlackBerry AtHoc mobile app can be downloaded from Apple App store, Google Play store, and the BlackBerry World store.

Combined with the BlackBerry AtHoc management system, BlackBerry AtHoc's award-winning, unified, netcentric technology, the BlackBerry AtHoc mobile app enhances an organization's ability to reach key personnel during the most extreme conditions, extending situational awareness and the reach of the BlackBerry AtHoc management system.

Product requirements

The BlackBerry AtHoc mobile app has the following software requirements and supported OS versions and requirements.

Supported OS versions

- Android version 6.0 and above
- iOS version 11 and above
- iPadOS (with iOS 13)

Software requirements

BlackBerry AtHoc release 7.5 or later version.

Set up the BlackBerry AtHoc mobile app

The BlackBerry AtHoc mobile app is available as a download from Apple App store, Google Play store, and BlackBerry World. When the BlackBerry AtHoc mobile app is installed, a  appears on your device home screen.

When new alert content is published, the BlackBerry AtHoc mobile app displays an audio/visual alert notification on a mobile phone. The end-user can choose a response option (if response options are sent) and click a link to view complete Alert Inbox information on active alerts.

Personal Safety System (PSS) set up

For detailed information about PSS and how to connect the BlackBerry AtHoc management system with the mobile app, contact the BlackBerry AtHoc Customer Support team.

Register the Mobile app

Prerequisites

- Download and install the BlackBerry AtHoc mobile app from the Google Play store, Apple App store, or BlackBerry World store.
- Before you register the BlackBerry AtHoc Mobile app on your device, you must have the organization code provided by your BlackBerry AtHoc administrator.
- If the BlackBerry AtHoc mobile app is pushed by UEM/MDM and you belong to the same organization configured in the UEM/MDM, then you only have to verify your email address when registering for the first time and are directed to the home screen. In this case, you do not have to enter the organization code. You must enter the organization code if you switch organizations after registering for the first time.
- You may have to enter the organization code when registering for the first time if the organization you belong to is not configured in UEM/MDM, or there is no organization code configured in UEM/MDM.

1. Tap the BlackBerry AtHoc app icon on your device.
2. On the **Registration** screen, read the welcome message. Close the message.
3. On the **Registration** screen, enter the email address that is associated with your BlackBerry AtHoc management system email address.
4. Enter the PSS server URL. This URL is used for debugging purposes.
5. Tap **Send** (iOS device) or  (Android device). The Email Verification screen with a confirmation message is displayed.
6. Check your email for a welcome email from the BlackBerry AtHoc system administrator with a link to activate your account to your registered email address.
7. On the welcome email, click **Verify Now**.

   After the email address is verified, the Add Organization screen opens on your device.
8. Enter the organization code provided by your BlackBerry AtHoc administrator and tap **Send** or  .

   Note: If your organization is already configured with your email address and organization code, then you may not see this screen.

The screen indicates that you are connected to the organization.

Add BlackBerry AtHoc to the app list in BlackBerry UEM

Before you can manage BlackBerry AtHoc, you must add it to the app list in BlackBerry UEM. The app list contains apps that you can assign to users, user groups, and device groups. This section explains how to add BlackBerry AtHoc to BlackBerry UEM. For complete information on how to manage apps in BlackBerry UEM, see the *BlackBerry UEM Managing Apps Administration* guide.

Add BlackBerry AtHoc for iOS to the app list

If your organization is using a proxy server, you must ensure that no SSL interception occurs. For more information on ports that must be open, visit support.blackberry.com/ to read article 52777.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **App Store**.
4. In the search field, search **BlackBerry AtHoc**.
5. In the drop-down list, select the country of the store that you want to search in.
6. Click **Search**.
7. In the search results, click **Add** beside the BlackBerry AtHoc app.
8. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Tasks	Steps
Select a category for the app	**a.** In the drop-down list, select a category.
Create a category for the app	**a.** Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it. **b.** Press **Enter**. **c.** Press **Enter**.

9. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
   - If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
   - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
   - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
10. In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on.

    For example, you can prevent the app from being available in the Work Apps app for iPad.
11. If you want the app to be deleted from the device when the device is removed from BlackBerry UEM, select **Remove the app from the device when the device is removed from BlackBerry UEM**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.
12. If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
13. In the **Default installation for required apps** drop-down list, perform one of the following actions:

- If you want users to receive one prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later using the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device.
- If you don't want users to receive a prompt, select **No prompt**.

The default installation method applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.

14. In the app configuration table, complete one of the following tasks:

Create the app configuration from an XML template	**a.** Click **> Create from a template**. **b.** Click **Browse** and select the template that you want to add. **c.** Click **Upload**. **d.** Type a name for the app configuration and specify the following values: 1. **App Config Version**: Enter the version of the app configuration. The default is 1. 2. **Organization Code**: Enter your Organization Code for User registration. **e.** Click **Save**.
Create the app configuration manually	**a.** Click **> Configure manually**. **b.** Enter a name for the app configuration. **c.** Add the following settings: **d.** Click **Save**.

Key	Value
appconfigversion	Enter the version of the app configuration.
firsttime_orgcode	Enter your organization code for user registration.
firsttime_pssurl	Enter the PSS that the Mobile App communicates with, either US PSS or UK PSS.

15. Click **Add**.

After you finish

- Assign BlackBerry AtHoc to a user or user group.

Add BlackBerry AtHoc for Android to the app list if BlackBerry UEM is not configured for Android Enterprise devices

If BlackBerry UEM is configured to support Android Enterprise devices, see Add an Android app to the app list if BlackBerry UEM is configured for Android Enterprise devices.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. In the **App name** field, type **BlackBerry AtHoc**.
5. In the **App description** field, type a description for the app.
6. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Tasks	Steps
Select a category for the app	**a.** In the drop-down list, select a category.
Create a category for the app	**a.** Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it. **b.** Press **Enter**. **c.** Press **Enter**.

7. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
   - If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
   - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
   - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
8. In the **Vendor** field, type **BlackBerry**.
9. In the **App icon** field, click **Browse**. Locate and select an icon for the app. The supported formats are .png, .jpg, .jpeg, or .gif. Do not use Google Chrome to download the icon because an incompatible .webp image is downloaded.
10. In the **App web address from Google Play** field, type https://play.google.com/store/apps/details?id=com.athoc.panic or open Google Play, search for BlackBerry AtHoc and paste the URL.
11. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
12. In the **Send to** drop-down list, perform one of the following actions:
    - If you want the app to be sent to all Android devices, select **All Android devices**.
    - If you want the app to be sent to only Android devices that use Samsung KNOX Workspace, select **Only KNOX Workspace devices**.
13. Click **Add**.

After you finish

- Assign BlackBerry AtHoc to a user or user group.

Add BlackBerry AtHoc for Android to the app list if BlackBerry UEM is configured for Android Enterprise devices

If you have configured support for Android Enterprise devices, the connection to Google allows BlackBerry UEM to get app information from Google Play. The connection to Google Play is made directly from the computer that is running the BlackBerry UEM console. If your organization is using a proxy server, you must ensure that no SSL interception occurs. For more information on ports that must be open, visit support.blackberry.com/community to read article 52777. For more information about configuring BlackBerry UEM to support Android Enterprise devices, see "Configuring BlackBerry UEM to support Android Enterprise devices in the *BlackBerry UEM Configuration Guide*.

If BlackBerry UEM is not configured to support Android Enterprise devices, see Add BlackBerry AtHoc for Android to the app list if BlackBerry UEM is not configured for Android Enterprise devices.

To use Google Play to manage apps in the Samsung KNOX Workspace, devices must have Samsung KNOX 2.7.1 or later installed and you must allow Google Play app management for Samsung KNOX Workspace devices in the activation profile.

Note: In an upcoming release of BlackBerry UEM, the settings applicable to BlackBerry Hub+ and Divide Productivity will be removed from the email profile and will be available only in an app configuration in the app settings. In this release, if you configure app settings in the email profile and in an app configuration, the app configuration takes precedence if both are assigned.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. Search for and select **BlackBerry AtHoc**.
5. Click **Approve**.
6. To accept app permissions on behalf of users, click **Approve**. You must accept the app permissions to allow required apps to be automatically installed on Android Enterprise devices or in KNOX Workspace. If you don't accept the app permissions on behalf of users, the app can't be managed in BlackBerry UEM.
7. On the **Approval Settings** tab, choose how you would like to handle new app permission requests when there is an updated app.
   - To automatically accept the new permissions added by the app vendor, select **Keep approved when app requests new permissions**.
   - To manually re-accept the new app permissions added by the app vendor before the app can be sent to new devices, select **Revoke app approval when this app requests new permissions**.
8. If you selected the **Revoke app approval when this app requests new permissions** option on the Notifications tab, add a subscriber to be notified when the app permission changes. The administrator will have to re-approve the app before users can access it.
9. Click **Save**.
10. In the **App description** field, type a description for the app.
11. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
12. In the **Send to** drop-down list, perform one of the following actions:
    - If you want the app to be sent to all Android devices, select **All Android devices**.
    - If you want the app to be sent to only Android devices that use Samsung KNOX Workspace, select **Samsung KNOX Workspace** devices.
    - If you want the app to be sent only to Android Enterprise devices, select **Android devices with a work profile**.

13. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Tasks	Steps
Select a category for the app	**a.** In the drop-down list, select a category.
Create a category for the app	**a.** Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it. **b.** Press **Enter**. **c.** Press **Enter**.

14. In the **App configuration** table, click **+** to add an app configuration.
15. Type a name for the app configuration and specify the following values:
    - **App Config Version**: Enter the version of the app configuration. The default is 1.
    - **Organization Code**: Enter your Organization Code for User registration.
16. Click **Save**.
17. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
    - If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
    - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
    - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
18. Click **Add**.

After you finish

- Assign BlackBerry AtHoc to a user or user group.

Configure the Mobile App device in BlackBerry AtHoc

Configure the mobile gateway in the Settings section of the BlackBerry AtHoc management system to enable the BlackBerry AtHoc management system to publish alerts through the mobile app.

Enable the Mobile App device on the BlackBerry Athoc application server

Log in to the BlackBerry AtHoc management console and check the Delivery Gateways section to verify that the Mobile device has been installed. If the device is installed, skip this section.

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

Configure the Mobile App gateway settings

Configure the Mobile App gateway settings to deliver alerts to and receive alerts from the mobile device.

Note: Contact the BlackBerry AtHoc customer support for assistance in setting up the Mobile App for BlackBerry AtHoc. Before you begin this process, you should also contact your system administrator to get the NDS address used for the notification delivery server.

1. In the navigation bar, click .
2. In the **Devices** section, click **Mobile App**. The Mobile App gateway configuration screen opens with the default settings that are listed in the following table.

Option	Description
Notification Delivery Server Settings	
Notification Delivery Server Address	`https://mobile.athoc.com`
Username	Should be between 3 and 100 characters long
Password	Should be between 3 and 100 characters long
Debug Trace	**Default:** No Yes Avoid performance degradation by enabling debug tracing for the mobile delivery gateway only while actively debugging the mobile notifications for the Mobile application.

Option	Description
Features	
Alerts	Selected. Available to all users
Map	Selected. Available to all users
Alert Publishing	Selected. Available for operators only.
Advanced Features	Is available to a selected group of users only. When selected, advanced features display. Select a distribution list to give access to advanced features to a group of users. Options include Emergencies, Check In, Reports, and Tracking. When you select Tracking, the Tracking Interval option is displayed to set an interval. To learn about the advanced features, see Role-based permissions for the mobile app.
Settings	
Photo Quality	**Default:** Low High
Video Quality	**Default:** Low High
Emergency Contact Number	Designate the emergency contact telephone number. If no phone number is entered in the field, the Mobile App will not have an emergency contact number button.
Support Email Address	athocsupport@blackberry.com
Enable Mobile Analytics	Collects mobile app usage analytics. No personal, private, or sensitive information is collected. **Default:** No Yes
Enable Personal Alert Button	Enables sending an emergency using a paired personal alert button. Emergencies must be enabled in Advanced Features. **Default:** Yes No
Enable Jail-Break/Root Detection	Enables the mobile app check if the device OS security has been compromised **Default:** Yes
Send Location with Response	Sends user location information with alert or event responses. **Default:** Yes No

Option	Description
User Choice	Enables each mobile user to choose whether to send location information with alert or event responses. **Default:** No Yes This option is visible only when "Yes" is selected for Send Location with Response.

Note: You should use the default values to set up and configure the BlackBerry AtHoc mobile app.

3. Click **Copy Default Settings**.
4. In the **Notification Delivery Server Address** field, enter the NDS address you received from your system administrator.

   By default, the URL points to `mobile.athoc.com`.
5. Add the user name and password provided by BlackBerry AtHoc.
6. In the **Features** section, select the options that can be available to users when they are using their mobile device:
   - **Alerts**: Users can receive alerts.
   - **Map**: Users can view the SSA map.
   - **Alert Publishing**: Operators can publish alerts.
   - **Advanced Features**: Advanced features available to a selected group of users. When you select this option, advanced features are displayed. Each mobile feature in the Advanced Features section includes its own menu to select a distribution list. To learn about the advanced features, see Role-based permissions for the mobile app.
7. In the **Settings** section, select the photo and video quality.
8. In the **Emergency Contact Number** field, enter the phone number of the operations center where emergencies are sent from mobile devices.
9. In the **Support Email Address** field, enter an email address where logs are sent for error debugging.
10. In the **Enable Mobile Analytics** section, select whether to enable the mobile app to collect usage analytics.
11. In the **Enable Personal Alert Button** section, select whether to enable users to send an emergency duress message using a paired personal alert button.
12. In the **Send Location with Response** section, select whether to send location information with alert or event responses. When **No** is selected, location information is prevented from being returned with alert or event responses even if mobile location services are active on the mobile device.
13. In the **User Choice** section, select whether to enable mobile users to choose to send location information with alert or event responses. This option is only available when **Yes** is selected for the **Send Location with Response** option.
14. Click **Save**.

Configure the mobile device

After BlackBerry AtHoc Technical Support has set up the correct Notification Delivery Server (NDS) address, you can assign an AtHoc Mobile Gateway to the phone.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Devices**.

4. On the **Device Manager** screen, click **Mobile App**.
5. Click **Edit**.
6. In the **Delivery Gateway** section, click **Add a Delivery Gateway** and select **Mobile App**.
7. Click **Configure** to open the text-entry field.
8. By default, the configuration value appears in the text-entry field. If the text-entry field is empty, complete the following steps:
   a. Click **Remove**.
   b. Select **Mobile App**
   c. Click **Configure**.
   d. Copy the following text into the field:

```
<Configuration>
    <DeviceType>mobileNotification</DeviceType>
</Configuration>
```

9. Click **Save**.
10. Click **Enable**.

Role-based permissions for the mobile app

As a system administrator, you can specify what controls a user can see on the mobile device depending on their roles and responsibilities (also known as role-based permissions). For example, you might want an emergency team to be able to see the map, send field reports, start tracking, and send emergency duress alerts. However, you might want a student on a campus or non-emergency personnel to only be able to receive notifications and to send duress (emergency) alerts to security without having access to the map or to tracking or field reports.

1. For users who need advanced features, create a distribution list.

   Note: Only one distribution list can be used for the organization.
2. In the navigation bar, click .
3. In the **Devices** section, click **Mobile App**.
4. On the **Mobile app settings** page, in the **Features** section, select **Alerts** to grant permission to receive alerts on mobile devices.
5. Select **Map** to provide access to view the SSA map.
6. Select **Alert Publishing** to provide publishing permission to operators.
7. Select **Advanced Features** to provide advanced features to a selected group of users. The select advance features section appears.
8. In the **Select advanced features** section, select one or more features and distribution lists the user can access from the mobile application:
   - **Emergencies**: Send duress messages
   - **Check In**: User check ins on the map
   - **Reports**: Send field reports
   - **Tracking**: Track mobile device location for a specified amount of time.
9. After selecting an advanced feature, choose a distribution list that can use the selected feature.
10. Make any other needed changes for the Mobile App settings.
11. Click **Save**.

Configure mobile alert settings

Configure the mobile alert settings to respond to alerts. You can select a severity level, specify whether the incoming alert appears on the map, or whether an alert template is published. These alerts appear on the Situation map and on reports with icons. All three Mobile incoming alerts categories Emergency, Check In, and Report can be edited to trigger a template.

The following incoming mobile alerts types are available in the system:

- Mobile Standard
  - Emergency (Duress)
  - Check-in
  - Report
- Custom
  - Report: Add a custom report

Alert rules help determine which alert templates to run when an alert arrives in the Inbox. Mobile Alert rules have no conditions, the operator can select an alert template to be triggered on incoming mobile alert.

1. In the navigation bar, click .
2. In the **Basic** section, click **Mobile Alert Settings**.
3. On the **Mobile Alert Settings** screen, in the **Emergency** section, click . By default, the severity is set to High. You can send an alert with an emergency by selecting an alert template from the **Run Alert Template** list. Select **Automatically display on map**, and then click **Save**.

   Note: The Emergency title and icon are preset and cannot be changed.
4. In the **Check-In** section, click . By default, the severity is set to Moderate. You can select an alert template from the **Run Alert Template** list. Select **Automatically display on map**, and then click **Save**.

   Note: The Check In title and icon are preset and cannot be changed.
5. In the **Report** section, click **Add** to create a new incoming alert report that users can access through their mobile device.

Create a field report for the mobile app

When a mobile user sends a field report, they can choose from a list of report types. These field reports types can trigger an alert template.

1. In the navigation bar, click .
2. In the **Basic** section, click **Mobile Alert Settings**.
3. On the **Mobile Alerts Settings** screen, in the **Report** section, click **Add**.
4. On the **Report** screen, add or select values in the following fields:
   - **Title** Enter a descriptive label that identifies the field report.
   - **Message**— Enter the default message you want to appear in the message field. This text can be edited by end users prior to them sending the field report.
   - **Icon**: Select the specific icon you want to use on maps to represent the event report.
   - **Default Severity**: Select the default severity of the field report. Severity options include High, Moderate, Low, Informational, or Unknown. End users can change the severity prior to sending the report.
   - **Run Alert Template** Select an alert template to be published when a user sends the field report.

     Note: Only alert templates that are ready to be published are displayed.
   - **Automatically display on map** Optionally, select this option if you want the field report to appear by default on the map. This setting *cannot* be edited by end users prior to them sending the report.

5. Click **Save** to add the field report to the list of options in the Report section.
6. Optionally, repeat steps 3 to 5 to add additional report types that end users can access when preparing to send an event report.

Manage alert templates

Alert templates define the types of alerts that can occur within an alert folder, enabling operators to quickly publish the appropriate alert during an emergency.

When initially setting up the BlackBerry AtHoc system, the administrator defines the alert folders (categories of alerts) and appropriate alert templates for each folder. Later, the administrator or Advanced Alert Managers can add new alert templates or modify existing templates.

Note: When operators access the Alert Templates screen, they can see only alert templates associated with folders they have access to.

Create an alert template

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Alerts**.
3. Click **Alert Templates**.
4. On the **Alert Templates** screen, click **New**.
5. On the **New Alert Template** screen, select or enter values in each of the following sections, details of which can be found in each of the following sections of this guide:
   - Alert template
   - Content
   - Target users
   - Mass devices
   - Schedule
6. After you have reviewed the template content, 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. Click **New**.
3. On the **New Alert Template** screen, in the **Alert Template** section, in the **Name** field, enter a meaningful name for the alert template to help publishers identify it. The Name and Description display in BlackBerry AtHoc only and are not displayed to end users.
4. In the **Description** field, provide details about the alert template's purpose or content. This description is not seen by end users and is only visible within the application.
5. In the **Folder** field, select the alert folder you want to add the alert template to.
6. Optionally, select **Available for Quick Publish** if you want to make the new alert template available through all quick publish links in the application.
7. Select **Available for mobile publishing** if you want to make the new alert template available for publishing from the mobile app.
8. When you are done, configure the Content section.

Define content for an alert or alert template

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

1. Optionally, if you are creating an alert or alert template in a language other than the default language displayed on the screen, click the button next to the **Severity** field and select the language from the list that appears. Note that 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 is in the language you selected.
2. In the **Severity** field, select the severity level.

   Important: High severity is reserved for extreme emergencies. On the Mobile application, it overrides the device sound settings to emit any sounds associated with the alert or alert template.
3. In the **Title** field, enter a one-line summary that communicates the purpose of the alert or alert template. The title is required and displays at the top of the recipients' screen when the alert is sent out.
4. Optionally, if you want to insert a placeholder into the alert or alert template title, click + and select the placeholder from the list.
5. In the **Body** field, enter up to 2000 characters of text that communicates why the alert has been sent and provide instructions to the target audience.
6. Optionally, if you want to insert a placeholder into the event or template body, click + and select the placeholder.
7. In the **Type** field, select the type that fits with the alert or alert template you are creating.
8. In the **Response Options** field, do one of the following:
   - Click **Custom Response Options** to view a list of preset responses you can add to the alert or alert template.
   - Click the **Add Response Option** to define one or more responses that alert recipients can send to let you know that they have received the message. If the response involves a call bridge, select **Call Bridge**, then, in the two fields that appear below the check box, enter the call bridge number and passcode users will need in order to respond. For specific details about what call bridges are and how they are used, see What is a call bridge?
   - Optionally, if you want to insert a placeholder into the **Response Options** field, click + and select the placeholder.
9. Optionally, in the **More Info Link** field, enter one of the following:
   - A URL that opens a Web page where users can go to get more details about the alert when it is sent out. When users receive the alert, a **For Further Information** link will take them to the Web page.
   - 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.
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** field, click **Add** to access a map on which you can designate a geographic area for the alert or alert template.

    For a detailed description on how to specify a geographic location, see Select an alert location.
12. Optionally, in the **Attachments** field, drag and drop or click **Browse** to select files to include as attachments in the alert. For more information, see Add attachments to an alert.
13. When you are done, configure the Target individual users section.

What Is a Call Bridge?

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

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

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

Add attachments to an alert

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

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

The following file types are supported:

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

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

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

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

Add an attachment using Dropbox

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

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.

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 **Sign In** 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 **Share**.
8. Copy the link location that appears in the **Link to file** field.
9. Paste the link location into the **More Info Link** field in the **Content** section of the alert, event, or template you are creating.

Select an alert location

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

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

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

   A separate screen appears, displaying an interactive map.

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

   Note: Uploading multiple layers with different set of predefined locations is recommended to improve usability and system performance. Map layers are configured on the Map and Layers screen, accessible to Administrators at **Settings** > **Situation** > **Map and Layers**.
4. Select one or more predefined locations within the layer by clicking them on the map or selecting the checkbox beside their names in the drop-down menu.

   As you make selections, the locations are highlighted on the map.
5. To create a custom location, click **Create Custom Locations** button to display the drawing tools for creating shapes.
6. Click one of the shape buttons in the **Map Tools** bar and click and drag on the screen to cover the location you want to use in the alert or event.
7. To view the size of a custom location, click the shape on the map. A black box appears beside the Create Custom Locations button, listing the total area of the custom location in square miles or square kilometers, depending on which unit of measure your system uses.
8. To edit a custom location, click the shape and then click and drag on any of the circles that appear around the edge of the shape.
9. To scale new shapes up and down while preserving their dimensions, complete the following steps:

   a. Press and hold the **SHIFT** key on your keyboard.
   b. Click and release the shape to select it.
   c. Move your cursor over one of the white squares around the shape.
   d. Click and hold on the white box while dragging the mouse to increase or decrease the shape size.

   As you create shapes and select predefined locations on the map, the Location Summary field in the bottom-right corner updates to provide you with an overview of the total number of locations that are displayed on the map and the locations that will be included in the alert or event.
10. To delete one of the custom locations you created, do one of the following:

- In the **Location Summary** field, click **X** next to each location you want to remove. Note that if you have created more than one custom location, they are combined in the list and cannot be deleted individually. To delete individual custom locations, use the method described below.
- Click the border of the location shape on the map to select it, then click to remove it.

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

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

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

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.
- **Pre-set**—Defined in advance as user attributes. The pre-set options have a feature that is not available in custom responses. When a user responds to the alert using a pre-set 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 type.

Benefits of Using a Pre-Set Response Option

Pre-set response options created as user attributes are appropriate in the following situations:

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

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

   Tip: On the New Attribute screen, enter the name of the new attribute prefixed with "RO" to indicate that the attribute is for response options: for example, RO-OfficeLocation.
4. On the **New Attribute** screen, in the **Values** field, add the response options for each picklist option.
5. In the **Page Layout** field, leave all options set to **Do not show**.
6. Optionally, to track the responses, in the **Personnel Reports** section, select **Enabled** and enter a report name, such as "Office Locations Response Options".
7. Click **Save**.

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

If you selected **Enable** in Step 6, each time an operator publishes an alert with the response options you created, the option 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 the name you gave the report in Step 6.

Define target users for an alert or alert template

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

As the event progresses, the affected users list updates in real time. For example, if you select to notify "By Location," if additional people enter the selected area during an event with tracking enabled on their mobile device, they are added to the list of affected users and begin receiving messages.

Target groups in alerts or alert templates

Using the By Groups tab, publishers can target groups of users based on their memberships in organizational hierarchical nodes and in distribution lists. The alert is sent to users within the selected groups.

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. The "All User Base" is the first node that appears and is the only node from the hierarchy that appears when collapsed.
- **Distribution Lists**—Static and dynamic

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**.
2. In the **Groups** field, select the checkbox beside each group or distribution list that you want to target.

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

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

Target individual users

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

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

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

   As you select (and block) users, the total number selected updates automatically at the top of the screen and the total number targeted and blocked appears below the search field.
4. After you have selected all users you want to include in the alert, click **Apply**.

The Users screen then reappears, displaying the names of the users you added with a ✔ beside their name. If you blocked any users, a ⊘ appears beside their name.

Note: To remove a targeted user from the alert recipient list, click ✖ beside their name.

Target by location

To target users by location, you must first define a location in the Content section of the alert or alert template. For detailed instructions on how to do this, see Select an alert location.

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

1. In the **Target Users** section, click the **By Location** tab.
2. Select **Users in the defined location**.

   The **Targeting Summary** field at the bottom of the **Target Users** section updates to display the total number of locations on the map that can be used to target recipients when alerts are generated from the alert template.
3. Click the number in the **By Location** field to open a new screen that displays a map showing each of the locations that have been targeted. This is the same map that can be seen in the **Location** field in the **Content** section.

Target or block users by advanced query

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

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

   Note: The list of operations varies depending on the type of attribute selected.
5. If the Operation you selected in Step 3 requires additional query values, a third field appears. Enter or select a value for the attribute.
6. Optionally, click **Add Condition** and then repeat steps 2 to 4 for each additional condition you want to add.

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

   The Targeting Summary field at the bottom of the Target Users section updates automatically to display the total number of users who match the query conditions you have created.
7. Optionally, click the number in the **Advanced Query** field in the **Targeting Summary** to view a screen that displays the criteria that you created for the advanced query.
8. Optionally, modify the query conditions as needed to isolate the exact user group you want to send the alert to. Click **Add Condition** to add more conditions. Click ⛔ beside the condition to remove it.

Review the targeting summary

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

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

By Groups

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

By Groups-Blocked

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

By Users

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

By Users-Blocked

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

By Location

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

By Advanced Query

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

Personal Devices

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

   A list of all available personal devices appears, accompanied by statistics that reveal the total number of selected users who can be reached by each device type.
2. Select the check box next to each personal device you want to include.

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

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

Specify personal device options for an alert or alert template

After you select personal devices for an alert or alert template, you can specify options for most of the devices.

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

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

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

The following sections detail the options that are available for the BlackBerry AtHoc mobile app.

Option: **Repeat Notification**

Each alert is only sent once. This option is used to specify if and how often notifications about the alert are repeated on a mobile device.

- **None**: Send the alert notification once
- **Default**: Use the default time that has been defined for the selected severity.
  - For alerts with a severity level of **High**, the default is one notification a minute for 10 minutes.
  - For alerts with a severity of **Moderate**, **Low**, **Informational**, or **Unknown**, the default is one notification a minute for 2 minutes.
- **Custom**:
  - 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 time frame. For example, you can set the **Stop Repetition After** value for 5 minutes, and the **Pause between Notifications** value to 30 seconds. The notification can be repeated up to 9 times. However, if the **Stop Repetition After** value is 5 minutes, but the **Pause between Notifications** value is 6 minutes, the notification is repeated only once.

Alert notifications repeat until one of the following actions occur:

- The recipient responds to the alert from at least one device.
- The defined time frame for repeat notifications elapses.
- The alert ends.

Option: **Deliver Alert with Sound**

Select **Yes** or **No** to deliver the alert with a sound.

Select and configure mass devices for an alert or alert template

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

1. In the **Mass Devices** section, select the check box next to each mass device you want to use to broadcast alerts.
2. Optionally, click **Options**.Each of the mass devices you selected in Step 1 appears as a separate tab on the Mass Devices Options screen that opens. The contents of each tab vary depending on the type of mass device selected.
3. Click each tab on the screen and then configure each mass device by selecting from the range of options that appear.
4. When you have finished configuring all of the mass devices, click **Save**.

Configure the schedule for an alert or alert template

The Schedule settings specify how long alerts remain active.

1. Scroll down to the **Schedule** section in the alert or alert template.
2. In the **Schedule** field, select **Activate Recurrence** if you want to create an alert that will be used more than once. If you select this option, additional fields appear at the bottom of the screen. You will configure them in steps 5 through 7 below.
3. In the **Alert Timings** section, specify the following values:
   - **Start Time**—By default, this field cannot be edited and displays the text, "Set during alert publishing." However, if the Activate Recurrence checkbox was selected in Step 2, the field displays hour, minute, and AM/PM fields that you can use to set the start time for the alert template.
   - **Alert Duration**—The amount of time the alert should be active. Use the drop-down list to specify whether the time is in minutes, hours, or days.
4. If you *did not* select **Activate Recurrence** in Step 2, click **Save** to finish creating the alert or alert template. If you *did* select **Activate Recurrence**, complete the following additional steps using the Recurrence-related fields on the screen.
5. In the **Recurrence Pattern** section, use the drop-down list to determine how often you want the alert to recur: daily, weekly, monthly, or yearly.
6. In the **Start Date** field of the **Recurrence Period** section, do one of the following:
   - Manually enter the day, month, and year that you want the alert to begin, writing the date in **MM/DD/YYYY** format.
   - Click and navigate to and then click the day, month, and year that you want to use.
7. In the **End Date** field, select one of the following three options:
   - **No end date**—The alert continues to recur until you or someone else manually deletes it, adds an end date to it, or limits the number of occurrences.
   - **End after <X> occurrences**—The alert continues to be sent out at the time interval you specified in Step 5 until it has been sent out the number of times you specify in this field.
   - **End by <date>**—The alert continues to be sent out until the date you select in this field.
8. Click **Save**.

Edit an alert template

Within BlackBerry AtHoc, alert templates typically consist of alert content, response options, a list of targeted recipients, and a list of delivery devices for a specific situation.

You can edit an existing alert template to change features such as the default header, body text, and target audience.

1. In the navigation bar, click the **Alerts**.
2. Click **Alert Templates**.
3. Use the search field or scroll down in the alert template list to locate the alert template you want to edit.
4. Click the name of the alert template.
5. Edit values in any of the following sections:
   - Alert template
   - Content
   - Users
   - Mass devices (Only available in English-language alert templates)
   - Schedule
6. Click **Save**.

Duplicate an alert template

Duplicating an alert template creates an exact copy of it in the system and can be used to speed up the creation of similar templates. You can duplicate any alert template that contains a checkbox next to its name.

1. In the navigation bar, click **Alerts**.
2. Click **Alert Templates**.
3. Use the search field or scroll down in the alert template list to locate the alert template you want to duplicate.
4. Select the checkbox beside the alert template name.

   Note: If the template does not have a checkbox beside its name, it cannot be duplicated.
5. Click **Duplicate**.
6. On the **New Alert Template** screen, make whatever changes you want to the alert template details.

   At a minimum, you should change the name of the alert template so that you can distinguish it from the original.
7. Click **Save**.

The screen refreshes and the new alert template appears in the list on the Alert Templates screen.

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

Delete an alert template

Within BlackBerry AtHoc, alert templates typically consist of alert content, response options, a list of targeted recipients, and a list of delivery devices for a specific situation.

You can delete alert templates individually or in groups from the Alert Templates screen.

1. In the navigation bar, click **Alerts**.
2. Click **Alert Templates**.
3. Use the search field or scroll down in the alert template list to locate each of the alert templates you want to delete.
4. Select the checkbox beside each alert template that you want to delete.
5. Click **Delete**.

   A confirmation popup screen opens, listing each of the alert templates you are about to delete.
6. Click **Delete**.

The Alert Templates screen refreshes to show the alert template list without the alert template or alert templates you deleted.

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 and publish alerts from the Alerts menu.

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

Before you begin you must have at least one of the following roles to publish an alert from the mobile app:

- Enterprise Administrator
- Organization Administrator
- Advanced Alert Manager and SDK User
- Alert Publisher and SDK User

Publish an alert from an existing alert template

Important: Before creating and publishing 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. Doing so will help you avoid creating a duplicate alert.

The most common way to create an alert is to open an existing alert template, modify its contents, and then publish it.

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

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

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

     Note: See Create an alert template for detailed instructions on how to fill in the content and target users.

View the details of a sent alert

If you have just clicked **Publish** to send an alert, you can access the Alert Summary report by clicking **Alert Summary** at the bottom of the Review and Publish screen.

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

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

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

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

The Alert Summary screen lists the current status of the alert: Live or Ended. For live alerts, the information on the page updates automatically every minute. You can manually update the screen at any time by clicking ↻.

Details tab

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

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

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

For live events, 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.

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 drop-down menu next to the number contains the following options:

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

The **Response Details** section of the Summary tab displays a list of all of the possible alert response options, each assigned a different color. Next to each option the total number of alert recipients who have selected that option is displayed. This information is also graphically represented on the screen by a circle divided into colored segments in proportion to the number of response options of each type that were selected.

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

- **Export Delivery Summary (CSV) for sent alert**: Click this option to create an exportable .csv file containing the names of all recipients who chose the corresponding response option. Where applicable, the .csv 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.

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 drop-down list on the Organizations tab contains a **Export Delivery Summary** option. There is no option to send the alert again to the selected organizations.

Mass Devices tab

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

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

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

Advanced Reports button

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

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

Edit an alert

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

- If the alert has a status of **Draft** or **Scheduled**, you can edit any of the details.
- If the alert has a status of **Live**, you can only edit the End Time for the alert.
- If the alert has a status of **Ended**, you cannot make any changes to it.

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 checkbox beside the alert name.
4. Click **More Actions** > **Edit**.
5. Make any changes you want to the unlocked fields.
6. Click **Save**.

Resend an alert

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

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click the alert that you want to resend.
4. On the **Alert Summary** screen, click the **Users Targeted**.
5. View the **Sent Details** section of the report.
6. To resend the alert to everyone in the original targeting list, for example if you want to make modifications to the original alert, do the following:
   a. Click the drop-down menu in the **Targeted** row.
   b. Select **Send alert to these users**.

   c. Optionally, revise the copy of the alert that opens.
   d. Click **Review and Publish**.
   e. Click **Publish**.
7. To resend the alert to everyone the alert was successfully sent to, for example, if you want to give them further details or instructions, do the following:
   a. Click the drop-down menu in the **Sent** row.
   b. Select **Send alert to these users**.
   c. Optionally, revise the copy of the alert that opens.
   d. Click **Review and Publish**.
   e. Click **Publish**.
8. To resend the alert to everyone whose receipt of the alert is either still in progress or has failed, do the following:
   a. Click the drop-down menu in the **In Progress or Failed** row.
   b. Select **Send alert to these users**.
   c. Optionally, revise the copy of the alert that opens by targeting new or additional personal devices.
   d. Click **Review and Publish**.
   e. Click **Publish**.

End an alert

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

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

The alert status changes from Live to Ended.

Delete an alert

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

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

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

Track alerts with advanced reports

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

View advanced reports

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

1. In the navigation bar, click **Alerts**.
2. Click **Sent Alerts**.
3. Click a live or ended alert.
4. Click **Advanced Reports**.
5. In the **Report** section, select a report from the **Select a Report** list.
6. Select a report type to view.

The report opens in a new browser screen.

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

Manage incoming alerts from the inbox

The Inbox displays information about live and expired alerts coming from mobile users. The Inbox provides organizations with a means of managing incoming alerts and monitoring what is happening in their system. Updates to the Inbox are fully automated, so if a new alert is received or an operator reviews or replies to an alert, the list will update immediately to display the new item. Alerts coming from mobile users and outside organizations are called incoming alerts.

Access the inbox

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

   The Inbox opens, showing all incoming alerts in the system. Alerts that have not yet been reviewed appear in bold font.

   The Inbox list displays the following for each incoming alert:

   - **Severity icon**: Hovering your cursor over the icon displays the severity level, which is one of the following: High, Moderate, Low, Informational, or Unknown.
   - **Alert title**: Displays the subject of the alert.
   - **Source type icon**: Displays a  if the source is a person or an  if the source is an organization.
   - **Source name**: Displays the name of the person or organization that created the alert.
   - **Creation date and time**: Displays the time and date stamp for the alert.
   - **Latitude, Longitude**: Displays GPS coordinates (for incoming live mobile alerts only).
   - **Alert type**: Displays the category of alert.
   - **Location icon**: Displays only if the related alert has a map associated with it.
   - **Attachments icon**: Displays only if the related alert has files, videos, or images attached to it.

Manage the situation map

Map provides an interactive crisis environment in which teams can manage an emergency by using the map to view people, create shapes, and manage incoming alerts. In the BlackBerry AtHoc management system, the map is found under **Settings** > **Basic** > **Map Settings**.

Access the situation map

This section describes how to work with the map, which provides a highly visual way to share information among end users that are part of a distribution list to which you are publishing. The map displays shapes, incoming alerts, people, and alert responses. It also includes links to multimedia files that are shared with mobile team members.

To open the map, click **Situation** in the navigation bar, and then click **Map**.

The Map screen opens and displays three colored tabs on the side: **Display**, **Inbox**, and **Tools**. These tabs allow you to manage objects, people, and shapes on the map and work with incoming alerts from mobile users and outside organizations.

When multiple people, pins (markers), alert responses, and incoming alerts are clustered together within a small area of a map, the Situation Map displays a large circle with a number on it, called a cluster, to let you know that multiple objects exist in that location.

Single-clicking on a cluster causes the list of clustered objects to appear in the Tools tab in the sidebar. Double-clicking on a cluster zooms the map in far enough to show each individual object in the cluster.

Add shapes to the map

You can add shapes to the map and define their properties through the Tools sidebar.

1. In the navigation bar, click **Situation** > **Map**.
2. If necessary, zoom in on the map to more easily see the area where you want to add the object.
3. Click to open the Tools sidebar.
4. On the **Tools** sidebar, click to select one of the drawing tools, and then move your mouse over the area of the map where you want to create the object.
   - For the **Marker** tool, click the mouse to specify a single point on the map.
   - For the **Circle** and **Square** tools, click and drag to set the size of the object.
   - For the **Polygon** tool:
     a. Click and release at the first place you want to start creating your own custom shape.
     b. Move your mouse to the end of the first edge, then click again to start creating the second edge.
     c. Continue the process until you have defined all edges and are back at the start of the first edge.
     d. Double-click to finish the creating the object. The border changes color to indicate that the object has been created.

   After you have finished creating the object, the **Tools** details screen opens.
5. Enter a name and description for the object.
6. Select the **Visibility** setting for the object. The setting you choose determines who can see the shape.
7. Select the map **Layer** that you want the object to appear on.
8. Optionally, select **Mobile Access** if you want the item to be visible on mobile devices.
9. Optionally, click **Add Media** if you want to add a video, photograph, or any other media to the object.
10. Click **Save** to add the new object to the layer you specified in Step 7.

Attach media to objects on the map

The BlackBerry AtHoc system allows you to attach media, such as images or video to the shapes and pins on the map so that you can share the media when sending alerts to your team. If you are the creator of an object, you can attach media when the object is first created or at any time in the future. If you are not the object creator, you can add media as long as you have the required permissions to view and modify the object.

1. In the navigation bar, click **Situation** > **Map**.
2. On the map, locate the object you want to add media to. If necessary, zoom in on the map to view the object better.
3. Click the shape or pin to select it.

   The border around the object changes color to indicate that it has been selected. The **Tools** sidebar opens.
4. Enter a name for the selected location.
5. Click **Add Media**.
6. Choose the media file in one of the following ways:
   - Select the file from the existing media files field.
   - Click **Upload Media** to access media files on your computer and upload them to your BlackBerry AtHoc media library.

   Note: Only .mpeg, .mp4, and .webm video formats and .gif, .jpeg, and .png image formats can be uploaded.
7. Click **Attach**.
8. On the **object properties edit** screen, click **Save**.

Operators can view full-sized versions of attached pictures and video by clicking the relevant thumbnail in the Tools sidebar.

Share map objects

Various participants in an organization have different types of permissions to view objects on the map, making it possible to restrict sensitive information to specific users. You can share incoming alerts, shapes, and pins (but not people) directly from a map by changing the visibility permissions for all users, the emergency team, organizations, or your team. You can also grant mobile access to users.

Share incoming alerts, shapes, and pins directly from a map

You can change visibility permissions and share Situation Map objects such as incoming alerts, shapes, and pins.

1. In the navigation bar, click **Situation** > **Map**.
2. On the **map**, locate the object you want to share. If necessary, zoom in on the map to view the object better.
3. Click the shape or incoming alert object to select it.

   The border around the object changes color to indicate that it has been selected. The **Tools** sidebar opens to display the object properties.
4. Click the  at the bottom of the screen to open the object properties edit screen.
5. Click **Visibility** to change the visibility permissions for the object.
6. Click **Layer** to change the layer in which the object appears.
7. Optionally, change the mobile device visibility of the object by selecting or deselecting **Mobile Access**.
8. Click **Save** to update the object properties.

Share people

Note: Only Administrator users have the ability to make the People layer visible on mobile maps. In addition, the permission is all-or-none, meaning all people become visible or no people are visible. Administrators cannot make some people visible and some not visible at the same time.

1. In the navigation bar, click **Situation** > **Map Settings**.

   The Map and Layers screen that appears provides separate areas for setting up and configuring maps, shape layers, and people layers, with default layers displayed for maps and layers.
2. In the **People layers** section, click next to the layer you want to make visible.
3. Click **Visibility** to change the visibility permissions for the layer.
4. Optionally, change the mobile device visibility of the object by selecting or deselecting **Display on mobile**.
5. Optionally, if you selected the check box in Step 5, select a time filter for displaying people on the mobile map by clicking **Show items with location updates within the following timeframe** and selecting one of the following options: All, 1 Week, 1 Day, 8 Hours, 4 Hours, 30 Minutes, Now (1 Minute).
6. Click **Done** to update the object properties.
7. Click **Save** or **Save + Exit** at the top of the Map and Layers screen to save your changes.

   Important: If you forget to do this, the changes you made to the People layer are not saved in the system, even if you clicked **Done** in Step 6.

Work with map layers

Shared Situational Awareness maps allow you to filter the map by layers for organizing and segregating information that can then be selectively displayed on a single map, with different users able to see different layers depending on their roles and permissions. These layers can include one for infrastructure, one for weather, one for only members of a private team, a shared one available to the public, and so on.

1. In the navigation bar, click **Situation** > **Map**.
2. On the map, click to open the Display sidebar.
3. In the **Layers** section, select the layers of the map that you want to view, or click **All** to view everything or **Default** to view only the default map layers.

   Note: The default layers of the map are configured on the Map and Layers screen, accessible to Administrators at **Settings** > **Situation** > **Map and Layers**.
4. In the **People** section of the **Display** sidebar, select the groups of people to be displayed on the map.

   Note: As with the Layers section, the default groups are configured by Administrator users at **Settings** > **Situation** > **Map and Layers**.
5. In the **Alert Responses** section of the sidebar, click next to an alert to expand it and view the alert responses that have been received.
6. Select the checkbox next to each response you would like to see on the map.

The map then refreshes and displays the responses you selected.

Monitor incoming alerts

Incoming alerts are created by external organization, or by users using their mobile devices and are displayed within the Map feature of BlackBerry AtHoc. There are three Incoming alerts categories—Mobile, Other (IPAWS), and Standard—all of which appear within the Inbox sidebar of the Maps screen.

1. In the navigation bar, click the **Situation** > **Map**.

2. Click .

   The Inbox sidebar opens, displaying a list of any Mobile, General, and IPAWS incoming alerts that are currently in the system.

   Click any of the incoming alerts to open the details screen. If you click a Mobile alert, it also displays on the map with a tool tip.
3. Optionally, use the **Filters** field at the bottom of the screen to modify the map display.

   You can use the filter fields to set the following:

   - The maximum age of an incoming alert that can appear on the screen. Use the slider bar to specify incoming alerts that are anywhere from 1 minute old to no limit.
   - Whether to display people and incoming alerts based on the range of visibility settings that have been used in creating the incoming alerts.

     Note: The **Show by visibility** filter only appears if you belong to at least one team within the Emergency Community.
   - Whether to display only users who are accessible on mobile devices, only users who are not accessible on mobile devices, or all users.

Publish alerts from the map

You can publish alerts from any object on the map. For example, if there is an emergency incoming alert, you might want to publish an alert to a team to respond. Or, if the incoming alert is represented by a shape on the map, you can send the coordinates of the shape and any relevant pictures to your team by publishing an alert.

1. In the navigation bar, click **Situation** > **Map**.
2. Do one of the following:

   - Locate the object on the map. If necessary, zoom in on the map to view the object better.
   - Click and select an incoming alert.
3. Select the object to open the details view.
4. Click .
5. Enter a title and message for the alert.
6. Add any response options.
7. Enter the targeted recipients, including teams and organizations, and verify that your targeted audience is accessible.
8. Click **Publish Now** at the bottom of the sidebar.

   A notification appears, containing a link to the User Tracking report for the alert.
9. Click **OK**.
10. Optionally, click **Display** on the map to review alert responses.

Enable Collaboration in BlackBerry AtHoc

When you set up collaboration, you enable mobile app users to effectively communicate with other users and administrators. Only administrators can initiate collaboration.

1. Log in to the BlackBerry AtHoc management system.
2. Navigate to **Settings > System Setup > Feature Enablement**.
3. In the **Feature Name** list, click **IsCollaborationSupported**. The Edit Feature Enablement dialog box appears.
4. In the **Enabled** list, click **True**.
5. Click **Save**.

To initiate a collaboration session with other users, navigate to Collaborate > Collaborate.

Note: You might need to log out of the BlackBerry AtHoc management system and log back in to see the Collaborate tab in the navigation bar.

Manage users

The following topics describe how to manage users in the BlackBerry AtHoc system. Users can be the end users that receive alerts, operators with varying degrees of privileges, or administrators that configure BlackBerry AtHoc settings.

The Users screen lists all users associated with an organization and provides you with tools to manage the status and details for those users.

Create a user

Note: You must have End User Manager privileges to create users.

Note: If the "Enterprise Features" setting is enabled in the General Settings of an enterprise organization, the BlackBerry AtHoc system enforces user uniqueness in the enterprise organization and its sub organizations. Users created in the enterprise organization or in any of its sub organizations must have a unique username and Mapping ID.

1. In the navigation bar, click **Users** > **Users**.
2. Click **New**.

   Note: Fields marked with an asterisk (*) on the New User screen are required.
3. In the **Basic Information** section, enter the following details about the user:
   - **Username**—The name the user is assigned by the system. Usernames are frequently imported from external systems and cannot be edited later.
   - **First** and **Last Name**
   - **Display Name**—The name used to refer to the user within the system. This field can be edited later by the end user.
   - **Organizational Hierarchy**—If available, click the **/** (forward slash). On the pop-up screen that appears, navigate to the specific organization to which the user belongs. Click **Apply** to add the organization information to their record in the system.
   - Any custom fields added by the administrators, including details such as CPR certification status, Emergency Community membership, or special skills.
4. In the **Numbers** section, enter the work number, mobile number, pager numbers, and any other numbers that could be used to contact the user.

   Note: International numbers and numbers with extensions are supported.

   BlackBerry AtHoc then runs a validation check to make sure the number is valid. If it is not, an "Invalid Phone Number" error appears under the text field. You cannot save the new user information until you correct or remove the number.

   Note: For pagers, only devices that are enabled for the organization appear in the list.
5. In the **Online Addresses** section, enter work and home email addresses.
6. In the **Physical Addresses** section, enter work and home addresses.
7. In the **Distribution List Membership** section, specify the distribution lists the user is a member of.

   Note: Required memberships are provided by default and cannot be deleted. If you do not have management permissions for a group, the group is read-only.
8. In the **Advanced Information** section, which is configurable for each system, complete any required fields plus any of the non-required fields you want to include in the account details for the user.
9. Provide a password that meets the displayed rules, if required.
10. Click **Save**.

The details of the new user then appear in summary form on the screen. You can then return to the Users screen or grant the user operator permissions.

Grant Operator Permissions

Note: After you make changes to publisher permissions, you must disconnect and re-connect from the mobile app.

1. Create a user.
2. On the **User Details** screen, click **Grant Operator Permissions**.
3. On the **Operator Permissions** screen, from the **Operator Roles** list, select each of the roles you want to assign to the user.

   As you select roles, they appear on the screen under the Operator Roles list. If you select more than three roles, the first three are displayed and the rest can be seen by clicking the scrollbar that appears in the field.
4. Optionally, enter and confirm a password that meets the specified requirements.
5. Optionally, select the check boxes to specify if the user must change their password at the next login, and whether the password expires.
6. Click **Save**.

Edit operator permissions

If you want to revoke all Operator permissions for a user, see Revoke operator permissions.

Note: After you make changes to publisher permissions, you must disconnect from and reconnect to the mobile app.

1. In the navigation bar, click **Users** > **Users**.
2. Click the operator name in the list.
3. On the **user details** screen, click **Edit Operator Permissions**.
4. On the **Operator Permissions** screen, from the **Operator Roles** list, select each of the roles you want to assign to the user.
5. To remove an operator permission, click **X** next to the name.
6. Click **Save**.

Revoke operator permissions

Revoke operator permissions to remove all permissions.

1. In the navigation bar, click **Users** > **Users**.
2. Click the name of the operator in the list. The user details screen opens, displaying all of the information for that user in the system.
3. Click **More Actions** > **Revoke Operator Permissions**.

   A warning notification screen appears, asking "Are you sure you want to revoke Operator Permissions for this user?" and informing you that this action cannot be reversed. Revoking Operator permissions cannot be reversed, but you can later assign the permissions to the operator again using the Edit Operator Permissions button on the user details screen.
4. Click **Revoke**.

Note: If a user is logged in to the system when their operator permissions are revoked, they are logged out on their next page navigation and redirected to an error screen with the following message: "You do not have the required Operator Permissions to access this page. Contact your administrator."

View user details

You must have End User Manager privileges to view detailed information about users in the system, including contact address, memberships, login information and location information.

1. In the navigation bar, click **Users** > **Users**.
2. Click the user name.

   The detail screen for the user appears. The details screen displays the following information about the user:

   - Basic information, including username, first and last name and date the user was created.
   - Numbers
   - Online addresses
   - Physical addresses
   - Distribution list membership
   - Permissions
   - Login and location
   - User activity
   - Any user attributes defined by administrators

Edit user details

You can make changes to the details of an individual in the system. You must have End User Manager privileges to edit user details.

1. In the navigation bar, click **Users** > **Users**.
2. Click the  next to the name of the user whose details you want to edit.
3. Make changes to any of the user fields in the following sections of the screen:

   - Basic Information
   - Numbers
   - Online Addresses
   - Physical Addresses
   - Distribution List Membership
   - Login and Location
   - Any user attributes defined by administrators

   Note: System-generated user details such as Desktop Software Session Information, Mobile Device Location, and most of the User Activity information cannot be edited.
4. Click **Save**.

BlackBerry AtHoc Customer Support Portal

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

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

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

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada