BlackBerry AtHoc
Mobile App User Guide

4.13

2023-08-22Z

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 the Apple App and Google Play stores.

Combined with the BlackBerry AtHoc management system, 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.

Supported OS versions

- Android: 13.0, 12.0, 11.0, 10.0
- iOS: iOS 16, iOS 15
- iPadOS: with iOS 14

App version support

The following BlackBerry AtHoc mobile app versions are no longer supported:

- 3.5.x
- 4.0
- 4.1.x
- 4.2
- 4.3
- 4.3.1
- 4.4
- 4.5
- 4.6
- 4.6.1
- 4.7
- 4.7.1

Home screen

This is the main screen where most interactions take place and where the core utilities of the application appear.

Some of the following features may be available on the Home screen depending on the permissions from your operator.

Item	Name	Description
≡	Menu	Opens the navigation menu.

Item	Name	Description
◥	Track Me	Periodically sends your location to your organization for the duration you choose.
◉ / ◉	Check In/Check Out	Sends your location and timestamp to the server.
➕	Alert Publishing	Displays the login screen on tapping the icon. After logging in the alert template screen appears that has the list of alert templates to publish alerts.
All Inbox	Change view	**All**: Displays all activities including reports, tracking, and registration. **Inbox**: Displays all alerts that have been sent to you.
You are connected to *organization-name*	Organization settings	Displays information about the organization you are currently connected to. For more information, see Organization settings.
💬	Alerts	Displays the number of unread alerts as a badge on the icon.
Emergency Report ❗ ‹‹‹ ❗ ››› 📄	Red knob	Slide the red knob to view the following options: • **Report**: Sends information to the central operations center of an organization. Users can select a template to send a report. • **Emergency**: Sends duress messages.
👥	Collaborate	Displays a list of collaborations that you are involved in.

Menu

Tap ≡ at the top left corner of the home screen. From the menu you can access the following items:

Name	Description
My Organization	Displays the name and logo of the organization you are connected to.
Manage Organization	Adds and manages organizations to receive alerts from one or multiple organizations. Specifies the primary organization.

Name	Description
Personal Alert Button	Displays details about paired Bluetooth buttons. Provides features to pair, test, and unpair a Bluetooth device.
My Profile	Displays your user information including name, email, and phone numbers.
Subscriptions	Displays your organization subscriptions.
FAQs	Displays the list of frequently asked questions.
Send Feedback	Opens the email client to send feedback or suggestions.
Send Admin Log	Opens the email client to send a log file to report issues. The default email address, `support@athoc.com` is removed from sending Admin logs flow. When user taps on Send Log button, in the compose email screen, the "To" field is blank.
About Us	Displays the build version number.
Logout	Logs you out of the app. You must have the Alert Publishing or Accountability Manager permission. This option displays only if the user is authenticated and logged in to an organization
Terms of Use	Displays the BlackBerry Solution License Agreement.

Organization settings

Tap an organization name on the home screen to open the Organization Details screen to access the following settings.

Name	Description
Organization Details	Displays information about the selected organization.
Make this organization primary	This option is displayed if you are connected to multiple organizations. Select this option to make the selected organization your primary organization. The primary organization is the organization where advanced features including sending an alert, emergency, report, check-in, or check-out are performed.
You Are Connected Using	Displays the email address you are using to connect to the selected organization.
Keep my location in BlackBerry AtHoc updated	Updates the BlackBerry AtHoc system with your location when you respond to an alert or update your status.

Name	Description
Biometric authentication	If enabled for your organization, the organization settings screen displays the option to enable biometric authentication. For more information, see Enable or disable biometric authentication.
Available Features	Displays the list of available features and your current status (Enabled or Disabled) for each feature. Available features include: Alerts, Emergencies, Reports, Check In / Check Out, Tracking, Alert Publishing, and Collaboration. If authentication is enabled in your system, your authentication type (Username and Password or Smart Card) is displayed.

Location services

Turn on location services on your mobile device to ensure the best experience when using the BlackBerry AtHoc mobile app. Enabling location services provides access to advanced features such as sending emergencies and reports, performing check-ins and check-outs, and enabling tracking.

If you are using an Apple iPhone running iOS 14 or later, ensure the Precise Location setting is turned on. Turning Precise Location on enables the BlackBerry AtHoc mobile app to access your location more accurately. When this setting is turned off, the mobile app can only access your approximate location. Turn on the Precise Location setting under **Settings** > **Privacy** > **Location Services** > **AtHoc**.

On the Organization Details screen, tap the **When responding to alerts and updating status** setting to the **On** position to send updated location information to your organization.

VPN requirement

If you are using the mobile app with an on-premises BlackBerry AtHoc management system, you must establish a VPN connection from your mobile phone to your organization's corporate network before performing any of the following tasks from the mobile app:

- Publishing an alert
- Sending a report
- Updating the status of an accountability event
- Viewing or participating in collaborations
- Updating your user profile
- Subscribing to organizations
- Logging in using a smart card

Set up the BlackBerry AtHoc mobile app

The BlackBerry AtHoc mobile app is available as a download from Apple App store, Google Play store, or 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.

Install the BlackBerry AtHoc mobile app

If you have the BlackBerry AtHoc mobile app on your device, skip this section and go to the Register the mobile app section. If you don't have the app, download it from the Google Play or Apple App store.

Google Play Store

To download and install the BlackBerry AtHoc mobile app from Google Play (for Android devices), complete the following steps:

1. On your Android device, tap ▶.

   Note: You can also go to play.google.com.
2. In the **Search** field, type **BlackBerry AtHoc** and press 🔍.
3. Select ⬛ from the list of search results.
4. Tap **Install**.
5. Do one of the following:
   - If scheduled location access is enabled for your organization, on the **"AtHoc" Would Like to Access Your Location** dialog, tap **Continue**.
     a. On the **Allow AtHoc to access this device's location?** dialog, tap **While using the app**.
     b. On the **Location permission** screen, tap **Allow all the time**, **Allow only while using the app**, or **Ask every time**.
   - If scheduled location access is not enabled for your organization, a dialog is displayed that explains what the application can do to your device. Tap **Accept**.

After the BlackBerry AtHoc mobile app is installed, a ⬛ appears on your device home screen

Apple App Store

To download and install the BlackBerry AtHoc mobile app from the Apple App store (for iOS devices), complete the following steps:

1. On your iOS device, tap 🅰.
2. Tap the **Search** icon at the bottom of the screen.
3. n the search field, type **BlackBerry AtHoc**.
4. Tap **Search**.
5. Tap the **BlackBerry AtHoc** app to download.
6. Tap **GET** to the right of the app.
7. Tap **Install**.
8. Do one of the following:

- If scheduled location access is enabled for your organization, on the **"AtHoc" Would Like to Access Your Location** dialog, tap **Continue**.
    a. On the **Allow AtHoc to access this device's location?** dialog, tap **While using the app**.
    b. On the **Location permission** screen, tap **Allow While Using App** or **Allow Once**.

    Note: If you are using an Apple iPhone running iOS 14 or later, turn on the Precise Location setting.
- If scheduled location access is not enabled for your organization, a dialog is displayed that explains what the application can do to your device. Tap **Accept**.

After the BlackBerry AtHoc mobile app is installed, a appears on your device home screen.

Register the mobile app

Prerequisites

- Download and install the BlackBerry AtHoc mobile app from the Google Play or Apple App store.
- Before you register the BlackBerry AtHoc mobile app on your device, you may need the organization code provided by your BlackBerry AtHoc administrator. If your organization has a mapped email domain, you can register using your work email address without providing an organization code.
- 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. Tap **Continue**.
3. On the **Register for Alerts** screen, if it is not displayed, enter the email address that is associated with your BlackBerry AtHoc user profile. If you do not already have a BlackBerry AtHoc user profile, one will be created for you automatically.
4. Tap **Send** or . A verification page with a confirmation message is displayed.
5. Check your email for a verification email from BlackBerry AtHoc with a link to activate your account to your registered email address.
6. On the verification email, click **Verify Now**.
7. After the email address is verified, do one of the following:

   - If your email address domain maps to a domain in the BlackBerry AtHoc system, the name of your organization appears on the Registration screen. You can tap **Enter your organization code** to register with a different organization. Tap **Continue** to register with the displayed organization. The My Profile page opens. Add additional contact information to your user profile, then tap **Save**. On the **Changes have been saved** pop-up, click **OK**. The Inbox opens.
   - If the email you entered does not match a mapped domain in the BlackBerry AtHoc system, the Add Organization screen opens on your device. Enter the organization code provided by your BlackBerry AtHoc administrator and tap **Send** or . The Inbox opens.

Update your user profile

1. Tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **My Profile**.
3. Optionally, if you are connected to multiple organizations, on the **Select Profile** screen, select an organization.
4. On the **My Profile** page, tap to update any of the following fields:

    - First Name
    - Last Name
    - Email
    - Work Phone
    - Mobile Phone
    - Text Messaging
    - Preferred Alert Language

5. Tap **Save**.
6. On the confirmation pop-up, click **OK**.

Pair a V.ALRT personal alert button with the BlackBerry AtHoc mobile app

You can pair a personal alert button with the BlackBerry AtHoc mobile app to be able to quickly and discretely publish an emergency alert.

Before you begin:

- Users must have permission to publish emergency alerts using a Bluetooth Alert Button.
- Bluetooth must be enabled on the device with the BlackBerry AtHoc mobile app installed on it.
- The V.ALRT personal alert button must be within two meters of the device with the BlackBerry AtHoc mobile app installed on it.

1. On the BlackBerry AtHoc mobile app, tap ≡ > **Personal Alert Button**.
2. Tap **Add** (+).

   The BlackBerry AtHoc mobile app searches for and lists all active **V.ALRT** personal alert buttons within a two meter range. The **V.ALRT** personal alert button flashes a red light when it is in discovery mode.
3. Tap the **V.ALRT XX:XX:XX** personal alert button that you want to pair. For example, V.ALRT C3:60:E6 Bluetooth Alert Button.
4. Tap **PAIR**. The V.ALRT button flashes a green light while pairing. Wait until you see the following confirmations:

   - When the pairing completes, on the **Button Pairing** screen, you will receive a message that the device was successfully paired and a green check mark is displayed.
   - When the connection completes, you will receive a "Button Connected. V.ALRT Personal Alert Button has been connected." message.
5. After you receive the confirmation messages, tap **Done**.

You can monitor the connectivity status, connectivity strength, and battery levels on your personal alert button. The following statuses are displayed:

- **Red**: You are disconnected from the device but paired.
- **Green**: You are successfully connected to the device.

If your device is not paired with the personal alert button, a message with a **Start Pairing** link is displayed on the Personal Alert Button screen.

Test the V.ALRT personal alert button

After the V.ALRT personal alert button is paired with the BlackBerry AtHoc mobile app, you can test it to make sure that it is functioning as expected.

1. On the BlackBerry AtHoc mobile app, tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **Personal Alert Button**.
3. Tap **TEST**.
4. Tap the Bluetooth button three times in two seconds. If you perform this task correctly, you will receive the confirmation message, "Excellent! Button is ready for use".
5. Tap **Done**.

Publish a V.ALRT emergency alert

Before you begin:

- Users must have permission to publish emergency alerts using a Bluetooth Alert Button.
- The V.ALRT personal alert button must be paired with the BlackBerry AtHoc mobile app.

Tap your V.ALRT personal alert button 3 times in 2 seconds to publish an emergency alert.

After the alert is published, you will receive the following notification message: "Button is pressed. Emergency has been sent successfully."

Unpair your Bluetooth alert button

1. On the BlackBerry AtHoc mobile app, tap ≡ > **Personal Alert Button**.
2. Tap the personal alert button that is paired with the mobile app.
3. Tap **Unpair**.
4. Tap **Unpair** to confirm that you want to unpair the device.

When the upairing completes, the personal alert button makes a quick beep sound and displays a flashing red light.

Respond to alerts

The main function of the BlackBerry AtHoc mobile app is to respond to incoming alerts.

1. Tap on your device.
2. Tap the alert you want to view and respond to.

   Alert details can include instructions such as evacuation information, response options, and attachments.
3. Optionally, if there are attachments included in the alert, tap an attachment to view it. If there are multiple attachments, you can swipe right and left to view them. If there are .html, .kml, or .xml file attachments, you can tap the file and then tap **Download** to download it to the document directory on your device.

   Note: On Android devices, on the window that appears, select the folder you want to download the file to.
4. Optionally, if there is a location associated with the alert, tap **View on map** to view the location on a map.
5. Tap **Reply** or **Acknowledge** to respond to the alert. You will see an **Acknowledge** button when the alert does not have any response options.
6. Tap a response option.

   Note: Response options may include conference call bridge numbers, which are visible under the text of the response option. When you select this response option, the app initiates a call. The passcode is automatically dialed. If you are disconnected, both the phone number and pass code are available on the alert details screen.

The Alert Details screen displays the alert that you responded to with the response option you selected.

Note: Ended alerts are removed from the Inbox after 24 hours. This is a system setting that cannot be changed.

Alert icons

The colors and icons identify the state of each alert. The following table describes the alert icons:

Icon	Icon Name	Description
●	Blue dot	A blue dot next to the title of an alert indicates that the user has not opened the alert. The blue dot disappears when the alert is opened by the user.
LIVE ↩	Live with a reply arrow	A Live alert with a reply arrow indicates that a response is requested and that you have not responded to the alert.
LIVE	Live without reply arrow	A Live alert without a reply arrow indicates that you have responded to the alert.
ENDED	Ended	An alert with an Ended icon indicates that the alert has ended. You may or may not have viewed or responded to the alert.
❗	High	A high severity alert. High severity is reserved for extreme emergencies.
⚠	Moderate	A moderate severity alert.

Icon	Icon Name	Description
⬇	Low	A low severity alert.
?	Unknown	An unknown severity alert.
ℹ	Informational	An alert that includes information. For example, a meeting invite.
🌐	Globe	An alert with a globe icon indicates that a location is associated with the alert.
📎	Attachment	An alert with an attachment icon indicates that the alert includes one or more attachments.

View alert responses

1. To view the alert response delivery summary, tap **Alert Name**.
2. Do one of the following:
   - If smart card authentication is enabled, a certificate selection window opens on your device. Tap a valid certificate and then tap **Continue**.
   - If smart card authentication is not enabled, click **OK** on the **Enable biometric authentication** window. The Face ID or Touch ID screen opens. Touch the fingerprint sensor or use Face ID to authenticate.

     Note: If biometric authentication is not enabled on your device, or if this is the first time you are using biometric authentication, you are redirected to the login screen to provide your username and password. If you click **Don't Use** you are redirected to the login screen.
   - If smart card and biometric authentication are not enabled, enter your username and password on the login screen.

     Note: If the biometric or smart card authentication fails, you have the option to continue by entering your username and password.

   When authentication is successful, the following statuses are displayed:
   - **Targeted**: The number of targeted users to send alerts to.
   - **Sent**: The number of users that the alerts were sent to.
   - **Responded**: The number of users who responded to the alert. The Responded count indicates the number of people who have responded.
   - **Not Responded**: The number of users who have not responded to the alert.
3. Tap **>** to view a list of users who have responded using a specific response option (for example, I am safe).
4. In the **Search for users** field, you can search for a specific user who has sent the selected response.
5. Tap on a user in the list to view their contact details.
6. If you need to contact a user, do one of the following:
   - Tap **Call** to call the user.
   - Tap **Message** to send a message to the user.
   - Tap **Email address** to send an email message to the user.

Update the status of an accountability event

This section describes how to respond to accountability events.

1. Tap ⬛ on your device.
2. Tap an accountability event.
3. Optionally, if there are attachments included in the event, tap an attachment to view it. If there are multiple attachments, you can swipe right and left to view them.
4. Tap **Update Status**.
5. Tap a status.
6. Optionally, pull down the **Manage User's Status** screen to refresh the display and view the user's latest status.

You can continue to update your status for the duration of the event.

Note: If you do not respond to the event, reminder messages are sent to you at intervals until the event ends. The **Related Messages** field displays the number of messages received for a particular event. Tap the **Related Messages** field to view the messages.

Check Accountability Officer availability

When an accountability event is sent to an Accountability Officer (AO) to reply on behalf of targeted users, the operator who initiated the accountability event from BlackBerry AtHoc does not know whether AOs are available to do their job. To enable operators to confirm AOs are available, a response option is added for AOs.

Note: You must have Accountability Manager and Accountability Officer permissions to manage users.

1. Tap ⬛ on your device.
2. Tap the accountability event.
3. Optionally, if your administrator has enabled smart card authentication, a certificate selection window opens on your device. Tap a valid certificate and then tap **Continue**.
4. Tap **Reply**. The response options are displayed.
5. Tap one of the following options depending on your availability:

   - **I am available to update user status**
   - **I am not available to update user status**
6. If you tap **I am available to update user status**, complete the following steps:

   a. Tap **I am available to update user status**. A pop-up message with options is displayed.
   b. Tap **Manage Users' status** to update the users' status or tap **Close** to close the message window.
   c. When you tap **Manage Users' status**, the Manage Users status screen opens.
   d. From the list of users, tap **Manage** to update the status of the user you want.
   e. From the **Status** list, select a status.
   f. Optionally, in the **Comments** text box, add a comment.
   g. Tap ✓.
7. If you tap **I am not available to update user status**, your status gets updated.

When an accountability event has ended, you can only view the status history of the impacted users. You cannot edit the status of the users.

Accountability event icons

The colors and icons identify the category of each event. The following table describes the accountability event icons:

| Icon	Icon Name	Description
●	Blue dot	A blue dot next to the title of the accountability event indicates that the user has not opened the accountability event. The blue dot disappears when the accountability event is opened by the user.
⦿	Person	A Person icon indicates an accountability event.
LIVE | ↩	Live with Reply	A Live accountability event or accountability officer event with a Reply arrow indicates that a status update is requested.
LIVE | ↩	Live with Replied	A Live accountability event with a Replied arrow indicates that you have updated the status of the accountability event. A Replied icon replaces the Reply icon.
LIVE	Live	A Live accountability officer event indicates that the accountability officer has responded to the event.
📋	AO	An accountability officer event.
ENDED	Ended	An accountability event with Ended icon indicates that the accountability event has ended. You may or may not have updated your status for that accountability event.
🔴	High	An accountability event with a high severity. High severity is reserved for extreme emergencies.
⚠	Moderate	An accountability event with moderate severity.
🟢	Low	An accountability event with low severity.
⦾	Unknown	An accountability event with an unknown severity.
ℹ	Informational	An accountability event that includes information. For example, a meeting invite.
🌐	Globe	An accountability event with a globe icon indicates that a location is associated with the event.
📎	Attachment	An accountability event with an attachment icon indicates that the event includes one or more attachments.

Manage organizations

This section describes how you can connect, disconnect, or subscribe to organizations. You can connect to and receive alerts from multiple organizations at the same time. You can send alerts, reports, emergencies, check-ins and check-outs from your primary organization.

Add a new organization

You can be registered with one or more organizations. This section describes how to add a new organization.

Note: Ensure you have the organization code provided by BlackBerry AtHoc.

1. Tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **Manage Organization**.
3. On the **Manage Organization** screen, tap ⧉ (Android) or **Add** (iOS).
4. On the **Registration** screen, do one of the following:
   - From the list, select the registered email address to connect to the new organization, and tap **Continue**.
   - Enter a new email address to register with the BlackBerry AtHoc mobile app and complete the steps detailed in the Register the mobile app section.
5. From the list, select the registered email address to connect to the new organization, and tap **Continue**.
6. On the **Add Organization** screen, enter the new organization code.
7. Tap **OK** on the confirmation message.
8. On the **New organization settings received** message, tap **Allow**.

You are now connected to the new organization. If you are connected to multiple organizations, the organization you connect to last becomes the primary organization. If you want to designate a different connected organization as the primary organization, tap ≡ > **Manage Organization** and select the organization to designate as the primary organization. On the organization details page, tap the **Make this organization primary** setting to the **On** position.

Select a primary organization

You can connect to multiple organizations at the same time and receive and respond to alerts from them. The primary organization is the organization where alerts, emergencies, reports, check-ins and check-outs are sent from. The last organization you connect to is designated as the primary organization. You can select any connected organization as your primary organization. Only one organization can be the primary organization. On the home page, your primary organization appears highlighted and is labelled as "Primary."

1. Tap ≡.
2. Tap **Manage Organization**.
3. On the **Manage Organization** screen, tap the organization you want to select as your primary organization.
4. On the organization details screen, tap the **Make this organization primary** setting to the **On** position.
5. On the confirmation window, click **Continue**.

Subscribe to organizations

If your administrator has configured the ability for users to subscribe to different organizations, you can subscribe to any organization that has been configured for subscription from the Subscriptions screen.

When you subscribe to another organization, you can be targeted in alerts and accountability events from both your home organization and your subscribed organizations. You can subscribe to a maximum of 10 organizations.

Dependent users cannot be subscribed to organizations. If you subscribe to an organization your dependent users remain in your home organization and are still targetable in alerts and events from the home organization. They cannot be targeted from any subscribed organizations.

You can cancel your organization subscriptions at any time from the Subscriptions screen.

1. Tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **Subscriptions**.
3. On the **Subscriptions** page, tap ⊕ **Add Subscription**.
4. On the **Select Organizations** page, search for and tap the organization you want to subscribe to.
5. Optionally, select a start date for the subscription. If you do not select a start date, the current date is used.
6. Optionally, select an end date for the subscription.
7. Tap **Save**.
8. Optionally, to remove an organization subscription, tap ⊖ beside the organization, and then tap **Confirm** in the **Delete Subscription** window that appears.

Disconnect from an organization

If you do not want to receive alerts from any organization you are registered to, you can disconnect from the organization.

1. Tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **Manage Organization**.
3. On the **Manage Organization** screen, tap the name of an organization.
4. On the organization details screen, tap **Disconnect**.
5. On the confirmation message, tap **Disconnect**.

Enable or disable biometric authentication

When you start the alert publish flow from the mobile app, you can choose to log in using biometric authentication on your device. Biometric authentication enables operators to quickly authenticate on their device without the need to enter a username and password. When biometric authentication is enabled, the app displays a face or fingerprint authentication screen when the alert publishing flow starts. You can also use biometric authentication to view the alert summary for a sent alert.

When biometric authentication is enabled, if smart card authentication is then enabled, biometric authentication is disabled and the **Enable biometric authentication** setting is not displayed. A message is displayed on the mobile app to notify the end user.

Before you begin:

- Biometric authentication must be supported and set up on your device. iOS devices support Touch ID and Face ID. Android devices support Touch ID.
- BlackBerry AtHoc management system release 7.10 or later release.

1. Tap BlackBerry AtHoc mobile app to launch the app.
2. On the **Organization settings** page, tap the **Enable biometric authentication for alert publishing and reporting** setting to the **On** position.
3. On the **Enable biometric authentication** screen, tap **OK**.
4. On the **Login** screen, enter your username and password.
5. Optionally, when biometric authentication is enabled, tap the **Enable biometric authentication for alert** setting to the **Off** position to disable biometric authentication.

Advanced features

This section describes the advance features a user can use on the mobile app. The advanced features that you can see on your mobile app depend on the distribution list selected by the BlackBerry AtHoc administrator. Each feature in the Advanced Features section on the Mobile App settings page includes its own menu to select a distribution list. If you are connected to multiple organizations, advanced features happen on your primary organization. For more information, see Select a primary organization.

Publish an alert

Alerts are communications sent to your organization, to mobile users, or to outside organizations. A user with BlackBerry AtHoc operator permissions can publish alerts using predefined alert templates. If the management system operator selects the "Available for mobile publishing" check box in the alert template, then that alert template appears in the alert publisher template list in the mobile app. 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.

Note: You must have alert publishing permissions.

If you are connected to multiple organizations, alerts are published from your primary organization. For more information, see Select a primary organization.

1. Open the BlackBerry AtHoc mobile app on your device.
2. Tap ＋ at the top right corner of the home screen.

   Tip: You can also press and hold the BlackBerry AtHoc mobile app icon to open the alert template screen.
3. Do one of the following:

   - If smart card authentication is enabled, a certificate selection window opens on your device. Tap a valid certificate and then tap **Continue**.
   - If smart card authentication is not enabled, click **OK** on the **Enable biometric authentication** window. The Face ID or Touch ID screen opens. Touch the fingerprint sensor or use Face ID to authenticate.

     Note: If biometric authentication is not enabled on your device, or if this is the first time you are using biometric authentication, you are redirected to the login screen to provide your username and password. If you click **Don't Use** you are redirected to the login screen.

   Note: If the biometric or smart card authentication are not enabled or fail, you can authenticate by entering your username and password on the login screen.
4. On the **Template** screen, tap the template you want to publish.

   Tip: If the title of a template is truncated, you can long press (Android) or 3D touch (iOS) to view the complete title in a message box. Tap outside of the message box to close it and return to the alert template list.
5. Optionally, tap ✎ next to a section to make changes, then tap ✓ to save the changes.
6. Tap ➢.
7. On the **Publishing Confirmation** message, review the content.
8. Tap **Publish**.
9. Optionally, to end the alert, tap the **All** tab on the home screen, then select the alert. On the alert details screen, tap **End Alert**.

Edit the alert template

1. In the **Title** section, tap ✎ and do the following:

    a. From the **Severity** list, select a severity.

    b. From the **Type** list, select a type.

    c. In the **Title** field, enter a name.

    d. In the **Body** field, enter the content of the alert.

    The Severity, Type, and Body that you set in the Title section display on the template screen.

2. In the **Response Option** section, tap ✏ and do the following:

    a. Tap **Add Response Option** to add response options.

    b. Tap ✕ to remove a response option.

    c. Tap ✓ to save the changes.

    The Response Options section displays the response options.

3. In the **Target Users** section, tap ✏ and do the following:

    a. Tap the distribution list you want to edit. The following options are displayed:

       • **Targeted**: All users in that distribution list are selected.

       • **None**: No user is selected.

       • **Blocked**: All users in that distribution list are blocked.

    b. Tap an option.

    c. Tap ✓ to save the changes.

4. In the **Personal Devices** section, tap ✏ and do the following:

    a. Tap the device you want to target.

    b. Tap ✓ to save the changes.

Send an emergency

The Emergency feature (⚠) sends a duress message and device location to your organization.

Note: Ensure that your device location services are enabled.

Note: If you are using an Apple iPhone running iOS 14 or later, turn the Precise Location setting on at **Settings** > **Privacy** > **Location Services** > **AtHoc**.

If you are connected to multiple organizations, emergencies are sent from your primary organization. For more information, see Select a primary organization.

1. Open the BlackBerry AtHoc mobile app on your device.

2. On the home screen, slide the 🔴 to the left to create an emergency.

3. A dialog appears with a countdown of 5 seconds with the options **Cancel** and **Send Now**. Choosing **Cancel** cancels the report. **Send Now** sends a duress message immediately. If the countdown reaches zero without you choosing either option, the emergency is reported and your location is sent. A screen is displayed where you can enter messages.

4. Optionally, tap 📕 to make a call, add a message with additional information, or tap 📷 to attach a video or photo.

Note: You can also send an emergency using a paired personal alert button. For more information, see Publish a V.ALRT emergency alert.

Note: You can also send an emergency using the KNOX button on supported Samsung devices. For more information, see Send an emergency using the Top key on Samsung Knox devices.

Send an emergency using the Top key on Samsung Knox devices

You can press the Top key twice within 1 second on supported Samsung Knox devices to send a BlackBerry AtHoc emergency.

If your mobile device is a managed device, you do not need to map the Top key. If your mobile device is unmanaged, map the Top key with BlackBerry AtHoc in your device settings.

The BlackBerry AtHoc mobile app must be running on your device and location services must be enabled to send an emergency using the Top key.

1. On your supported Samsung Knox device, tap **Settings**.
2. On the **Settings** screen, tap **Advanced features**.
3. On the **Advanced features** screen, tap **Top key**.
4. On the **Top key** screen, tap to enable the **Use Top key with app** option.
5. On the **Use Top key with app** screen, select **BlackBerry AtHoc**.

Send a report

The Report feature () sends information and application level location services to the central operations center of an organization. The organization can configure a report type so that when a user activates any report type, the content gets forwarded to the targeted users. That way, organizations can build work flows around the reports. The report list is configured in the BlackBerry AtHoc management system.

If your location services are disabled, you can send a report but it does not include your location details. When you send a report, you are prompted to enable the app and device location services if they are disabled. A **Turn Location on** link is displayed in the Send a message screen if the location services are disabled.

Note: If you are using an Apple iPhone running iOS 14 or later, turn the Precise Location setting on at **Settings** > **Privacy** > **Location Services** > **AtHoc**.

If you are connected to multiple organizations, reports are sent from your primary organization. For more information, see Select a primary organization.

1. Open the BlackBerry AtHoc mobile app on your device.
2. On the Home screen, slide the to the right to send a report.
3. On the **Reports** screen, tap a template to choose the report you want to send.
4. Optionally, you can change the message, location, or attach a photo or video to the report.
5. Tap . You are directed to the home screen where you can see the report activity.
6. Optionally, tap **Cancel** to cancel the report.

Tracking

The Tracking feature periodically sends your location to your organization for the duration you choose. The interval for tracking is set on the BlackBerry AtHoc management system. You can increase or decrease the tracking duration manually at any time. Once you start tracking, the countdown displays how much time is left until tracking stops. Tracking stops if you disconnect from the current organization or switch to another organization.

Note: Ensure that your device location services are enabled.

Note: If you are using an Apple iPhone running iOS 14 or later, turn the Precise Location setting on at **Settings** > **Privacy** > **Location Services** > **AtHoc**.

If you are connected to multiple organizations, tracking occurs in your primary organization. For more information, see Select a primary organization.

1. Open the BlackBerry AtHoc mobile app on your device.
2. Tap ◀ at the top of the home screen.
3. Drag the slider to set a desired duration for location tracking. Sliding all the way to the right results in tracking until it is manually stopped. The default duration is 5 minutes.
4. Tap **Start Tracking**. The dialog closes and an arrow lights up (◀) until tracking is stopped. You are directed to the home screen where you can see the tracking activity.
5. To stop tracking, tap ◀ and tap **Stop Tracking**.

Scheduled location access

When your BlackBerry AtHoc administrator enables scheduled location access, your location is automatically tracked for a specific period of time. When location access begins or ends, a "Your location is being shared with the system" message is displayed. Your BlackBerry AtHoc administrator may enable the ability to deny the location access request. When scheduled location access is enabled, and the location service on your mobile device is enabled, your location information may be sent to BlackBerry AtHoc automatically.

Leave the BlackBerry AtHoc mobile app running in the foreground or background to ensure accurate location access.

Note: For users running Android 12, the notification message cannot dismissed.

Check In/Check Out

When you tap the Check In or Check Out icon, your current location and time stamp are sent to the server.

If you close the app after sending a check-in, the mobile app maintains the check-in. If you disconnect from your organization after sending a check-in, when you reconnect you will need to check in again before you can check out.

If you are connected to multiple organizations, check-ins and check-outs are sent from your primary organization. For more information, see Select a primary organization.

Note: Ensure that your device location services are enabled. If your location cannot be determined, the check-in our check-out is not sent.

Note: If you are using an Apple iPhone running iOS 14 or later, turn the Precise Location setting on at **Settings** > **Privacy** > **Location Services** > **AtHoc**.

Prerequisites

• To perform a check-out, you must have BlackBerry AtHoc release 7.13.1 or later.
• The check-in/check-out feature must be enabled on the Mobile App gateway configuration settings page in the BlackBerry AtHoc management system.

1. Open the BlackBerry AtHoc mobile app on your device.
2. At the top of the home screen, tap ⚬ to check in, or ⚬ to check out. You are directed to the home screen where you can see the check-in and check-out activity.
3. Optionally, tap **Cancel** to cancel the check-in or check-out.

Check in and check out using the XCover key on Samsung Knox devices

You can press the XCover key twice within 1 second on supported Samsung Knox devices to perform a BlackBerry AtHoc mobile app check-in or check-out.

If your mobile device is a managed device, you do not need to map the XCover key. If your mobile device is unmanaged, map the XCover key with BlackBerry AtHoc in your device settings.

The BlackBerry AtHoc mobile app must be running on your device and location services must be enabled to perform a check-in or check-out using the XCover key.

1. On your supported Samsung Knox device, tap **Settings**.
2. On the **Settings** screen, tap **Advanced features**.
3. On the **Advanced features** screen, tap **XCover key**.
4. On the **XCover key** screen, tap to enable the **Use XCover key with app** option.
5. On the **Use XCover key with app** screen, select **BlackBerry AtHoc**.

Collaboration

Collaboration enables users to send text based messages to a group of people. This easy to deploy and configurable feature is available on Android and iOS smartphones. The security of collaboration messages is enhanced with GDPR and HIPAA compliance. Only an administrator can initiate Collaboration.

When you upgrade your BlackBerry AtHoc mobile app, or install a new version of the app on Android or iOS smartphones, you are automatically enrolled for Collaboration, if your organization has configured the

feature. When you tap ☰ > **Collaborate** in the menu, the list of collaborations that you are a part of displays in descending order of the creation date. Collaborations that have unread messages are displayed on the top of the list.

- BlackBerry AtHoc mobile app 4.6 or later must be installed on the device.
- Administrators can add and remove users from a collaboration that is already in progress.
- When you are added to a collaboration, you receive a notification that you can tap to open the collaboration.
- If you are added to a collaboration that is already in progress, you can see all previously sent messages.
- You can securely quote, delete, edit, and retract messages in a collaboration.
- You can add attachments to a collaboration and open attachments that are in a collaboration.
- A delivery status for each message displays so you can see who has viewed each message.
- If you navigate away from the Collaborate screen, you are disconnected from any active collaborations. Tap the Collaborate menu to reconnect.

View collaborations

To view a collaboration, do one of the following:

- Tap 👥 on the bottom right corner of the home screen. The list of collaboration messages displays.
- Tap the notification that the administrator sent.

Working with collaborations

1. Tap 👥 on the bottom right corner of home screen. The list of collaboration messages displays.
2. To participate in a collaboration, tap on the group icon you wish to participate in, type your message in the

   message box, and tap ➤ .
3. In a collaboration you can perform the following actions:
    - **Quote**: Respond to specific messages.
    - **Edit**: Edit your sent messages.
    - **Retract**: Retract a sent message. When you retract a message, the app displays a message to other users that the message was retracted.
    - **Delete**: Delete a specific sent message.
4. To add an attachment to a collaboration, click 📄, and browse to the file that you want to attach.
5. To send a high priority message, click ⓘ .

View the delivery status of messages

The following icons display beside each message you send to indicate the status of each message:

- ✅: Sent.
- Ⓓ: Delivered to at least one participant.
- 🅳: Delivered to all participants.
- Ⓡ: Read by at least one participant.
- 🆁: Read by all participants.

Click the status icon beside a message to open the Message Delivery Status window to see the delivery status for each collaboration participant.

Log out of the mobile app

Before you begin:

- This option appears only if you have authenticated and are logged in to an organization using a username and password.
- This option does not appear if you are using smart card authentication.

1. Tap ☰ > **Logout**.
2. Tap **OK**.

The following message is displayed: You will be logged out from <Organization Name>.
You will continue to receive alerts, but will need to re-authenticate to publish alerts or messages.

Smart card authentication error codes

When smart card authentication is enabled, the mobile app may display the error codes described in the following table.

Error code	Error message
1020	The request contains an invalid RedirectUri. The parameter exists in the query string and is not an empty value.
1030	The request contains an invalid organization code.
2010	MTLS authentication is not configured for the organization based on the organization code and Client ID.
2020	The primary regex (CAC/PIV) is not defined for the organization.
2030	The mapping ID cannot be extracted from the certificate. The regex is invalid or the mapping ID is empty.
3010	The user could not be found in BlackBerry AtHoc. The mapping ID is not set for the user.
3020	The user is disabled or deleted in BlackBerry AtHoc.

BlackBerry AtHoc Customer Support Portal

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

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

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

Documentation feedback

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

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

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

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada