



BlackBerry AtHoc

AtHoc Account

7.20

Contents

- What is AtHoc Account?..... 5**

- Manage AtHoc Account..... 6**
 - AtHoc Account use cases..... 6
 - Accountability Officer workflow..... 7
 - Grant Accountability Officer permissions..... 8
 - Restrict the user base for an Accountability Officer..... 9

- Manage accountability templates..... 10**
 - Create an accountability template..... 10
 - Access the Accountability Templates screen..... 10
 - Define accountability template details..... 10
 - Define details for an accountability template or event..... 11
 - Create a custom accountability status response..... 12
 - Define affected users for an accountability template or event..... 12
 - Target affected users by groups..... 13
 - Target or block affected users individually..... 13
 - Target dependents..... 13
 - Target affected users by location..... 14
 - Target or block affected users by advanced query..... 14
 - Select personal devices for an accountability template or event..... 15
 - Specify personal device options for a template or event..... 16
 - Select the device delivery preference..... 23
 - Define user messages and workflow for an accountability template or event..... 23
 - Add Accountability Officers..... 24
 - Add Accountability Officers by distribution list..... 24
 - Add individual Accountability Officers..... 25
 - Add Accountability Officers by advanced query..... 25
 - Add Accountability Officers by location..... 25
 - Define Accountability Officer messages..... 26
 - Set recurrence..... 26
 - Edit an accountability template..... 26
 - Duplicate an accountability template..... 27
 - Delete an accountability template..... 27

- Configure accountability template settings..... 28**
 - Manage visibility options for event details fields..... 28
 - Manage visibility options for affected users fields..... 29
 - Manage visibility options for user messages and workflow fields..... 29
 - Manage visibility options for Accountability Officer fields..... 30

- Manage accountability events..... 31**

Start an accountability event.....	31
Search for and sort accountability events.....	31
Change the end time of a live event.....	32
Report on behalf of users.....	32
Report on behalf of dependents.....	33
End an accountability event.....	34
Generate an accountability event report.....	34
Export accountability events.....	34

View accountability events.....36

View an accountability event summary.....	36
List of user statuses.....	36
Updated by.....	37
Accountability Officers Targeted.....	37
Status chart.....	37
View users for an accountability event.....	38
View accountability event status by organization.....	39
View accountability event activity.....	40
View accountability event details.....	40
View live accountability events on a map.....	41

BlackBerry AtHoc Customer Support Portal..... 42

Documentation feedback.....43

Legal notice..... 44

What is AtHoc Account?

AtHoc® Account helps reduce post-emergency chaos by providing the tools you need to account for your personnel efficiently, reliably, and systematically. The following are the core capabilities of AtHoc Account:

- The ability to plan ahead by letting you establish and review your accountability procedures.
- Automated outreach work flow to quickly identify at-risk staff so that containment, rescue, and recovery efforts can be concentrated where they are needed the most.
- Automatic follow-up alerts to people who have not responded to rapidly identify those who need help.
- Individual status changes as events unfold.
- The ability to respond on behalf of other employees and to designate Accountability Officers who can report on behalf of others during an event.
- Automatic consolidation of information from all sources with advanced reporting and analysis tools.
- Available as a license and can be deployed in the cloud or via an on-premises implementation. AtHoc's cloud offering for US Federal government agencies is FedRAMP authorized.
- Compatible with the BlackBerry AtHoc mobile app for iOS and Android.

Manage AtHoc Account

Note: Only Accountability Managers, Accountability Officers, and Enterprise Administrators can access AtHoc Account features and functions.

AtHoc Account can help you to create an efficient process to determine what the safety status of the personnel in your organization is in a systematic way. In a disaster, you need to quickly determine who is impacted, and who is safe.

Use AtHoc Account to plan ahead before an incident

- Review and adjust the out-of-the box "Incident Recovery" template to account for personnel during and after an emergency or a crisis situation.
- Perform regular drills with the "Routine Accountability Exercise" template to evaluate the effectiveness of workflow processes, accuracy of data, and end-to-end experience for users.
- Use the "Incident Mitigation/Prevention" template to ensure awareness of preventive or mitigation measures for seasonal events. For example, airborne viruses or hurricane season.
- Use the "Incident Preparedness" template to check users' preparedness before an incident. For example, have users evacuated the area or are they sheltering in place?
- Assign dedicated Accountability Officers who can report on behalf of other personnel during an incident.

Use AtHoc Account during an incident

- Select the "Incident Recovery" template to collect the safety status of your users.
- Quickly narrow down a large set of personnel to only those in an affected area by targeting users by location advanced targeting.
- Choose User Historical Status to capture any user status set by previous safety events or set manually by the user.
- Choose Accountability Officers to delegate status collection.
- Start the event, which starts alerting all affected users and Accountability Officers. When an event starts, reminder messages are also scheduled for users that do not reply to the first alerts.
- As responses are received, monitor the situation in real time using the main event dashboard.
- For users who do not respond to alerts, manually set status based on other communication channels.
- Focus the deployment of your resources on those who need assistance.
- Export reports and send them to management and first responders.

Use AtHoc Account after an incident

- Perform recall of key team member to restore operations with the "Restore Business Operations" template.
- Provide detailed report and analysis of your accountability processes to ensure more efficient responses for future events.
- Refine and adjust templates for future incidents.

AtHoc Account use cases

Responding to a terrorist attack

A terrorist attack occurs near a company's satellite office. AtHoc Account enables the company's emergency management team to target only employees in the area of the satellite office. Using AtHoc Account's preplanned workflow and templates, emergency management sends out a roll call request to all employees at the satellite office. Because of the chaos, not everyone responds immediately. In each round of alerting, AtHoc Account tracks employees who have not responded and automatically re-sends another roll call request. Additionally, assigned Accountability Officers help account for staff by reporting on behalf of fellow employees they know are not in the

affected area because they were out of the office that day on vacation, were working from home, or in another office for a conference.

After four rounds of alerts, fears are put to rest as HQ knows everyone is safe. After the incident, the emergency management officer has detailed reports on how and when employees responded to report back to the CEO to improve future incident response.

Weather incident

A major city is hit by the strongest blizzard in 25 years, which causes the city to shut down key metro rail and busing operations. The city operations manager needs to know when she can restart transportation services, which requires a minimum number of key personnel to be available. She uses AtHoc Account to initiate a recall process, asking employees when they would be able to return to work. After three rounds of automatic alerts and reliance on Accountability Officers, the manager can tell that there are enough available employees to return to work. With this information, the operations manager is able to coordinate continuity of business operations.

Chemical leak

A chemical leak occurs at the manufacturing plant near a company's headquarters. Using AtHoc Account, the head safety and security officer initiates the preplanned account procedure for unplanned incidents to quickly assess the safety of all employees and to deploy resources to help those in need. During the first round of alerts, only 30% of employees respond. AtHoc Account automatically re-alerts unaccounted-for employees. Some employees misplace their phones during the panic, so they are able to ask coworkers to report for them, bringing the total to 80% after 30 minutes of the incident. Within 45 minutes, all personnel are accounted for, and the security officer is able to send company shuttles to employees' locations to move them outside of the affected areas quickly and safely.

Accountability Officer workflow

Accountability Officers can provide status on behalf of other users during or after an accountability event, and can generate accountability event reports.

Accountability Officers can be designated to serve as reporters based on location, job function, or team membership. The Accountability Officer role can be added to any user with operator permissions, or as a standalone role.

Before an event

System Administrators should include Accountability Officer messages with appropriate targeting as part of their accountability templates. This enables administrators to quickly include Accountability Officers as part of their emergency accountability process. When creating a template, administrators can include an initial message, tailored to Accountability Officers, that informs them that an event has started and requests that the Accountability Officers begin accounting for their users. Administrators can also configure an Accountability Officer ending message, informing their Accountability Officers when an event has ended, or when all users that the Accountability Officer is responsible for have a reported status.

Out of the box accountability templates include standard response options for the Accountability Officer initial message. Accountability Officers can select from "I'm available to update user status" or "I'm not available to update user status."

During an event

When an event begins, the System Administrator selects an accountability template with accountability officer messages already predefined in the system. During the publishing flow, the System Administrator has the option to add additional Accountability Officers prior to publishing the accountability event.

Once the event is published, the Accountability Officer receives a notification that an accountability event has started. The notification can contain instructions for the Accountability Officer about how to report status

on behalf of other affected users for the event. The notification also includes response options that the Accountability Officer can use to indicate their availability to update their users' statuses. Accountability Officers can select a response option using Self Service, mobile devices, email, or text messaging.

Notifications can be sent on any of the devices targeted when the event was published. Devices are system based and can include one or more of the following: email, phone, SMS, and mobile app. Email notifications can contain a link which takes the Accountability Officer to the login screen of the BlackBerry AtHoc management system. The severity of the notification email is the same as the severity set for the accountability event.

After logging in, the Accountability Officer is sent directly to the Users tab of the live accountability event for the specific organization or provider. The Users tab displays only the users with no reported status that the Accountability Officer is responsible for reporting status for. The Accountability Officer can then select a single user, or multiple affected users, and update status on their behalf.

Accountability Officers can view and export reports of the status of their users as the event progresses.

When an accountability event is started from an enterprise or super enterprise, the "For more info" link in the notification alert opens the Summary tab of the event in the management system. This gives Accountability Officers access to the correct users based on the Accountability Officer role assignments and restrictions. When an accountability event is started from an enterprise or super enterprise organization, Accountability Officers can respond on behalf of others only when they have been granted the Accountability Officer role in the originating enterprise or super enterprise organization. Accountability Officers who do not have an operator account in the enterprise or super enterprise organization can be targeted, but must first be granted the Accountability Officer role in the enterprise or super enterprise organization in order to respond on behalf of other users.

After an event

The Accountability Officer receives a notification in an email that the accountability event has ended. The notification contains a link which takes the Accountability Officer to the login screen of the BlackBerry AtHoc management system. After logging in, the Accountability Officers is sent directly to the Users tab of the live accountability event for the specific organization or provider. On the event dashboard, the Accountability Officer can view and export reports of their users after an event has ended.

These reports detail the time each user reported status, what the status was, and how many users reported their own status or had their status reported by an Accountability Officer.

Grant Accountability Officer permissions

You can grant accountability officer permissions to users in your organization that you want to provide status on behalf of others during live accountability events.

If you are an Enterprise Administrator logged in to an enterprise organization, you can grant accountability officer permissions to users in suborganizations in your enterprise. If you are an Enterprise Administrator logged in to a super enterprise organization, you can grant accountability officer permissions to users in your super enterprise or their respective sub enterprise organizations and suborganizations.

For accountability events that originate in an enterprise or super enterprise organization, Accountability Officers must have an operator account in the enterprise or super enterprise organization in order to respond on behalf of other users.

For accountability events that originate in an enterprise or super enterprise organization, Accountability Officers must have an operator account in the enterprise or super enterprise organization in order to respond on behalf of other users.

1. Log in to the BlackBerry AtHoc management system as an Organization Administrator, Enterprise Administrator, or System Administrator.
2. In the top navigation bar, click the **Users > Users**.

3. Optionally, click the name of an organization in the **Organization** column to view the organization hierarchy.
4. On the **Users** screen, click a user you want to grant accountability officer permissions to.
5. On the user profile page, click **Edit Operator Permissions**.
6. On the **Operator Permissions** screen, click **Operator Roles > Accountability Officer**.
7. Click **Save**.

Restrict the user base for an Accountability Officer

The user base of an Accountability Officer can be restricted based on standard or user attributes assigned to end users, as well as by membership in organization hierarchies. The user base is defined using dynamic queries that are performed when an alert is created and when it is published.

1. Log in to the BlackBerry AtHoc management system as an Organization Administrator, Enterprise Administrator, or System Administrator.
2. In the navigation bar, click **Users > Users**.
3. Optionally, click the name of an organization in the **Organization** column to view a user's organization hierarchy.
4. Click anywhere in the row containing the accountability officer name. The details of the accountability officer are displayed.
5. Click **Edit Operator Permissions**.
6. On the user details screen, scroll down to the **User Base** section and select **Restricted**.
7. Click the **Modify** link that appears next to the **Restricted** option.
8. On the **Create Conditions** screen, click **Select Attribute** and then select the first attribute you want to use as restriction criteria.
9. Click **Select Operation** and select the operation that you want to assign to the attribute.
Note: The list of operations varies depending on the type of attribute selected.
10. In the next field that appears, enter or select a value for the attribute.
11. Optionally, click **Add Condition** and then repeat steps 7 through 9 for each additional attribute condition you want to add.
12. Optionally, if your organization is set up to display organizations, in the **Organization Hierarchy** section of the **User Attribute** list, select one or more options that the operator can select from as alert targets.
Note: Users must belong to the selected organizational nodes and meet the other specified attribute conditions in order to be included in a user base.
13. When you are done creating restriction criteria, click **Apply**.
14. Optionally, on the **Operator Permissions** screen, to view the list of end users who meet the criteria click **View users** in the **User Base** section.
15. Click **Save**.

Manage accountability templates


The following sections describe how to create and manage AtHoc Account templates.

Create an accountability template

1. In the navigation bar, click **Account > Accountability Templates**.
2. On the **Accountability Templates** screen, click **New** or select one of the out-of-the-box templates.
3. On the **New Accountability Template** screen, select or enter values in the following sections:
 - [Accountability Template](#)
 - [Event Details](#)
 - [Affected Users](#)
 - [User Messages and Workflow](#)
 - [Accountability Officers](#)
 - [Accountability Officer Messages](#)
 - [Schedule](#)
4. After you have reviewed the template details, click **Save**.

Access the Accountability Templates screen

1. In the navigation bar, click **Account > Accountability Templates**.

Note: You can also access the Accountability Templates screen by clicking , and then clicking the **Accountability Templates** link in the **Basic** section.

The Accountability Templates screen opens, displaying the name, description, and last publishing time and date for each accountability template in the system. For accountability templates that have recurrence set, the next occurrence is displayed.

2. Optionally, do any of the following:
 - Click **Delete** to [delete the template or templates](#) that you have selected.
 - Click **Duplicate** to [create an exact copy of an existing template](#) that you have selected.
 - Click **New** to [create a new Accountability template](#).
 - [Search and sort the accountability templates](#) that appear in the list.

Define accountability template details

The Accountability Template section is used to establish the identifying characteristics of an accountability template in the system.

1. In the navigation bar, click **Account > Accountability Templates**.
2. On the **Accountability Templates** screen, click **New** to open the **New Accountability Template** screen, or select one of the out-of-the box templates.
3. In the **Accountability Template** section, in the **Name** field, enter a meaningful name for the template to help operators identify it. For example, "Account for People Post-Emergency." The Name and Description display only in the BlackBerry AtHoc application. They are not displayed to end users.

4. Optionally, in the **Description** field, provide details about the purpose or content of the accountability template. For example, "Start this event when you need to determine the location and safety status of all your personnel following an emergency." This description is not seen by end users. It is visible only to operators within the BlackBerry AtHoc application.
5. Configure the [Event Details](#) section.

Define details for an accountability template or event

Use the Event Details section to define the key parts of an accountability event or template in the system: the severity, name, description, status attributes, website links, or location details that are relevant.

1. To create an accountability event or template in a language other than default language displayed on the screen, click the button beside the **Severity** field and select the language from the list that appears. This does not change the language displayed on the screen. It changes the language that the message is delivered in. If text-to-speech is enabled on the system, the audio portion of the event is delivered in the language you selected.

2. From the **Severity** list, select the severity level.

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

3. In the **Name** field, enter a one-line summary that communicates the purpose of the event or template. The maximum number of characters is 100. The name is required and displays at the top of the recipients' screen when the event starts.
4. Optionally, to insert a placeholder into the event or template title, click **+** and select the placeholder from the list that appears.
5. In the **Description** field, enter up to 4000 characters of text that communicate why the event has been created and provide instructions to the affected users.
6. Optionally, to insert a placeholder into the event or template body, click **+** and select the placeholder from the list that appears.
7. Optionally, in the **Location** section, click **Add** to access a map where you can select a location for the event or template. This location can also be used to target affected users and Accountability Officers by location.

Note: If you select Email or Desktop Popup in the Select Personal Devices section when you create an event from this template, the map image is included in the event if this capability is enabled for your organization.

For a detailed description of how to specify a geographic location, see "[Select an alert or event location](#)" in the *BlackBerry AtHoc Create and Publish Alerts* guide.

8. Optionally, in the **Attachments** field, drag and drop files or click **Browse** to select files to include in the event. You can include the following file types as attachments:

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

Note:

- You can include a maximum of 5 files totaling up to 5 MB.
- Always use caution when including attachments in events and alerts. Alerts and events with a large number of targeted users and attachments will experience a significant delay in the expected delivery time. (The

delivery time is the total time taken, from when the operator sends the alert to when the last targeted user receives the alert.) For example, if an alert with a 5 MB attachment is sent to 20,000 users, the expected delivery time is 2 hours. If additional alerts with attachments are also in the BlackBerry AtHoc system, the expected delivery time can increase significantly.

- Files are converted to universally supported file types while they are uploading. This enables the use of file types that are not supported on all mobile platforms.

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

- A URL that opens a web page where users can go to get more details about the event when an alert is sent out. When users receive alerts generated from the event, a **For Further Information** link within it will take them to the web page.
- A URL that opens an attachment (media or documents) stored on Dropbox. For details on how to store an attachment on Dropbox, see ["Add an attachment using Dropbox"](#) in the *BlackBerry AtHoc Create and Publish Alerts* guide.


10. If you entered a URL in Step 10, click **Test URL** to verify that the link works.

11. In the **Status** field, click the list to view predefined statuses you can add to the event or template. The Status field represents the response options the event recipients can choose from when they respond to the event alert. Each status comes with a set of predefined responses that event recipients must choose from in order to stop receiving follow-up messages for the same event. You can create customized accountability statuses. See [Create a custom accountability status response](#).

12. In the **Affected Users** section, [define affected users for an accountability template or event](#).

Create a custom accountability status response

You can create custom accountability status responses to customize the responses available to accountability event end users. You can also select an out-of-the-box user status response.

1. In the navigation bar, click .
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, click **New > Status**.
4. On the **New Attribute** page, in the **Basic** section, enter a name for the accountability status.
5. In the **Values** section, click **Add value** to add a new status. Enter a value for the accountability status. For example, "I am safe."
6. In the row for the new value, click **Save**.
7. Click **Add value** to add additional status response values.
8. Click **Save** to save each status response value.
9. Click **Save** to save the Status user attribute.

The Status accountability user attribute is available to select when creating an accountability template and appears in the Status list.

Define affected users for an accountability template or event

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

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

Target affected users by groups

Use the By Groups tab to target groups of users based on their memberships in organizational hierarchical nodes and in distribution lists. Alerts generated from the event are sent to users in the selected groups.

The operator can also block recipient groups (exclude them from receiving alerts generated from the event).

The group target categories displayed are:

- **Organizational Hierarchy:** If your system is set up for them. The "All User Base" is the first node that appears and is the only node from the hierarchy that appears when collapsed.
- **Distribution Lists:** Static and dynamic

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

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

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

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

Target or block affected users individually

1. In the **Affected Users** section, click **By Users**.
2. In the **Users** field, click **Add/Block Users**.
3. On the **Add/Block Users** screen, select the check box next to each user you want to target in the alert. Click **Block** beside any user you want to block from receiving alerts generated from the event.

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

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

4. Optionally, to target dependents, click the **Dependents** tab and then select **Include all dependents of affected sponsors**.
5. Click **Apply**.

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

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

Target dependents

If dependents are enabled for your organization and in the accountability template, you can target them from the Dependents tab in the Targeting section.

1. In the **Affected Users** section, click **Dependents**.
2. Select **Include all dependents of affected sponsors**.

Target affected users by location

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

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

Tip: For a detailed description of how to select locations, see "[Select an alert or event location](#)" in the *BlackBerry AtHoc Create and Publish Alerts* guide.

3. Click **Apply**. The Affected Users Summary section updates to display the total number of locations on the map that will be used to target recipients.
4. In the **Affected Users** section, click **By Advanced Query**. By default, users who have a location attribute in the selected locations and have a Last Known Location attribute updated within the last 4 hours are targeted.
5. Optionally, click **map selection(s)** to change the selected locations.
6. Optionally, enter a number and select **Minute(s)**, **Hour(s)**, or **Day(s)** to change the timeframe for the Last Known Location attribute.
7. Optionally, in the **Affected Users Summary** section, click the number beside **By Location** to open a map that shows the targeted locations.


The Affected Users Summary section updates automatically to display the total number of locations on the map that will be used to target recipients when events are generated from the template.

Target or block affected users by advanced query

You can perform ad hoc targeting or blocking of users based by an advanced query on general attributes, organization hierarchies, geolocation, user attributes, or device types.

1. In the **Affected Users** section, click the **By Advanced Query** tab.
2. Select the AND/OR operator. When AND is selected, users must meet all conditions to be targeted in the event. When OR is selected, users that match any of the conditions are targeted. The default is AND.
3. Click **Add Condition**.
4. In the **Select Attribute** list, select the first attribute, organization hierarchy, geolocation, user attribute, or device you want to use as targeting criteria.
5. In the **Select Operation** list, select the operation that you want to assign to the attribute. To block users who have specific attributes, select a negative operation such as **not equals** or **does not contain**.

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

6. If the operation you selected in Step 5 requires additional query values, a third field appears on the screen. Enter or select a value for the attribute.
7. Optionally, click **Add Condition** and then repeat steps 3 through 6 for each additional condition you want to add. The Affected Users Summary field at the bottom of the Affected Users section updates automatically to display the total number of users who match the query conditions you have created.
8. Optionally, modify the query conditions as needed to isolate the exact user group you want to send event-generated alerts to. You can click **Add Condition** to add more conditions or click  to remove an existing condition.

- Optionally, in the **Affected Users Summary** section, click the number in the **By Advanced Query** field to view a screen that displays the criteria that you created for the advanced query.

Target affected users with the User Last Updated Source attribute

You can target affected users by the source that last updated the users' profiles. The following table lists the possible sources and the search terms required to target users with the User Last Updated Source attribute.

Source	Search term
Mobile app	<ul style="list-style-type: none"> • Check-in • Check-out • Report • Emergency • User Tracking - Mobile App • Mobile
Self Service	SelfService
BlackBerry AtHoc Management System	ManagementSystem
User Sync Client	UserSyncClient
API	API
CSV Import	UserImport
Targeted Device	<ul style="list-style-type: none"> • Alert Tracking - Desktop Popup • Alert Tracking - Email • Alert Tracking - Mobile App • Alert Tracking - Phone • Alert Tracking - Text Messaging

- In the **Affected Users** section, click the **By Advanced Query** tab.
- Select the AND/OR operator. When AND is selected, users must meet all conditions to be targeted in the event. When OR is selected, users that match any of the conditions are targeted. The default is AND.
- Click **Add Condition**.
- From the **Select Attribute** list, select **User Last Updated Source**.
- Select an operation from the **Select Operation** list.
- In the blank field that appears, enter the source that you want to target affected users by. The text you enter in this field must match one of the search terms listed in the table above. You can add more than one source, separated by a comma. For example, API, UserSyncClient.

Select personal devices for an accountability template or event

After selecting the users or groups to include in the event or template, you must select the personal devices that will be used to contact the target group.

1. In the **Affected Users** section, click the **Select Personal Devices** tab. A list of all available personal devices appears, accompanied by statistics that reveal the total number of selected users who can be reached by each device type.
2. Select the check box next to each personal device you want to include. As you select devices, the pie chart in the **Affected Users Summary** section updates to show the number of reachable and unreachable users based on your current selections.
3. Optionally, click the number beside the **Total Affected** field to view a Users screen that shows the username and organizational hierarchy for each user in the target group.
4. Optionally, click the numbers beside the **Reachable Users** and **Unreachable Users** fields to view separate pop-up screens providing user details for those subgroups.
5. Optionally, [specify personal device options](#).

Note: If no users are reachable based on the targeted users and devices you select, the event is not publishable.

Specify personal device options for a template or event

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

1. In the **Affected Users** field, click the **Select Personal Devices** tab.
2. In the **Personal Devices** field, select the check boxes next to the personal devices to use to contact the target group.
3. Click **Options** in the top corner of the **Personal Devices** field.

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

4. After selecting options, click **Apply** at the bottom of the screen.

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

Device Type	Options	Explanation
Desktop Popup	App Template	<ul style="list-style-type: none"> • All desktop pop-up event messages display the severity and type, and, if available, a link to the event location. BlackBerry AtHoc provides default templates, one for each type of severity: High, Moderate, Low, Informational, Unknown. • Specify the desktop delivery template, either the default template or a custom template. • If you choose Use Custom Template, you can pick from any existing templates. • Best Practice: Click Preview to preview the custom template. <p>Important: If your operating system has been magnified to 150% or higher, reduce the amount of text in the event message. If the event message exceeds the size of the event dialog, the scroll bars might be unavailable.</p>

Device Type	Options	Explanation
	App Audio	<ul style="list-style-type: none"> • Select whether to use the default or a custom audio sound. The default audio is predefined by your organization. • If you choose Use Custom Audio, you can pick from any existing audio sound. • Best Practice: Click ► to preview audio selections
	Map Image in Alert	Select Enable to include the location set in an alert template as a map image in an event message. Users who receive the event message can click the image of the map in the message to go to an interactive map.
Email	Email Template	<ul style="list-style-type: none"> • Specify the email template, either the default template or a custom template. BlackBerry AtHoc provides default templates for each type of severity: High, Moderate, Low, Informational, Forgot Password. <p>Note: If you select a custom template and your email delivery system does not support it, the default template is used.</p>
	Email Message Content	<ul style="list-style-type: none"> • Select Alert Title and Body to use the information in the alert title and body fields as the email message content. • Select Custom Text to enter a custom title and message body as the email message content.
	Map Image in Alert	<ul style="list-style-type: none"> • Select Enable to include the location set in an alert template as a map image in an event message. Users who receive the event message can click the image of the map in the message to go to an interactive map.

Device Type	Options	Explanation
Text Messaging	Content Sent Via Text	<ul style="list-style-type: none"> • Select Alert Title and Body (Short) to use the first 1250 characters of the alert title and body as the text message content. The text message content is truncated at the first space before the 1250th character. If the content is truncated, the text message includes a link users can click to view the complete alert text. This is the default option. • Select Alert Title to use only the information in the alert title as the text message content. • Select Custom Text to enter a custom message as the text message content. The maximum is 1250 characters. • Targeted users in countries that have a provisioned SMS country code can respond to SMS alerts. Users in countries that do not have a provisioned country code cannot respond to SMS alerts. For more information, including a list of countries with a provisioned code, see <i>How does AtHoc SMS support sending text messages to countries abroad?</i> on the BlackBerry AtHoc customer support site.
Pager	Content	<ul style="list-style-type: none"> • Select Alert Title and Body to use the information in the alert title and body fields as the pager message content. • Select Custom Text to enter a custom message as the pager message content. Custom text must be between 5 and 150 characters.
Cisco IP Phone Display	Alert Image	<ul style="list-style-type: none"> • Select None if you do not want an image to accompany the alert. • Select Image to select an image from a predefined list. • Select Online Image to enter the URL for an image that you want to accompany the alert.
	Ringtone	<ul style="list-style-type: none"> • Select No Ringtone if you do not want a ringtone to play before the alert • Select Use Ringtone to select a ringtone from a predefined list. The tone will sound before the alert content plays.

Device Type	Options	Explanation
	Audio Broadcast	<ul style="list-style-type: none"> • Select No audio message from the list if you want no audio to play when the alert is received. • Select Audio - Title and Body from the list if you want the alert title and body to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Audio - Title Only from the list if you want the alert title to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Audio - Body Only from the list if you want the alert body to play when the alert is received. If you select this option, you have the option of setting the alert to replay as many times as you want. • Select Custom from the list if you want to enter custom text for the alert. If you select this option, you have the option of setting the alert to replay as many times as you want.
Phone	<p>Phone Message Content</p> <p>Recipient Answers the Call</p> <p>Recipient Does Not Answer the Call</p>	<ul style="list-style-type: none"> • Select Send Alert Title and Body to use the information in the alert title and body fields as the phone message content. • Select Send Custom Text to enter a custom title and message body as the phone message content. • Select Send Recorded Message to create and upload a custom recorded message that will be played for the alert recipients. For details about creating a recorded message, see Create a custom recorded message for an event or event template. For details about uploading a recorded message, see Upload a custom recorded message for an event or event template. <p>Select what you want to happen after the recipient answers the call:</p> <ul style="list-style-type: none"> • Deliver alert without any authentication • Deliver alert only after the provided PIN is entered • Deliver alert only after user validation <p>Select what you want to happen if the call is not answered:</p> <ul style="list-style-type: none"> • Deliver alert as voice mail • Leave callback information in the voicemail • No voice mail

Device Type	Options	Explanation
	Requires Acknowledgment	Select if the alert has no response options. The acknowledgment steps are provided at the end of the alert.
	Stop Calling Options	Select the criteria you want to use to stop calls from being made to the alert recipient: <ul style="list-style-type: none"> • Recipient acknowledged the message • Recipient listened to entire message • Entire message left on voicemail
	Call Attempts	Enter the number of attempts the system should make to contact each recipient.
	Retry Interval	Enter the amount of time that must elapse before the system tries again to contact the recipient.

Device Type	Options	Explanation
BlackBerry AtHoc Mobile App	Repeat Notification	<p>Each alert is sent once. This option is used to specify if and how often notifications about the alert are repeated on a mobile device.</p> <ul style="list-style-type: none"> • None: Send the alert notification once. • Default: Use the default time that has been defined for the selected severity. <ul style="list-style-type: none"> • For alerts with a severity level of High, the default is one notification a minute for 10 minutes. • For alerts with a severity of Moderate, Low, Informational, or Unknown, the default is one notification a minute for 2 minutes. • Custom: <ul style="list-style-type: none"> • Select how long to repeat the notification if the user does not respond. • Select how long to pause between each repetition. <p>Note: Ensure that the pause time is smaller than the repetition time frame. For example, you can set the Stop Repetition After value for 5 minutes, and the Pause between Notifications value to 30 seconds - the notification can be repeated up to 9 times. However, if the Stop Repetition After value is 5 minutes, but the Pause between Notifications value is 6 minutes, the notification is repeated only once.</p> <p>Alert notifications repeat until one of the following occurs:</p> <ul style="list-style-type: none"> • The recipient responds to the alert from any of the mobile apps on which the same recipient is registered. Responses sent from other devices such as email, phone, or SMS, do not stop the notification. • The defined time frame for repeat notifications elapses. • The alert ends.

Device Type	Options	Explanation
	Deliver Alert with Sound	<p>Select Yes if you want the mobile device to play a sound according to the alert severity and device settings. For high severity alerts, this setting overrides the device settings and plays a sound when an alert is delivered. For all non high-severity alerts, the sound setting on the mobile device takes precedence.</p> <p>Select No to prevent the mobile device from playing any sounds. Alerts of any severity are delivered silently.</p>

Create a custom recorded message for an event or event template

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

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

1. In the **Target Users** section, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the appropriate check boxes next to the **Phone - Work** and **Phone - Mobile** devices, depending on which you want to use as targeting methods.
3. Click **Options**.
4. On the **Personal Devices Options** screen, click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Record New Message**.
7. On the **Record New Message** window, click **Record** and then start speaking.
 - Note:** As you speak, the timer on the screen counts down, showing you how many more seconds you can record. By default, the timer is set to 1 minute.
8. When you have finished recording the message, click **Stop**.
9. Optionally, click to listen to your message.
10. Optionally, if you want to re-record the message, click **Record**.
11. When you are satisfied with the recording, click **Use Recording**. The **Personal Devices Options** screen appears, with the **Phone** tab displayed and the filename field populated with a system-generated name for your recording.
12. Optionally, click to download your message as a .wav file.
13. Optionally, make selections in the other fields on the **Phone** tab.
14. Click **Apply**.

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

Upload a custom recorded message for an event or event template

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

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

1. In the **Affected Users** section of the event or event template, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the check boxes next to the **Phone - Work** and/or **Phone - Mobile** devices, depending on which you want to use as targeting methods.
3. Click **Options**.

4. On the **Personal Device Options** screen, click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Browse** and navigate to the location where the custom recorded message is stored.
7. Click the filename and then click **Open**. The name of the file appears in the filename field.
8. Optionally, click **Play** to hear the message before attaching it to the event or event template.
9. Optionally, make selections in the other fields on the Phone tab.
10. Click **Apply**.

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

Select the device delivery preference

After selecting the personal devices to use to contact the target group, you must select whether to use the organization defined, system defined, or user preferred device delivery preference to use to contact the target group. This selection applies to personal devices only. The default selection is system defined.

When the device delivery preference is system defined, all devices are targeted simultaneously. End users targeted in the event receive alerts on all of their enabled devices at the same time.

When the device delivery preference is organization defined, the operator-defined sequence and interval, configured in **Settings > Devices**, is applied.

When the device delivery preference is user preferred, the user-defined sequence configured in either the BlackBerry AtHoc management system or in Self Service, is applied. End users targeted in the event receive alerts on their enabled devices in the specified sequence and interval. Once a user responds to the event on one device, they do not receive the alert on any additional enabled devices.

Before you begin:

- Device delivery preference must be enabled for your organization.
 - Device delivery priority and interval must be configured in **Settings > Devices**.
1. In the **Affected Users** section, click **Device Delivery Preference**.
 2. Select **System defined**, **Organization defined**, or **User preferred**.

Define user messages and workflow for an accountability template or event

After selecting the personal devices you want to include in the event or template, you must define the workflow and messaging for the event.

1. In the **User Messages and Workflow** section, set the duration of the event in minutes, hours, or days.
2. Optionally, if you want to include the status of each recipient from before the event started in the event statistics (either set by previous safety events or set manually by the user), select to enable the **User Historical Status** option. Specify how many days, minutes, or hours before the start of the event you want to start tracking user statuses.
3. By default, the check box for the Initial, Reminder, and Ending messages is selected. Deselect the check box next to any of the messages you do not want to send. At least one message type must be selected.
4. Click **Edit** beside any message to change its content. The edit screen that appears contains text-entry fields for the message title and body. To include a placeholder, click **+** in the text-entry field and select the placeholder to add to the event title or description.
5. For the **Edit Reminder Message** screen only, select a time span in the **Schedule** section.

6. Click **Apply** to save any changes you make to the message content.
7. Optionally, click **Preview** to see how the event messages will look to recipients.
8. Click **Review and Start** (for accountability events) or **Save** (for accountability templates.)

Add Accountability Officers

After defining the user messages and workflow for an accountability template or event, you can add Accountability Officers to the event or template. Operators must have the Accountability Officer role to be added to an accountability event as an Accountability Officer.

Note: If you are an Enterprise Administrator logged in to an enterprise organization with suborganizations, Accountability Officers can be selected from both the enterprise and suborganizations. If you are an Enterprise Administrator logged in to a super enterprise organization, Accountability Officers can be added from sub enterprises and suborganizations.

If the Accountability Officer role has been assigned to an operator in a suborganization, they are displayed as available for targeting in the Accountability Officers section of an accountability event that originates in an enterprise or super enterprise. However, roles are assigned independently for each organization. To provide the Accountability Officer access to view and respond on behalf of users, the Accountability Officer role must be granted in the enterprise or super enterprise organization.

You can add Accountability Officers by any of the following methods:

- [Add Accountability Officers by distribution list](#)
- [Add individual Accountability Officers](#)
- [Add Accountability Officers by advanced query](#)
- [Add Accountability Officers by location](#)

Add Accountability Officers by distribution list

Use the By Distribution Lists tab to target groups of Accountability Officers based on their memberships in distribution lists. Alerts generated from the event are sent to the Accountability Officers in the selected groups.

The operator can also block recipient groups (exclude them from receiving alerts and messages generated from the event.)

Note: The administrator can restrict the contents of distribution lists for each operator.

1. In the **Accountability Officers** section of accountability template or event, click the **By Distribution Lists** tab.
2. In the **Distribution List Folders** section, select **All User Base** or click the check box to expand the list of distribution lists.
3. Select one or more distribution lists.
4. Optionally, click **Expand All** or **Collapse All** to open or close the distribution list folders.
5. Optionally, click **List Targeted Accountability Officers** to view the selected Accountability Officers.
6. Click **Save**.

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

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

Add individual Accountability Officers

Use the By Individual Accountability Officers tab to target individual Accountability Officers. Accountability Officer messages generated from the event are sent to the selected Accountability Officers.

1. In the **Accountability Officers** section of accountability template or event, click the **Add Individual Accountability Officers** tab.
2. Click **Add/Remove Accountability Officers**.
3. On the **Add Accountability Officers** dialog, select the check box beside each Accountability Officer to add.
4. Optionally, enter a name in the **Search by Name** field to narrow the list of Accountability Officers displayed.
5. Optionally, click the name of an organization in the **Organization** column to display the Accountability Officer's organization hierarchy.
6. Click **Apply**.
7. Optionally, click **List Targeted Accountability Officers** to view the selected Accountability Officers.
8. Optionally, to remove an Accountability Officer from the list, click the **X** beside their name.
9. Click **Save**.

Add Accountability Officers by advanced query

Use the By Advanced Query tab to target Accountability Officers by creating an advanced query based on general attributes, organization hierarchies, geolocations, user attributes, or device types.

1. In the **Accountability Officers** section, click the **By Advanced Query** tab.
2. Select the AND/OR operator. When AND is selected, users must meet all conditions to be targeted in the event. When OR is selected, users that match any of the conditions are targeted. The default is AND.
3. Click **Add Condition**.
4. In the **Select Attribute** list, select the first attribute, organization hierarchy, geolocation, user attribute, or device you want to use as query criteria.
5. In the **Select Operation** list, select the operation that you want to assign to the attribute.
Note: The list of operations varies depending on the type of attribute selected.
6. If the operation you selected in Step 5 requires additional query values, a third field appears. Enter or select a value for the attribute.
7. Optionally, click **Add Condition** and then repeat steps 3 through 6 for each additional condition you want to add.
8. Optionally, modify the query conditions as needed to isolate the exact Accountability Officers you want to add. You can click **Add Condition** to add more conditions or click **[-]** to remove an existing condition.
9. Optionally, click **List Targeted Accountability Officers** to view the selected Accountability Officers.
10. Click **Save**.

Add Accountability Officers by location

Use the Event Details section to add Accountability Officers by location.

1. In the **Event Details** section, in the **Location** area, click **Add** to access a map where you can select a location to target Accountability Officers.
2. On the map that opens, do any of the following:
 - Click **Create Custom Locations** to display the drawing tools for creating shapes.
 - Click **Select Predefined Locations** to use a predefined location on the map as a targeting criterion.
3. Click **Select By Location**.
4. Select **Target Accountability Officers**.
5. Click **Apply**.
6. Optionally, click **List Targeted Accountability Officers** to view the selected Accountability Officers.

7. Click **Save**.

For a detailed description of how to specify a geographic location, see "[Select an alert or event location](#)" in the *BlackBerry AtHoc Create and Publish Alerts* guide.

Define Accountability Officer messages

After adding Accountability Officers to your accountability template or event, you can create Accountability Officer messages for the event. Use these messages to inform your designated Accountability Officers that an accountability event has started or ended and to report status on behalf of their users.

Out of the box accountability templates include response options in the Initial Message section that Accountability Officers can use to indicate if they are available to update their users' statuses.

When an accountability event is sent from an enterprise or super enterprise organization, the More Info link in the initial message takes the Accountability Officer to the Summary tab of the event in the management system.

When Accountability Officers are selected, the Initial Message is required. The ending message is available only when Accountability Officers and the Initial Message have been selected.

1. In the **Accountability Officer Messages** section, the check box for the initial and ending accountability officer messages are selected by default. Deselect the check box if you do not want to send an initial or ending accountability officer message.
2. Click **Edit** beside either of the messages to change its content. The edit screen that appears contains text-entry fields for the message title and body. If you want to include an event placeholder rather than or in addition to regular text, click **+** in the text-entry field and select the placeholder you want to add to the message title or description.
3. Click **Apply**.
4. Optionally, in the **Initial Message** or **Ending Message** section, click **Preview** to see how the event will look to the assigned Accountability Officers.
5. Click **Save**.

Set recurrence

If you want to send an accountability event on a recurring basis without the need to manually send the event each time, set a recurrence in the accountability template.

1. In the **Schedule** section, in the **Start Time** section, select **Activate Recurrence** and select a time.
2. In the **Recurrence Pattern** section, select the **Interval**. You can choose Daily, Weekly, Monthly, or Yearly. The default is Daily. Select additional recurrence options as needed.
3. In the **Recurrence Period** section, select a start date. The default is the current date.
4. Optionally, select an end date for the recurrence. The default is no end date. You can choose to end the recurrence after a specified number of occurrences or on a specific date.
5. Click **Save**.

Edit an accountability template

Within BlackBerry AtHoc, accountability templates typically consist of event details, statuses, a list of affected recipients, a list of delivery devices for a specific event, and messages and workflow settings.

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

1. In the navigation bar, click **Account > Accountability Templates**.
2. On the **Accountability Templates** screen, use the **search** field or scroll down in the list to locate the accountability template you want to edit.
3. Click the name of the template.
4. Edit values in any of the following sections:
 - [Accountability Template](#)
 - [Event Details](#)
 - [Affected Users](#)
 - [User Messages and Workflow](#)
 - [Accountability Officers](#)
 - [Accountability Officer Messages](#)
 - [Schedule](#)
5. Click **Save**.

Duplicate an accountability template

Duplicate an accountability template to create an exact copy. Duplicating speeds the creation of similar templates.

1. In the navigation bar, click **Account > Accountability Templates**.
2. Use the **search** field or scroll down in the template list to locate the accountability template you want to duplicate.
3. Select the check box next to the template name.

Note: If the template does not have a check box next to its name, it cannot be duplicated.
4. Click **Duplicate**. A **<Template name> (copy)** screen appears, displaying the values that were part of the original template.
5. Make whatever changes you want to the template details.

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

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

Delete an accountability template

You can delete accountability templates individually or in groups from the Accountability Templates screen.

1. In the navigation bar, click **Account > Accountability Templates**.
2. Use the **search** field or scroll down in the list to locate the templates you want to delete.
3. Select the check box next to each template that you want to delete.
4. Click **Delete**.
5. On the **Delete Accountability Template** confirmation window, click **Delete**.

Configure accountability template settings

The contents and behavior of the different sections of the accountability template creation screen are controlled from a central Accountability Template Settings screen.

The visibility settings you select affect all events that are started from the template. For example, if you choose to hide the Severity field from a template called "Accountability – Severe Weather," that field will be hidden for all events that are started from that template.

You can customize the visibility settings for the fields in the Event Details, Affected Users, and Messages and Workflow sections of the event creation screen.

Manage visibility options for event details fields

You can manage the visibility settings for the Event Details fields in an accountability template.

1. In the navigation bar, click **Account > Accountability Templates**.
 2. On the **Accountability Templates** screen, click an accountability template from the list or click **New**.
 3. On the accountability template details screen, click **Settings**.
 4. On the **Accountability Template Settings** screen, on the **Event Details** tab, in the **Enable** section, select the check boxes next to each of the content options you want to make visible to operators who are creating events based on this template. You can show or hide any of the following options in the **Event Details** tab:
 - **Location:** Select this check box if you want users creating events from this template to be able to designate a specific location for the event on a map.
 - **Is Location Mandatory:** Select this check box if you want to make it mandatory for users creating events from this template to select a location for the event.
 - **Attachments:** Select this check box if you want operators to be able to include attachments including documents, videos, and image files, in accountability events.
 - **Dropbox:** Select this check box if you want users to be able to include an attachment in an event. Users can then upload media or documents to Dropbox and include a link to those resources within the event.
 - **Show Severity field:** Select this check box if you want event creators to be able to select a severity for the event. Some events have a default severity, so selecting this option enables creators to change the default before starting the event.
 - **Show Type field:** Select this check box if you want event creators to be able to select from a predefined list of event types while creating the event.
 5. In the **Visibility in Event** section, do one of the following:
 - Select **Show Event Details section**, and then select the check boxes next to each option you want to make available in the template.
 - Select **Show as initially collapsed** check box if you want the Event Details section to display in its collapsed state when the template is first opened.
 - Select **Show as read-only and prevent operator from editing** check box if you want the template Event Details section to be visible, but not editable.
 - Select **Hide Event Details section** if you do not want users who are creating events from the template to be able to see the Event Details section.
- Note:** If a section of the template is not ready, you cannot set the visibility options for that section to "Read-Only" or "Hide."
6. Click **Apply**.

Manage visibility options for affected users fields

You can manage the visibility settings for the accountability template Affected Users fields.

1. In the navigation bar, click **Account > Accountability Templates**.
2. On the **Accountability Templates** screen, click an accountability template from the list or click **New**.
3. On the accountability template details screen, click **Settings**.
4. On the **Accountability Template Settings** screen, click the **Affected Users** tab.
5. Optionally, in the **Enable** section, select the check box to enable targeting dependents in events.
6. In the **Enable Targeting** section, select the check boxes next to each of the user targeting options you want to make visible to users who are creating events based on this template.

Note: You must select at least one targeting method.

You can show or hide any of the following options for targeting users:

- By groups
 - By name
 - By advanced query
 - By location
 - By personal devices. This option displays a list of all personal devices you can make visible or hide from users who are creating events based on the template.
7. In the **Visibility in Event** section, do one of the following:
 - Select **Show Affected Users section**, then select the check boxes next to each option you want to make available to users who are creating accountability events from the template.
 - Select **Show as initially collapsed** if you want the Affected Users section to display in its collapsed state when the template is first opened by the accountability event creator.
 - Select **Show as read-only and prevent operator from editing** if you want the accountability event creator to be able to see the Affected Users section without being able to edit any fields within it.
 - Select **Hide Affected Users section** if you do not want users who are creating accountability events from the template to be able to see the Affected Users section.
- Note:** If a section of the template is not ready for publication, you cannot set the visibility options for that section to "Read-Only" or "Hide."
8. Click **Apply**.

Manage visibility options for user messages and workflow fields

You can manage the visibility settings for the accountability template Messages and Workflow fields.

1. In the navigation bar, click **Account > Accountability Templates**.
2. On the **Accountability Templates** screen, select an accountability template or click **New**.
3. On the accountability template details screen, click **Settings**.
4. On the **Accountability Template Settings** screen, click the **User Messages and Workflow** tab.
5. In the **Visibility in Event** section, do one of the following:
 - Select **Show User Messages and Workflow section**, then select the check boxes next to each option you want to make available to users who are creating events from the template.
 - Select **Show as initially collapsed** if you want the Messages and Workflow section to display in its collapsed state when the template is first opened by the event creator.

- Select **Show as read-only and prevent operator from editing** if you the event creator to be able to see the Messages and Workflow section without being able to edit any fields in it.
- Select **Hide User Messages and Workflow section** if you do not want users who are creating events from the template to be able to see the Messages and Workflow section.

Note: If a section of the template is not ready for publication, you cannot set the visibility options for that section to "Read-Only" or "Hide."

6. Click **Apply**.

Manage visibility options for Accountability Officer fields

You can manage the visibility settings for the accountability template Messages and Workflow fields.

1. In the navigation bar, click **Account > Accountability Templates**.
2. Double click an existing accountability template, or click **New** to create a new accountability template.
3. On the details screen for the accountability template, click **Settings**.
4. On the **Accountability Template Settings** screen, click the **Accountability Officers** tab.
5. Optionally, select **Show Accountability Officer Messages**.

Note: When **Show Accountability Officer Messages** is not checked, each message section is hidden, but users can still select each message section to have it available during event creation.

6. In the **Visibility in Event** section, do one of the following:

- Select **Show Accountability Officer section**, and then select the check boxes next to each option you want to make available to users who are creating events from the template.
 - Select **Show as initially collapsed** if you want the Accountability Officer Messages section to display in its collapsed state when the template is first opened by the event creator.
 - Select **Show as read-only and prevent accountability managers from editing** if you want the event creator to be able to see the Accountability Officer Messages section without being able to edit any fields within it. Event creators can still see the **List Targeted Accountability Officers** link when this option is selected.
- Select **Hide Accountability Officer section** if you do not want users who are creating events from the template to be able to see the Accountability Officer Messages section.

Note: If a section of the template is not ready for publication, you cannot set the visibility options for that section to "Read-Only" or "Hide."

7. Click **Apply**.

Manage accountability events

The following sections describe how to create and manage AtHoc Account events:

- [Start an accountability event](#)
- [Search for and sort accountability events](#)
- [Change the end time of a live event](#)
- [Report on behalf of users](#)
- [End an accountability event](#)
- [Generate an accountability event report](#)
- [Export accountability events](#)

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

- [View all Quick Action Guides.](#)
- [Create a new accountability event](#)
- [Generate an accountability report](#)
- [Report on behalf of users](#)

Start an accountability event



1. In the navigation bar, click **Account > New Event**.
2. On the **Select Accountability Template** screen, click **Select** next to the template you want to use as the basis for the event.
3. Refer to the following topics for detailed instructions on how to fill in or modify existing content in the template and identify affected users:
 - [Define details for an accountability template or event](#)
 - [Define affected users for an accountability template or event](#)
 - [Define user messages and workflow for an accountability template or event](#)
 - [Add Accountability Officers](#)
 - [Define Accountability Officer messages](#)
 - [Set recurrence](#)
4. When you have finished creating the event, click **Review and Start** to review the details and settings for the event. The Affected Users Summary section of the Review and Start screen displays device type and targeting information for all users. If dependents are enabled for your organization and targeted in the event, they are displayed.
5. If you need to change anything, click **Cancel** on the **Review and Start** screen and then make the changes on the event creation screen.
6. Click **Start**.

Search for and sort accountability events

The accountability events search engine matches any set of letters or numbers anywhere in an accountability template name or description and is not case-sensitive. You can search using multiple terms. Each search term entry creates a separate pill and has an AND condition between them.

Wildcards are not supported in searches.

1. In the navigation bar, click **Account > All Events**.

2. On the **Accountability Events** screen, type or paste a word or phrase found in the event title in the search box and then click  or press **Enter**.
3. Optionally, click **Advanced**. In the **Advanced Filter** window, you can select to filter events by severity, event status, organization, status attribute, or by date.
4. Optionally, for enterprise and super enterprise organizations, in the **Advanced Filter** window, select an organization from the **Event From** list to view accountability events from sub enterprise organizations and suborganizations.
5. Optionally, for super enterprise or enterprise organizations with suborganizations, click the options from the **All Accountability Events** list to view events from only the organization you are currently logged in to, only suborganizations, or all organizations.
6. Click **Apply**.
7. Click .

You can click a column header to sort the list of accountability events by **Name**, **Event Status**, **Start Time**, or **Started By** values.

Change the end time of a live event

After an accountability event has been published and is still live, you can change the end time of the event.

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, click the accountability event whose end time you want to change.
3. On the **Summary** tab, click **More Actions > Change End Time**.
4. On the **Change End Time** window, select the new end time.
5. Click **Apply**.

You can also change the end time of a live accountability event from the Details tab of the accountability event. Scroll down to the **Messages and Workflow** section and then click **Change End Time**.

Report on behalf of users

You can designate Accountability Officers who can update the status of users on their behalf. If the Accountability Officer is aware of user statuses, perhaps from their supervisor or a call they made to the call center, they can update their status in the system.

When you start an accountability event, you can specify emails to be sent directly to Accountability Officers. The Accountability Officer email contains a link that takes them directly to the Users tab of the Accountability Event in the BlackBerry AtHoc management system. Only users who do not have a status for the event are displayed, enabling the Accountability Officer to quickly respond on behalf of those users.

While an event is live, Accountability Officers can manually report the status of a user.

When an accountability event is started from an enterprise or super enterprise, the “For more info” link in the notification alert opens the Summary tab of the event in the management system. This gives Accountability Officers access to the correct users based on the Accountability Officer role assignments and restrictions. When an accountability event is started from an enterprise or super enterprise organization, Accountability Officers can respond on behalf of others only when they have been granted the Accountability Officer role in the originating enterprise or super enterprise organization. Accountability Officers who do not have an operator account in the enterprise or super enterprise organization can be targeted, but must first be granted the Accountability Officer role in the enterprise or super enterprise organization in order to respond on behalf of other users.

1. In the navigation bar, click **Account > All Events**.

2. On the **Accountability Events** screen, click the event whose user statuses you want to update.
3. On the **event dashboard** screen, click the **Users** tab.
4. To change the status for a single user, click in the **Status** column. The Change Status window opens. The Status History section displays up to 20 previous status updates for the selected user. The Change Status window also contains a link with the selected user's name. Click this link to view additional details about the selected user.

To update the status for multiple users, select the check boxes next to their names, and then click **Change Status** at the top of the screen. The **Change Status for selected users** screen opens.

Note: The Change Status button appears only while the event is live.

5. Select a status from the **Status** list. The default is "No Status." If you want to clear the current status, select "No Status."
6. Optionally, in the **Comments** field, enter details about why you are manually updating the user status. For example, "User showed up in the office and is out of the event zone" or "User is part of a group that called in their statuses together."
7. Click **Apply**.

The Users tab updates the user's details and displays the updated status in the **Status** column and the word "Operator" in the **Updated By** column, indicating that the status was provided by an operator.

Report on behalf of dependents

If dependents are enabled for your organization and in the accountability template, they can log in to Self Service and respond to events. If they are not able to respond, or a password has not been added to their profile so they can access Self Service, Accountability Officers and Accountability Managers can update the status of dependents from the Users tab of an accountability event.

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, click the event whose dependents' statuses you want to update.
3. On the event dashboard screen, click the **Users** tab.
4. Click **Add**.
5. Select the **Sponsor** attribute. The Users tab updates to include a column that shows the display name for each sponsor user.
6. Optionally, click the **Sponsor** column heading to group users by sponsor.
7. To change the status for a single dependent, click in the **Status** column.

To update the status for multiple dependents, select the check boxes next to their names, and then click **Change Status**. The **Change Status for selected users** screen opens.

Note: The Change Status button appears only while the event is live.

8. Select a status from the **Status** list. The default is "No Status." If you want to clear the current status, select **No Status**.
9. Optionally, in the **Comments** field, enter details about why you are manually updating the dependent user's status.
10. Click **Apply**.

The Users tab updates the user's details and displays the updated status in the **Status** column.

Note: Sponsors can update the status of their dependents from Self Service. For more information, see "[Respond to an event on behalf of your dependents](#)" in the *BlackBerry AtHoc Self Service User Guide*.

End an accountability event

You can end a live event in two ways: from the Accountability Event screen and from within the event details screen.

From the Accountability Event screen:

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, select the check box next to the event you want to end.
3. Click **End**.
4. On the **End Event** confirmation window, click **End**.

From the event details screen:

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, click anywhere in the line for the event you want to end.
3. On the event details screen, click **End Event**.

Generate an accountability event report

Tip: View the [Generate an accountability report](#) quick action guide for quick steps to complete this task. You can also view all [Quick Action Guides](#).

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** window, click the event that you want to export as a report.
3. Optionally, on the **Event Dashboard** screen, apply filters on the **Users** and **Hierarchy** tabs.
4. Optionally, on the **Users** tab, click **Add** to select and add user attributes, operator attributes, or devices to the report. To see if users are sponsor users or dependent users, add the **Sponsor** attribute. This enables you to see what sponsor user dependent users belong to.
5. Click **More Actions > Export**.
6. On the **Export Event** window, select the format for the export: **PDF** or **CSV**.
7. Optionally, add a description to the report. For .pdf files, the description appears under the report title and above the report content. For .csv files, the description appears as the first line in the file.
8. Optionally, select the **Summary** check box to include the information on the **Summary** tab. The .pdf displays a pie chart and bar graph. The .csv file displays the summary in tabular form.
9. Optionally, select the **Hierarchy** check box to include a breakdown of all user statuses by organization hierarchy. If you have applied a filter in the **Hierarchy** tab, the **View Filters** link appears under the **Users with status** check box.
10. Optionally, in the **Users with status** list, select the kind of user that you want to see event details for. This is a useful tool for quickly generating a list of all users who have not yet responded to alerts associated with the event or who have responded that they need help. You can also generate a list of all affected users, all users with any status, or users with a specific status. If you have applied a filter in the **Users** tab, the **View Filters** link appears under the **Users with a status** check box.

Note: At least one of the check boxes must be selected.

11. Click **Export**.

Export accountability events

You can export accountability events to a .csv file.

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, select the check boxes next to the events to export.
3. Click **More Actions > Export**.

A .csv file downloads to your local computer. The .csv file contains the following information for each exported event: Event ID, Event Name, Event Body, Event Status, Start Time, Organization, Affected, and Have Status.

View accountability events


You can view the details of individual live and ended accountability events.

1. In the navigation bar, click **Account > All Events**.
2. On the **Accountability Events** screen, click anywhere on the line containing the event whose details you want to view.
3. A detailed dashboard for the event appears, with the event information contained in the following tabs:
 - [Summary](#)
 - [Users](#)
 - [Hierarchy](#)
 - [Activity](#)
 - [Details](#)

Note: If you are an Accountability Officer or Accountability Manager with restricted user base permissions, only restricted users are visible in the event dashboard. A banner on all tabs of the event dashboard indicates how many affected users out of the total number for the event are accessible for you.

If you are viewing the Accountability Events screen from an enterprise organization, accountability events created by your suborganizations are also displayed. If you are viewing the Accountability Events screen from a super enterprise organization, accountability events created by your sub enterprise organizations and suborganizations are also displayed. The Organization column displays the name of the enterprise or suborganization.

You can use the **Advanced search** field to view accountability events from the organization you are currently logged in to, or specific suborganizations. You can use the **All Accountability Events** arrow to view events from only the organization you are currently logged in to, only suborganizations, or all organizations.

The individual alerts that are sent as part of an accountability event can also be viewed, but not duplicated, from the Sent Alerts screen. These alerts are indicated by a  on the Sent Alerts screen.

View an accountability event summary

The Accountability Event Summary tab is divided into two sections:

- A listing of users statuses and a graphical representation of that information
- A chart that shows the cumulative number of users who have had their status determined over the timeline of the event

List of user statuses

The top of the Summary tab contains a list of all of the available statuses for the event and the number of users who currently have each status. It also displays the percentage of overall users who have each status. Note that these statistics are cumulative. They include statuses provided by users from all alerts generated in relation to the event.

- Hover over the graphical representation of the user status to see a tool tip that displays the number of users with that status. If dependents are enabled in your organization and in the accountability template, the tool tip also displays the number of sponsors and dependents.
- Click a number or percentage in this field to open the Users tab, which displays only the users who have the status you clicked.
- Click the arrow next to the percentage value to display a menu with two options:

- **View:** The same functionality as clicking the number or percentage. Opens the Users tab displaying only the users with the status you clicked.
- **Send Alert:** Takes you to a details screen for the alert that the event is associated with in the system. The alert is automatically targeted at the users who have the status you clicked on in the Summary screen. Using this alert details screen, you can modify the alert and then resend it to the targeted users.

Note: If you click **Cancel** in the details screen, you are taken to the Sent Alerts screen. The individual alerts in an accountability event are displayed on the Sent Alerts screen, but the aggregated messages for accountability events themselves are not. Click **Account > All Events** to return to the list of accountability events.

Updated by

At the bottom of the list of user statuses section, the **Updated by User** and **Updated by Operator** fields tell you how many of the statuses listed on the screen were provided by users versus provided by operators on behalf of users. If dependents are enabled for your organization and in the accountability template, the **Updated by User** field is replaced by the **Updated by Sponsor** and **Updated by Dependent** fields.

While the event is live, an **Update status on behalf of users** button appears next to these fields. Clicking it takes you to the Users tab where you can manually update user statuses. After an event ends, this button disappears and you can no longer update user statuses.

Accountability Officers Targeted

Under the user status graphic, the Accountability Officers Targeted fields list the total number of targeted Accountability Officers and the number of Accountability Officers with the following response options:

- Available
- Not Available
- No Response
- In Progress or Failed

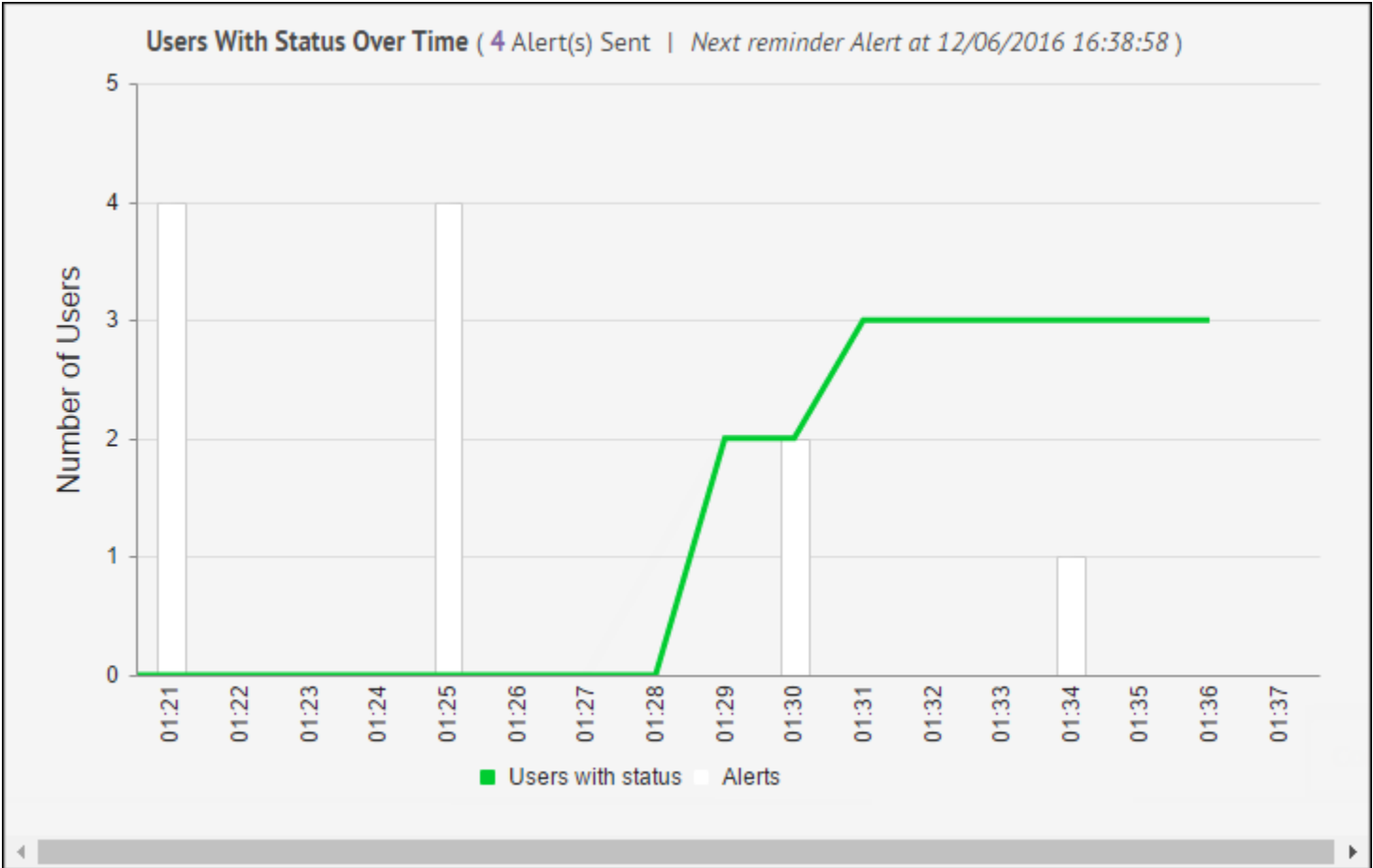
Click on the number link next to the In Progress or Failed option to view a User Tracking report in a separate browser tab. Click the number link next to any of the other options to view a Device Tracking report.

Status chart

The status chart section of the Summary tab displays a timeline with two different elements on it:

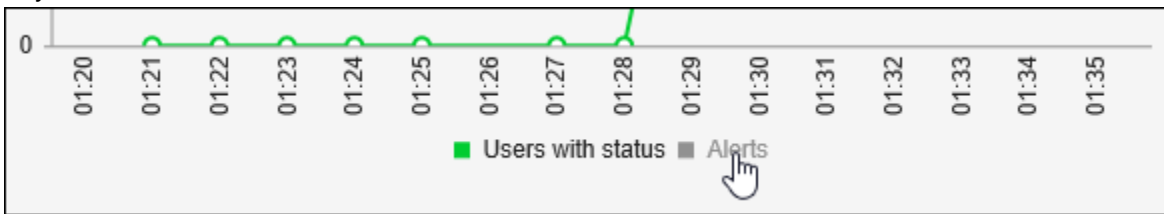
White vertical bars display the total number of users targeted in the initial and all subsequent alerts. This number normally decreases over time as more users provide their statuses and are excluded from subsequent reminder alerts. The final alert is sent to all users to notify them that the event has concluded.

A green continuous line displays the total number of users over time who have provided their status.



Click the number of alerts in the **Users With Status Over Time (<X> Alert(s) Sent)** title opens the Activity tab for the event. The Activity tab displays details of the original alert, ending alert (if the event has ended) and any reminder alerts that are in the queue or that have been sent.



Click the corresponding text in the line below the chart to toggle the white bars and the green line can on and off individually.




In addition to providing information on the progress of the event, the chart allows you to tell at a glance when statuses have been recorded for all users, making additional reminder alerts unnecessary. At that point, you can click **End Event** at the top of the screen. This halts all queued reminder alerts and causes an Ending Alert to be sent to all affected users.

View users for an accountability event

The Accountability Event Users tab lists all users who are affected by the event and provides information as to their current statuses. The default columns that appear on the screen are:

- **Display Name**
 - **Status:** While the event is live, you can click  in the Status column to open the **Change Status** window where you can select a status for a user and add a comment relating to the user's status. The name of the user is displayed as a hyperlink that opens a window displaying the user's profile information. The status history for the user is also displayed. When an event is ended, you can click  to open the **Status History** window and view the status history of the user, including the time the status was updated, any comments entered when the status was updated, and who updated the status.
 - **Updated By:** The Updated By column indicates whether the status information for the user was provided directly by the user or if it was added manually by an operator.
 - **Updated On:** The timestamp of the latest update for a user.
 - **Comments:** The Comments column displays status-related information about a user when the user's status was added manually by an operator. Examples of comments that might appear in this column include "User showed up in the office and is out of the event zone" or "User is part of a group that called in their statuses together."
 - **Add/Reset:** The Add link allows you to access a list of user attributes that you can add as columns in the list. The Reset link allows you to reset the list to the default column layout.
- Tip:** To view dependent users, add the Sponsor attribute. All users will be displayed and sponsor users appear with (self) after their username.

Use the **Advanced** button next to the search field to run an advanced search of the users who appear on the screen. This is useful during events when it is necessary to classify users in the list based on attributes such as work location, medical training, or organization membership.

Use the  button to filter the list of users by groups such as organization hierarchy or distribution list.

Dependent users also appear on the Users tab. To view the sponsors of dependent users, click **Add > Sponsor** to add the Sponsor attribute. The Sponsor column appears and shows the display name of the dependent user's sponsor. Sponsors are sponsors of themselves, so the Sponsor column shows their display name with "Self" in parenthesis. Click the Sponsor column heading to group sponsors with their dependents.

You can filter the types of users you see in the Users list by clicking the link that appears below the main search field and selecting the status type you want to display.

Although the specific statuses that appear in the list vary depending on the sort of event that was created, the **All Affected Users**, **All Statuses**, and **No Status** options always appear in the list.

- The *All Affected Users* option displays everyone affected by the event, regardless of whether they have a status recorded for the event.
- The *All Statuses* option displays only users who have a status recorded for the event.
- The *No Status* option displays only users who do not have a status recorded for the event.

View accountability event status by organization

The Accountability Event Hierarchy tab displays all event statuses based on the hierarchy of the organization affected users belong to. Presented in a table format, each possible status appears as a column and each organization hierarchy level appears as a separate row.

The numbers in each cell represent the number of users who are at the selected hierarchy level and who have the selected status. Click any number in a cell to open the **Users** tab with the hierarchy level preselected as a search criteria and the relevant users displayed in the users list.

The Hierarchy tab displays event statuses sorted by organization hierarchy by default.

When logged in to a super enterprise or enterprise organization, the hierarchy includes All Users as a parent node and suborganizations as child nodes. The All Users node includes an aggregate of all sub enterprise organizations and suborganizations.

When logged in to an enterprise organization without any suborganizations, the hierarchy of the enterprise organization is displayed.

View accountability event activity

The Accountability Event Activity tab displays all alerts that have been sent and that are queued up to be sent during the event.

At the start of an event, the Activity tab displays the **Start Alert** with a status of **Live** and a **View Alert** link in the Actions column. If reminder alerts are enabled for the event, a Reminder Alert line appears next in the list, followed by an Ending Alert line. Both of these alerts are initially listed with a status of **Queued**.

As each successive **Reminder Alert** is sent, the word "Reminder:" is appended to the alert name, its status changes to **Live**, and a **View Alert** link appears in its row in the Actions column.

When the event times out or when an operator manually ends the event—usually because all affected users have responded—the **Ending Alert** is sent, at which time the word "Ended:" is appended to the alert name, the status of all alerts on the Activity tab changes to **Ended**, and a **View Alert** link appears in the Ending Alert row in the Actions column.

View accountability event details

The Details tab displays the same information that is available on the **Review and Start** screen that appears after an operator has finished creating an event.

- [Event details](#)
- [Affected Users](#)
- [Messages and Workflow](#)
- [Add Accountability Officers](#)
- [Accountability Officer Messages](#)

If attachments are enabled for your organization and included in the event, they are displayed as images. Click the image of the attachment to preview the attachment. On the preview window, click **Download** to download the attachment.

To view event-related status information about each user, click the **Affected Users** link in the **Affected Users** section. This link brings you to the Details tab. The Affected Users section on the Details tab contains a link to the Users tab, which provides event-related status information about each user.

To view the Accountability Officers for the event, click the **List Targeted Accountability Officers** link in the Accountability Officers section.

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

View live accountability events on a map


You can view live accountability events and alerts on the live or publisher map. For details, see the [BlackBerry AtHoc Live Map](#) guide.

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

Click an event or alert on the map to open a pop-up window that displays the following information for the live event or alert:

- Name of the event or alert
- Type of item: accountability event or alert
- Last updated date and time
- GPS coordinates in Latitude, Longitude (for incoming mobile alerts only)
- Number of affected users
- Number and percentage of users with a status
- Summary of user statuses by response option

In the event pop-up window, click **Open Event** to go to the Summary tab of the event in the event manager.

If there are multiple events or alerts in the same location on the map, click  to scroll through the event pop-ups for each alert or event.

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

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

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, MERCHANTABILITY, 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