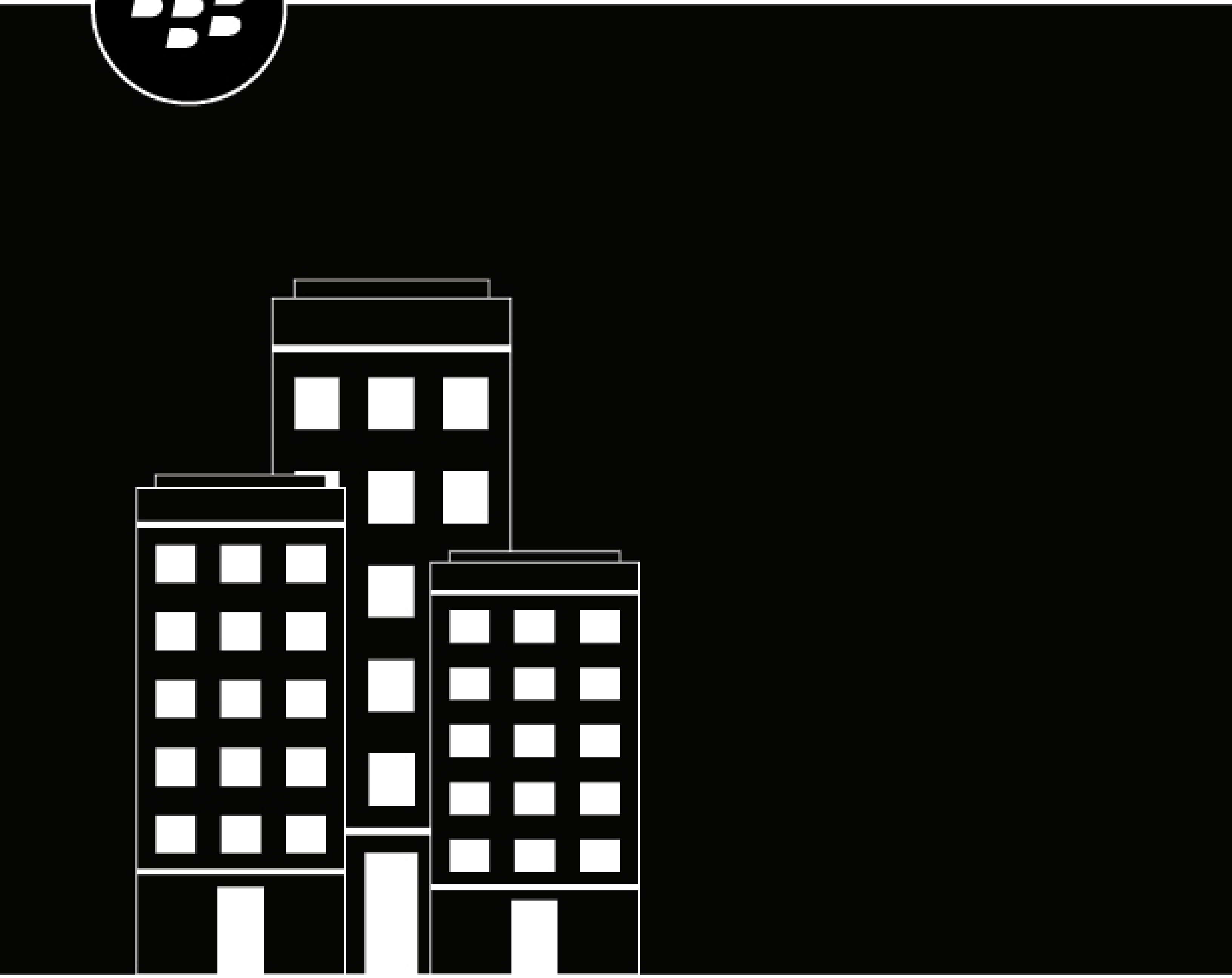

BlackBerry AtHoc

Mobile App Administrator Guide

4.8

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: 11.0, 10.0, 9.0, 8.0, 7.0. Android 6 and below are not supported.
- iOS 14, iOS 13 and iOS 12. iOS 11 and below are not supported.
- iPadOS (with iOS 13 or iOS 14)

Software requirements

- BlackBerry AtHoc release 7.5 or later release
- BlackBerry AtHoc release 7.10 or later release to enable biometric authentication

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, if it is not displayed, enter the email address that is associated with your BlackBerry AtHoc management system account.
4. Enter the PSS server URL. This URL is used for debugging purposes.
5. Tap **Submit**. 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:

<table>
<tr>
<td>Create the app configuration from an XML template</td>
<td><b>a.</b> Click <b>&gt; Create from a template</b>.
<b>b.</b> Click <b>Browse</b> and select the template that you want to add.
<b>c.</b> Click <b>Upload</b>.
<b>d.</b> Type a name for the app configuration and specify the following values:
<b>1. App Config Version</b>: Enter the version of the app configuration. The default is 1.
<b>2. Organization Code</b>: Enter your Organization Code for User registration.
<b>3. User registration email</b>: Enter the email address for user registration.
<b>e.</b> Click <b>Save</b>.</td>
</tr>
<tr>
<td>Create the app configuration manually</td>
<td><b>a.</b> Click <b>&gt; Configure manually</b>.
<b>b.</b> Enter a name for the app configuration.
<b>c.</b> Add the following settings:
<table>
<tr><th>Key</th><th>Value</th></tr>
<tr><td>appconfigversion</td><td>Enter the version of the app configuration.</td></tr>
<tr><td>firsttime_orgcode</td><td>Enter your organization code for user registration.</td></tr>
<tr><td>firsttime_pssurl</td><td>Enter the PSS that the Mobile App communicates with, either US PSS or UK PSS.</td></tr>
<tr><td>firsttime_email</td><td>Enter the email address of a user for registration.</td></tr>
</table>
<b>d.</b> Click <b>Save</b>.</td>
</tr>
</table>

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.
- **User registration email**: Enter the email address of a user for 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.

Configure the Mobile App device on the BlackBerry AtHoc application server

Log in to the BlackBerry AtHoc management system 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 for all users
Collaboration	Selected. Available for all users and operators.
Map	Not selected. Available for 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/Check Out, 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 No

Option	Description
Send Location with Response	Sends user location information with alert or event responses. **Default:** Yes No
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**: Operators can view alerts and users on the map.
   - **Collaboration**: Operators and users can participate in collaborations.
   - **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 **Enable Jail-Break/Root Detection** section, select whether to enable the mobile app to check if the device OS security has been compromised.
13. 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.
14. 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.
15. Click **Save**.

Enable 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. On the **Mobile App** page, click **Edit**.
6. In the **Delivery Gateways** section, click **Add a Delivery Gateway** > **Mobile App**.
7. In the **Mobile App** row, click ✎.
8. By default, the configuration value appears in the **Configuration XML** text-entry field. If the text-entry field is empty, copy the following text into the field:

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

9. Click **Submit**.
10. Click **Save**.
11. Click **More Actions** > **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 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 accessing 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** page, in the **Features** section, select **Alerts** to grant permission to receive alerts on mobile devices.
5. Select **Alert Publishing** to provide publishing permission to operators.
6. Select **Advanced Features** to provide advanced features to a selected group of users. The select advance features section appears.
7. 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 / Check Out**: User check ins and check outs on the map
   - **Reports**: Send field reports
   - **Tracking**: Track mobile device location for a specified amount of time.
8. After selecting an advanced feature, choose a distribution list that can use the selected feature.
9. Make any other needed changes for the mobile app settings.
10. Click **Save**.

Configure mobile alert settings

Configure mobile alert settings to configure the response to alerts. From the **Event Rules** tab of the Mobile Alert Settings page, you can edit incoming alert types, manage report categories, and associate alert templates with incoming mobile alerts. From the **Scheduled Location Access** tab you can configure location access rules.

Note: For information about how to create a new incoming alert report that users can access through their mobile devices, see Create a field report for the mobile app. For information about how to create location access, see Configure scheduled location access.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Mobile Alert Settings**.

   The Mobile Alert Settings screen opens with the **Event Rules** tab open. The Event Rules tab displays information about incoming alert types, any alert templates associated with incoming alert types.
3. Optionally, select an event rule to open it and view or edit the rule defaults.

   The following characteristics apply to the Edit screens for incoming alert categories:

   - **Emergency**, **Checked In**, and **Checked Out** event rule titles and icons are preset and cannot be changed.
   - Report titles and icons are configurable and can edited by any authorized user. Report event categories also contain a **Message** field.
   - For all types of event categories, the following are true:

     - The **Default Severity** option is preset and can be changed as needed. Options include High, Moderate, Low, Informational, or Unknown.
     - The **Run Alert Template** option is sometimes preset and can be changed as needed. Select None to avoid running an alert template.
4. Enter or select values in each of the fields on the screen.
5. Click **Save**.

Note: When an administrator creates, deletes, or updates the mobile alert settings, it is captured in the operator audit trail. To view these entries in the operator audit trail, click ⚙. In the **System Settings** section, click **Operator Audit Trail**. Select **Mobile Event Rules** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select specific actions from the **Action(s)** list.

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, on the **Event Rules** tab, click **New**.
4. On the **Event Rule details** screen, add or select values in the following fields:

   - **Title**: Enter a descriptive label that identifies the field report.
   - **Message**: Optionally, 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. Only alert templates that are ready to be published are displayed.
5. Click **Save**.

6. Optionally, repeat steps 3 through 5 to add additional report types that end users can access when preparing to send an event report.

Mobile alert types

The following event types are available in the system:

- Mobile Standard
  - Emergency (Duress)
  - Check in
  - Check out
  - Report: Send a Message

Configure scheduled location access

The scheduled location access feature enables operators to actively track a group of users for a selected interval. Scheduled location access enables operators to more accurately track where mobile personnel are without relying on end users performing manual check-ins from the mobile app. When location access is enabled, the last known location for all users in the selected distribution lists are updated at the configured interval. Operators can then target alerts and events by geolocation based on users' locations. End users receive a notification on their mobile app when tracking starts. By default, end users have the option to opt out from the location tracking.

If a user belongs to multiple distribution lists that are selected for tracking, the tracking interval for that user is set to the lowest selected tracking interval.

Before you begin:

- The Mobile App gateway and mobile app device must be enabled.
- Scheduled location access must be enabled in **Settings** > **Feature Enablement**.
- Distributions lists for targeting must be created.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Mobile Alert Settings**.
3. On the **Mobile Alert Settings** page, click the **Scheduled Location Access** tab.
4. Click **New**.
5. On the **Scheduled Location Access** screen, select a distribution list.
6. Optionally, select an **Interval**. The default is 24 hours.
7. Select one or more days of the week for the **Recurrence**. All days are selected by default.
8. From the **Start Date** and **Start Time** fields, select when to begin tracking.
9. From the **End Date** and **End Time** fields, select when to stop tracking, or select **No End Date**.
10. Optionally, select **Enforce geolocation (No Opt-out)**. If this option is selected, the end user does not receive the opt-out option on the mobile app when tracking begins.
11. Click **Save**.

Enable smart card authentication

By default, end users authenticate on the mobile app by entering a username and password on the login screen. Administrators can also enable smart card authentication. When smart card authentication is enabled, when an operator starts the alert publishing, report summary, or accountability officer respond-on-behalf-of-others (ROBO) flows, a window appears to select a valid certificate. The certificate must already be present on the operator's device. When a valid certificate is selected, the operator can then complete the flow. If the selected certificate is not valid, the operator is redirected to the username and password login screen.

When smart card authentication is enabled, it becomes the primary authentication method. When the primary authentication type changes from username and password to smart card authentication or vice versa, any current access and refresh tokens expire and the operator must authenticate with the new primary authentication method when they access the alert publishing, report summary, or ROBO flows.

When smart card authentication is enabled, biometric authentication is disabled and the biometric authentication setting is not displayed on the settings screen. The username and password authentication method cannot be disabled.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, in the **Enabled Authentication Methods** section, select the **Smart Card** option.
4. In the **Assign Authentication Methods to Applications** section, in the **Mobile App** section, select **Smart Card** from the **Authentication Method** drop-down list.

   Username and Password is selected by default and cannot be deselected.
5. Click **Save**.

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. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Feature Enablement**.
4. On the **Feature Enablement** page, click **IsCollaborationSupported**.
5. On the **Edit Feature Enablement** window, in the **Enabled** list, select **True**.
6. 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.

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

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://support.athoc.com.

Legal notice

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada