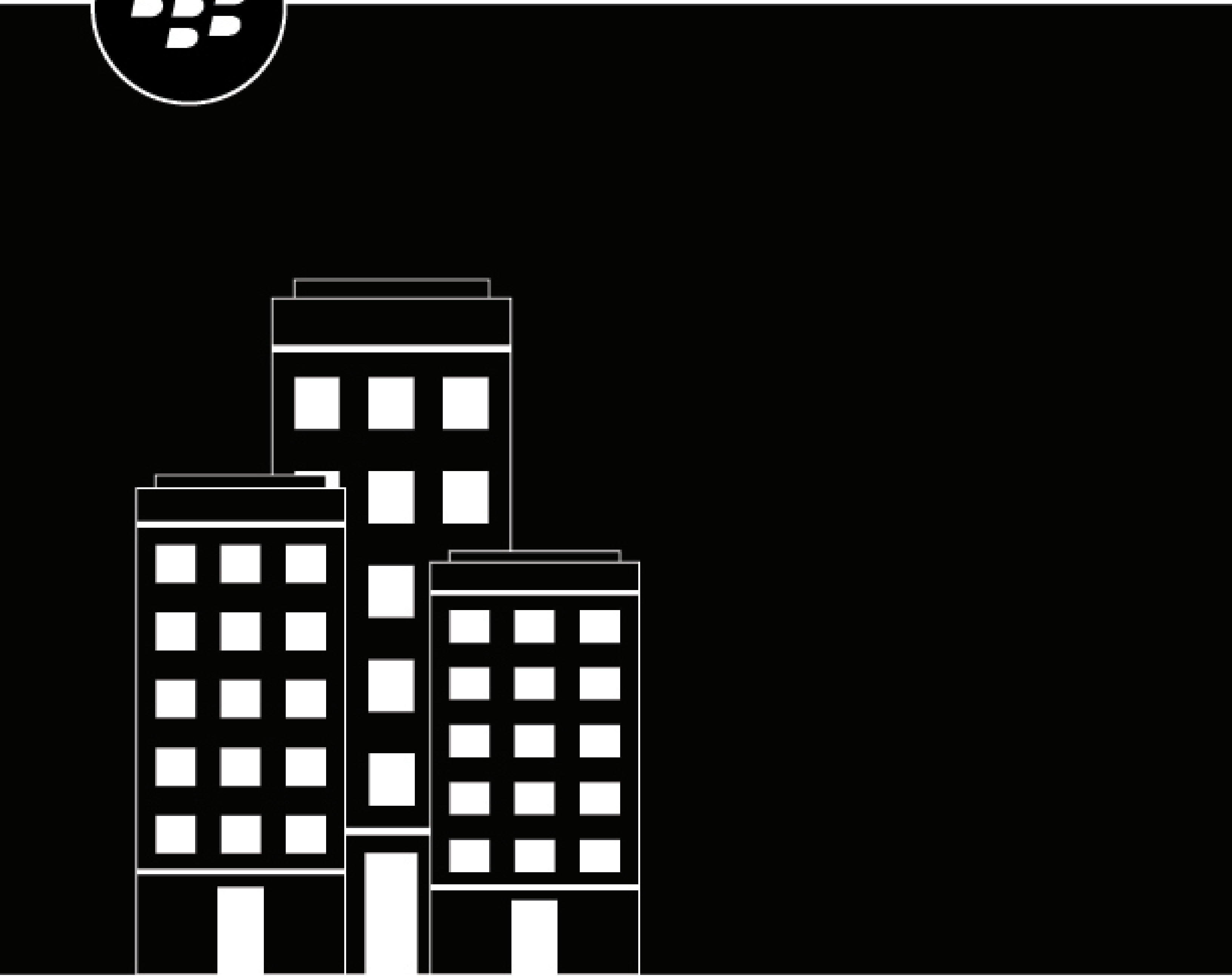


BlackBerry AtHoc

Self Service User Guide

7.16

Contents

What is BlackBerry AtHoc Self Service?

The BlackBerry® AtHoc® emergency notification system has been installed at your site to deliver alerts regarding critical incidents and situations such as severe weather events, external threats, and environmental disasters.

Self Service is a web application that allows you to receive and respond to critical alerts and accountability events targeted to you. Using Self Service, you can also view and manage your profile, update your password, manage your dependents, move to another organization, and subscribe to other organizations.

Note: Self Service is section 508-compliant.

Tip: View the following quick action guides for simple steps to complete key tasks in Self Service:

- Register for Self Service
- Move to an organization
- Subscribe to organizations
- Prioritize your personal devices
- Add a dependent

Register for Self Service

Note: If you have the BlackBerry AtHoc desktop app installed on your desktop, you do not need to register and this section is not relevant to you.

1. Click the URL link for BlackBerry AtHoc Self Service that was provided to you by your administrator.
2. On the **Registration** screen enter an email address or username.
3. Create and confirm a password for your account.
4. Complete any additional required fields.
5. If your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
6. Click **Register**. Your profile page opens in Self Service.
7. On the **My Profile** page, complete all required fields.
8. If your system is configured to require an organizational hierarchy selection, click **Select** next to **Updated Organizational Hierarchy**.
9. On the **Select the Organizational Position** window, select your organizational hierarchy and click **Apply**.
10. Click **Submit**.

You can now go to your Inbox to view and respond to alerts and messages from your organization.

Access Self Service using the BlackBerry AtHoc desktop app

1. Right-click in your system tray menu.
2. In the menu that appears, click **Access Self Service**.
3. On the **Welcome pop-up screen**, click **OK**.

The Self Service application opens, displaying the Inbox, which contains information about all alerts in the system that relate to you.

Access Self Service from a URL link

Note: The only time you need to sign in to Self Service is if the computer you are using does not have the BlackBerry AtHoc desktop app installed, single sign-on is disabled for your organization, and you do not use a Windows username/domain combination or a CAC card for authentication.

1. Click the **URL** provided by your administrator.
2. On the **Login** screen, enter your **Username** and **password**.

   Note: Your username and password are normally the same as your Windows login username and password. In some cases, though, your organization will send you a unique username and password that you should use instead.
3. Optionally, click **English (US)** at the bottom of the Login screen to switch the language that is displayed in Self Service.
4. Click **Log In**.
5. If your system has two-factor authentication enabled, you will see the Two-Factor Authentication page. To continue accessing Self Service, complete the following steps:

   a. Choose a delivery method to receive a verification code (email, phone, or text.)
   b. Optionally, if your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
   c. Click **Next**. The Verification Required window opens and a verification code is sent to your device.
   d. Enter the verification code and click **Submit**.

Reset your forgotten password

Note: The information in the following topic is relevant only if you log in to Self Service using a username and password.

1. On the login screen, click **Forgot Password?** under the **Password** field.
2. On the **Reset Password** screen, from the **Select Verification Method** list, select **Email** or **Text Message**.
3. Enter the email address or text-messaging number associated with your BlackBerry AtHoc account.
4. If your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
5. Click **Submit**. If your email address or text-messaging number is found in the BlackBerry AtHoc system, a message is displayed instructing you to check your email or text for instructions to reset your password. If your email or text-messaging number is not found in the BlackBerry AtHoc system, a message is displayed.
6. Open the email or text message, then click the **Create/reset your password here** link embedded in the body of the message.
7. On the **Create/Reset Password** screen, enter your username.
8. Click **Next**.
9. On the **Create/Reset Password** screen, enter and re-enter your new password.
10. Click **Next.** If your password meets the length and complexity requirements set by your administrator, a confirmation screen appears.
11. Click **Go to Login**.

Recover your forgotten username

Note: The information in the following topic is relevant only if you log in to Self Service using a username and password.

1. On the login screen, click **Forgot Username?** under the **Username** field.
2. On the **Retrieve Username** screen, from the **Select Verification Method** list, select **Email** or **Text Message**.
3. Enter the email or text-messaging number associated with your BlackBerry AtHoc account.
4. If your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
5. Click **Submit**. If your email address or text-messaging number is found in the BlackBerry AtHoc system, a message is displayed instructing you to check for your username in your email or text. If your email or text-messaging number is not found in the BlackBerry AtHoc system, a message is displayed.
6. Log in to Self Service using the username that appears in the email or text message.

Inbox

The Inbox displays the alerts and events that have been sent to you.

View a list of your alerts and events

To view a list of your alerts and events in Self Service, click the **Inbox** button in the top navigation bar. The Inbox appears, and displays the following information about your alerts and events:

- Severity
- Title
- Status (Live or Ended)
- Updated date and time
- Type
- Published By

Alerts and events in the Inbox that include a map display a ◀.

By default, 20 items are displayed per page. You can set the Inbox to display 50 or 100 items per page.

Note: This list contains only live and ended alerts and events that have been sent to you.

Tip: Click any column heading to sort the Inbox. Click ↻ to update the Inbox.

View the details of an alert or event

You can view details about the alerts and events in your Self Service Inbox.

1. Click **Inbox** in the top navigation bar. The Inbox opens, displaying your alerts and events.
2. Click the alert or event that you want to view. The alert or event details screen opens.

   The following information is displayed for a selected alert:

   - **Details** section:
     - Severity
     - Title
     - Status
     - Time
     - Type
     - Published By
     - Expiration date and time
   - **Response Options** section:
     - Available response options
     - Replied on date and time
   - **Content** section:
     - Body content
     - Location (if included in the alert)

   The following information is displayed for a selected event:

   - **Details** section:

    - Severity
    - Title
    - Status
    - Date and time
    - Published By
    - Expiration date and time
  - **Update Status** section:
    - Display name and status of users
  - **Content** section:
    - Body content
    - Location (if included in the event)
  - **Status History** section:
    - Status, date, time, and updated by information
  - **Dependents Status History** section:
    - Status, date, time, and updated by information for each dependent
  - **Alerts** section:
    - Alert title for the initial, reminder, and ending alerts for the event
    - Date and time for each alert
    - Content text of each alert

3. Optionally, for alerts that require a response, select your response in the **Response Options** section and click **Submit Response**.
4. Optionally, for events that require a response, in the **Update My Status** section, click ✎. On the **Affected Users** window, select your status from the list and click **Apply**.

View an alert location on a map

To view location details for an alert or event that appears in the Inbox, complete the following steps:

1. Click **Inbox** in the top navigation bar. The Inbox appears, displaying all of your alerts and events.
2. Click the alert or event whose location details you want to view. The alert or event details screen opens.
3. In the **Content** section, click ✎ next to the small map to view the alert or event location on a large map.

Search your Inbox for an alert or event

1. Click **Inbox** in the top navigation bar. The Inbox appears, displaying your alerts and events.
2. In the **Search** field, enter all or part of a word or phrase that appears in the title or content of the alert or event you are searching for.
3. Click 🔍.

The screen refreshes and displays all alerts and events that match your search criteria.

Filter the Inbox

You can filter the Inbox by the clicking **Advanced** beside the search field. Filter by any of the following event or alert parameters:

- **Published By**: Enter the username for an alert or event publisher.
- **Alert type**: Click **Select Types**. On the **Select Alert Types** window, select one or more types and click **OK**.
- **Severity**: Select one or more severity options.
- **Pending Reply**: Select **Yes** or **No**.
- **Status**: Select **Live** or **Expired**.
- **Sent** and **To**: See Filter the Inbox by date.

When you have selected the parameters, click **Apply**. Your Inbox refreshes and displays the alerts and events that have the parameters you selected.

Filter the Inbox by date

You can filter the Inbox so that it displays only alerts or events that fall within a specific date range. To include all alerts and events up to a specific date or all alerts and events on or after a specific date, leave the other date range field blank and create an open-ended filter. For example, a filter set to `Show alerts between 06/01/2021 and MM/dd/yyyy` includes all alerts that took place on or after June 1, 2021 up to and including the current date. Similarly, a filter set to `Show alerts between MM/dd/yyyy and 06/01/2021` includes all alerts that took place up to and including June 1, 2021.

1. In the top navigation bar, click **Inbox**. The Inbox appears, displaying your alerts and events.
2. Click **Advanced** beside the search field to expand it.
3. In the first field in the **Sent** section, enter the month, date, and year that you want to use as the starting date.

   Note: You can also click 📅 and select the date you want from the calendar. To navigate to a different month, click ‹ and ›. To navigate to a different year, click the current year and then use the ‹ and › arrows to move to the year you want.
4. In **To** field, enter or select the month, date, and year that you want to use as the ending date.
5. Click **Apply**.

The Inbox refreshes to display only the alerts and events that fall within the range you specified.

Respond to an alert from the Inbox

1. In the top navigation bar, click **Inbox**. The Inbox appears, displaying your alerts and events.
2. Click the alert you want to respond to.
3. On the alert details page, in the **Response Options** section, select your response.
4. Click **Submit Response**. A success message appears and the Response Options section refreshes to display the date and time of your response.
5. Click **Back** to return to the Inbox.

Respond to an event from the Inbox

1. In the top navigation bar, click **Inbox**. The Inbox appears, displaying your alerts and events.
2. Click the event you want to reply to.

   Tip: Click ⟲ to view the Status History for the event. This option is visible only for users who have a status.

3. On the event details page, in the **Update My Status** section, click ✎.
4. On the **Affected Users** window, select your status from the list.
5. Optionally, add text in the **Comments** field.
6. Click **Apply**. The event details page refreshes and displays your updated status in the **Update Status** section.
7. Click **Back** to return to the Inbox.

Respond to an event on behalf of your dependents

You can respond to an event on behalf of your dependents from your Self Service Inbox.

1. In the top navigation bar, click **Inbox**. The Inbox appears, displaying your alerts and events.
2. Click the event that you want to respond to on behalf of your dependents.

   Tip: Click ⟲ to view the Dependents Status History for the event. This option is visible only for dependents who have a status.
3. On the event details page, in the **Update Status** section, click ✎ in the row for your dependent.
4. On the **Affected Users** window, select a status from the **Status** list.
5. Optionally, add a comment about the status of your dependent in the **Comments** field.
6. Click **Apply**. The event details page refreshes and displays the updated status of your dependent in the **Update Status** section.
7. Optionally, repeat Steps 3 through 6 to update the status of additional dependents.
8. Click **Back** to return to the Inbox.

My Profile screen

The My Profile screen displays information related to your profile in the BlackBerry AtHoc system and allows you to view and update your profile information, prioritize your personal devices, move to a different organization, and subscribe to organizations.

View your profile

To view your profile in Self Service, click **My Profile** in the top navigation bar. The My Profile screen appears, displaying your profile information divided into the following sections:

- **Basic Information**: Displays your Username, Mapping ID, First name, Last name, Display name, Pin (if your system is set up to receive voicemail on mobile, VoIP, and land line phones), Created on date, Home Address, Temporary work location, Organizational hierarchy, and User ID.
- **Numbers**: Displays your home and mobile phone numbers.
- **Online Addresses**: Displays your personal and work email addresses and your text messaging number.
- **Physical Addresses**: Displays your home and work addresses. If you have performed a check in or check out, turned on tracking, sent a report or emergency, or responded to an alert from the BlackBerry AtHoc mobile app, your last known location is also displayed.
- **Password**: This section appears only if your organization requires manual authentication. Displays the date and time the password was last changed and includes an Edit link that can be clicked to change the password.
- **Organization Subscriptions**: This section only appears if the organization subscription feature is enabled for your organization and organizations are configured for subscription. This section displays your organization subscriptions and the end date for each subscription, if set.
- **BlackBerry AtHoc Apps**: Shows whether you are active on the BlackBerry AtHoc desktop app and mobile app. If you are logged in, the number of instances you are logged in to on each app is displayed. If you are not logged in, the field displays the phrase *Not Available*.
- **Advanced Information**: Displays any custom attributes defined by your System Administrator.

Edit your profile

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** screen, click **Edit**.

   The screen refreshes and the following fields become editable:

   - **Basic Information**: You can edit any attributes that are configured for your organization, if your organization is set up to allow attributes to be updated by end users.
   - **Numbers**: Phone - Mobile and Phone - Home
   - **Online addresses**: Email - Personal and Email - Work
   - **Physical addresses**: Displays your home and work addresses. For more information, see Update a physical address. If you have performed a check in, check out, turned on tracking, sent a report or emergency, or responded to an alert from the BlackBerry AtHoc mobile app, your last known location is displayed. Click **Clear** to remove your last known location. You cannot edit your last known location from Self Service.
   - **Password**: The Password section appears only if your organization requires manual authentication. For more information, see Update your password.
   - **Organization Subscriptions**: This section only appears if the organization subscription feature is enabled for your organization and organizations are configured for subscription. This section displays your

organization subscriptions, the start and end dates, and the assigner for each subscription. For more information, see Subscribe to organizations.

- **BlackBerry AtHoc Apps**: Shows whether you are active on the BlackBerry AtHoc desktop app or mobile app. If you are logged in, the number of instances you are logged in to on each app is displayed. If you are not logged in, the field displays the phrase *Not Available*. Click **Generate Code** during the desktop app registration process to generate a registration code. To delete an unused mobile device, see Delete unused mobile devices from your profile.
- **Advanced Information**: Any custom attributes that your system administrator has given you permission to edit.

3. Make changes to any of the editable fields.
4. Click **Save**.

Delete unused mobile devices from your profile

To prevent reaching the device limit for your profile, you can remove unused mobile devices.

1. In the top navigation bar, click **My Profile**.
2. On your profile page, in the **BlackBerry AtHoc Apps** section, beside **Mobile App**, click **Active (*x*)**.
3. On the **User Mobile Devices** window, click ✖ beside the mobile device you want to delete.
4. On the confirmation window, click **Delete**.

The mobile device is removed from your profile.

Add or update a PIN for voicemail

If voicemail alerts have been configured for your system, you can create or update a PIN for retrieving BlackBerry AtHoc alerts on voicemail.

1. In the top navigation bar, click **My Profile**. The My Profile screen appears, displaying all of your profile information.
2. Click **Edit**.
3. In the **Basic Information** section, enter or update your PIN in the **Pin** field.
4. In the **Confirm Pin** field, enter your PIN again.
5. Click **Save**.

Update a physical address

The system does not allow you to edit the physical addresses associated with your profile, but you can remove them and then enter updated addresses in their place.

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** screen, click **Edit**.
3. In the **Physical addresses** section, click **Clear** beside the address you want to update. The original address is replaced by a text-entry field.
4. Enter the new address, including the zip code.
5. Click **Save**.

The new address appears in the Physical addresses section. Click 🌐 beside the address to see it on a map.

Update your password

Note: The information in the following topic is relevant only if you log in to Self Service manually using a username and password.

1. In the top navigation bar, click **My Profile**. The My Profile screen appears, displaying all of your profile information.
2. In the **Password** section, click **Edit**.
3. On the **Password** window, enter and confirm your new password.

   Note: Any password rules that your organization has created appear on the screen under the Confirm New Password field. If you do not follow the rules, an error message appears and your password is not accepted.
4. Optionally, if your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
5. Click **Update**.
6. On the **My Profile** page, click **Save**.

Update your organizational hierarchy

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** page, click **Edit**.
3. In the **Basic Information** section, click **Select** beside **Updated Organizational Hierarchy**.
4. On the **Select the Organizational Position** window, select your organizational hierarchy and click **Apply**.
5. Click **Save**.

Choose your preferred language

If the Bilingual Alert feature is enabled for your organization, you can select a preferred language to receive alerts in.

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** page, click **Edit**.
3. In the **Basic Information** section, select a language from the **Preferred Language** pull-down menu.
4. Click **Save**.

Prioritize your personal devices

If your administrator has configured the ability for users to prioritize the order of their personal devices, you can prioritize the personal devices you use to receive alerts from the My Profile screen in Self Service. The highest priority personal device will receive any alerts you are targeted in first. If you respond to the alert on that device, the alert is not sent to your other personal devices. You must have at least one personal device enabled with a device address in your user profile to prioritize your personal devices.

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** screen, click **More Actions** > **Prioritize Personal Devices**.
3. On the **Prioritize Personal Devices** window, click ⇕ and drag to reorder the device. Personal devices are prioritized according to their position in the list, with the highest priority device appearing on top. The higher a device is in the list, the higher its priority.

If the desktop app appears in the list of your devices, it cannot be reordered.

4. Click **Save**.

Move to organization

If your administrator has configured the ability for users to move themselves to different organizations, you may move yourself from one organization to another from the My Profile screen in Self Service.

When you move to another organization, your profile data is moved to the new organization. The Self Service page of your new organization may have a different look and layout. If you are an operator, any permissions that you had in your original organization are revoked. If you were an Enterprise Administrator in the enterprise organization, you retain this role. If you had permissions in other organizations within the enterprise or organizations outside of the enterprise organization, they are retained. If you have dependents, they are also moved. If you have subscriptions to other sub organizations, they are cancelled.

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** screen, click **More Actions** > **Move to Organization**.
3. On the **Move to Organization** window, select an organization from the list. You can type the name of the organization to narrow the list.
4. Click **OK**.
5. On the confirmation window, click **Continue**.

Subscribe to organizations

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

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

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

You can cancel your organization subscriptions at any time from the Organization Subscriptions section of the My Profile screen.

1. In the top navigation bar, click **My Profile**.
2. On the **My Profile** screen, click **Edit**.
3. In the **Organization Subscriptions** section, click **Add Subscription**.
4. On the **Subscribe Organization** window, select an organization.
5. Click **Apply**.
6. In the **Organization Subscriptions** section, enter a date or click 📅 to select a start date for the subscription.
7. Optionally, click 📅 to set an end date for the subscription.
8. Optionally, in the **Basic Information** section, enter an address in the **Temporary work location** field.
9. Click **Save**.

Dependents screen

The Dependents screen displays information related to your dependents in the system and allows you to add, edit, or delete dependents.

View, edit, or delete your dependents

1. Log in to Self Service and click **Dependents**. The Dependents screen opens, listing your current dependents.
2. Optionally, enter a name in the **Search by name** field to find a specific dependent.
3. Click the row for a dependent. The Edit Dependent screen opens.
4. Edit the basic user information, contact information, or password as needed.
5. Optionally, in the **BlackBerry AtHoc Apps** section, click **Active (*x*)** beside **Mobile App** to delete your dependent's unused mobile device. On the **User Mobile Devices** window, click ✖ beside the mobile device you want to delete.
6. Click **Save**.
7. Optionally, to delete a dependent click ✖ and then click **Delete** on the confirmation window.

Add a dependent

You can add dependent accounts for family members or anyone that should receive alerts when you do. Add a dependent account for anyone who is your responsibility and does not have an account in the system.

The operator has the option to include dependents when sending out an alert or requesting accountability status.

Dependents can respond to alerts and update their status for events from the Self Service inbox if a password is added to their user profile and manual user authentication is enabled for Self Service in the organization.

If your dependent does not respond to an accountability event, you may be requested to provide their status through the Inbox.

1. Log in to Self Service and click **Dependents**.
2. On the **Dependents** page, click **Add**.
3. On the **New Dependent** window, in the **Basic Information** section, enter a Username, First Name, Last Name, and Display Name. Only a Username is required.
4. Optionally, in the **Online Addresses** section, add contact information for your dependent.
5. Optionally, in the **Password** section, enter and confirm a password for your dependent. You must enter and confirm a password for your dependent if you want your dependent to be able to log in to Self Service to view and respond to alerts and events.
6. Click **Save**.

A Success message is displayed at the top of the New Dependent window.

Prioritize personal devices for your dependents

If your administrator has configured the ability for users to prioritize the order of the personal devices that they receive alerts on, you can prioritize the personal devices for your dependents from the Dependents screen in Self

Service. Your dependent must have at least one personal device enabled with a device address in their user profile to prioritize their personal devices.

1. Log in to Self Service and click **Dependents**.
2. On the **Dependents** screen, click **Prioritize personal device** in the row for the dependent whose devices you want to prioritize.
3. On the **Prioritize Personal Devices** window, click ↕ and drag to reorder the device.
4. Click **Save**.

Troubleshooting

This section describes issues you might encounter with Self Service. In most cases, the solutions provided in this section will resolve these problems. If they do not, contact BlackBerry AtHoc customer support at athocsupport@blackberry.com.

Unable to log in to Self Service

The three most common reasons you might be having trouble logging in to Self Service are described and resolved below.

Registration verification problem

Issue: When you enter your username and password, an Account Verification screen appears, telling you that your account has not yet been verified in the system.

Cause: You have logged into your account before verifying your email.

Solution: Click the **Resend Email** button, then open the email that is sent to your email address and click the **Verify Now** button that appears in the body of the email.

Expired link problem

Issue: When you enter your username and password, an Account Verification screen appears, telling you that the account verification email has expired.

Cause: You did not click the email verification button embedded within the registration email within the specified time of receiving the email. The verification link is only valid for 48 hours; after that you need to request a new link be sent to you via email.

Solution: Click the **Resend Email** button, then within 48 hours, open the email that is sent to your email address and click the **Verify Now** button that appears in the body of the email.

Unrecognized link problem

Issue: When you click a link to access the BlackBerry AtHoc system for your organization, the phrase "The link was not recognized" appears at the top of the login screen.

Cause: There are different reasons why this message might appear, including the following:

- The link you clicked was somehow truncated: for example, if it was in an email and wrapped to a new line.
- The link has changed.
- The link was used in the past.
- Your registration was never completed and your username has been removed from the system. This happens if a username is created and then not verified within 60 days.

Solution: The solution in each of the cases listed above is the same: enter your username and password on the Login screen that you are on, then click **Log In**.

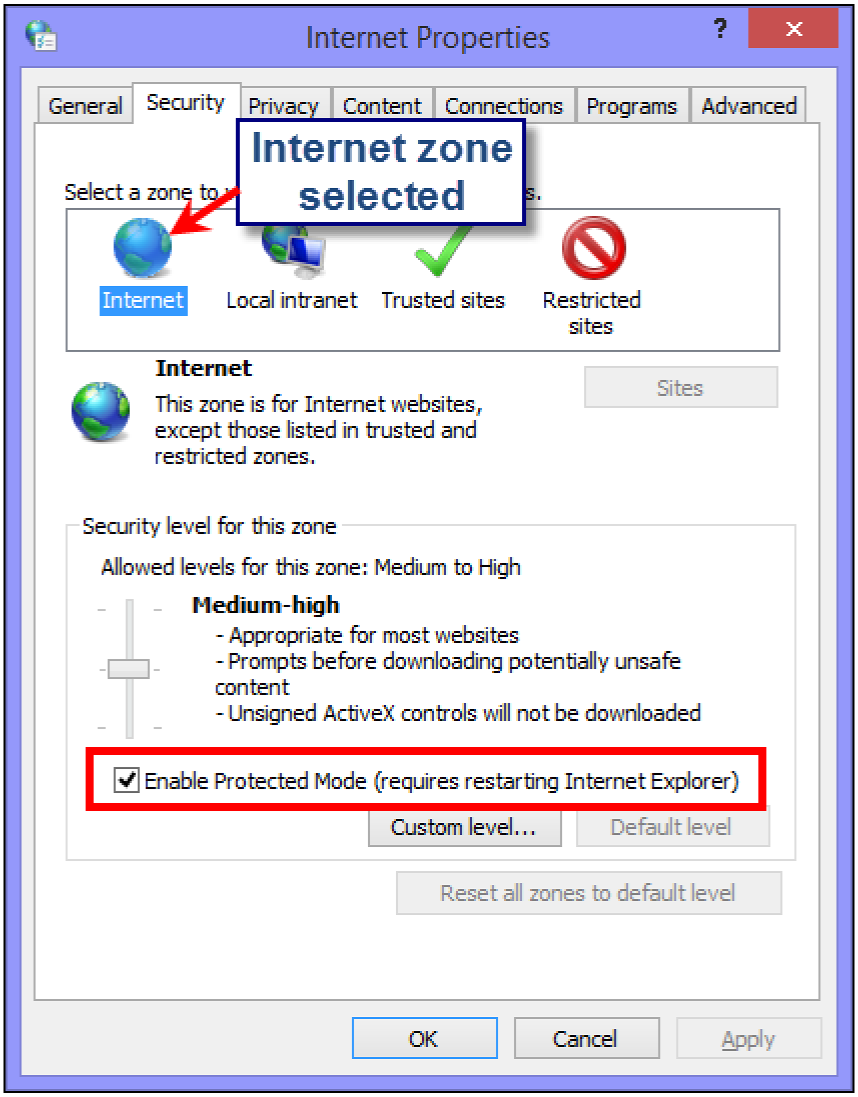
- If the original problem was caused by a truncated or corrupted link but you have successfully registered in the past, entering your username and password on the screen will grant you access to the system.
- If you have forgotten either your username or password, click the corresponding **Forgot Username?** or **Forgot Password?** link on the screen and enter the requested information on the screen that appears.

- If the original problem was due to a registration verification issue, the screen described in the "Registration Verification Problem" section above will appear. Follow the instructions in that section to resolve the issue.
- If the original problem was due to an expired, unverified username, an error message will appear, telling you that the username does not exist. On the Registration screen that appears, create a new username and password.

Workaround for the Self Service validation error

If you are using Internet Explorer (IE) 9 or later with Windows 7 or later, you might receive a validation error when you try to view the Self Service screen. To fix this error, complete the following steps:

1. Go to **Control Panel** > **Internet Options** and click the **Security** tab.
2. With the Internet zone options displayed, select **Enable Protected Mode**.



Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

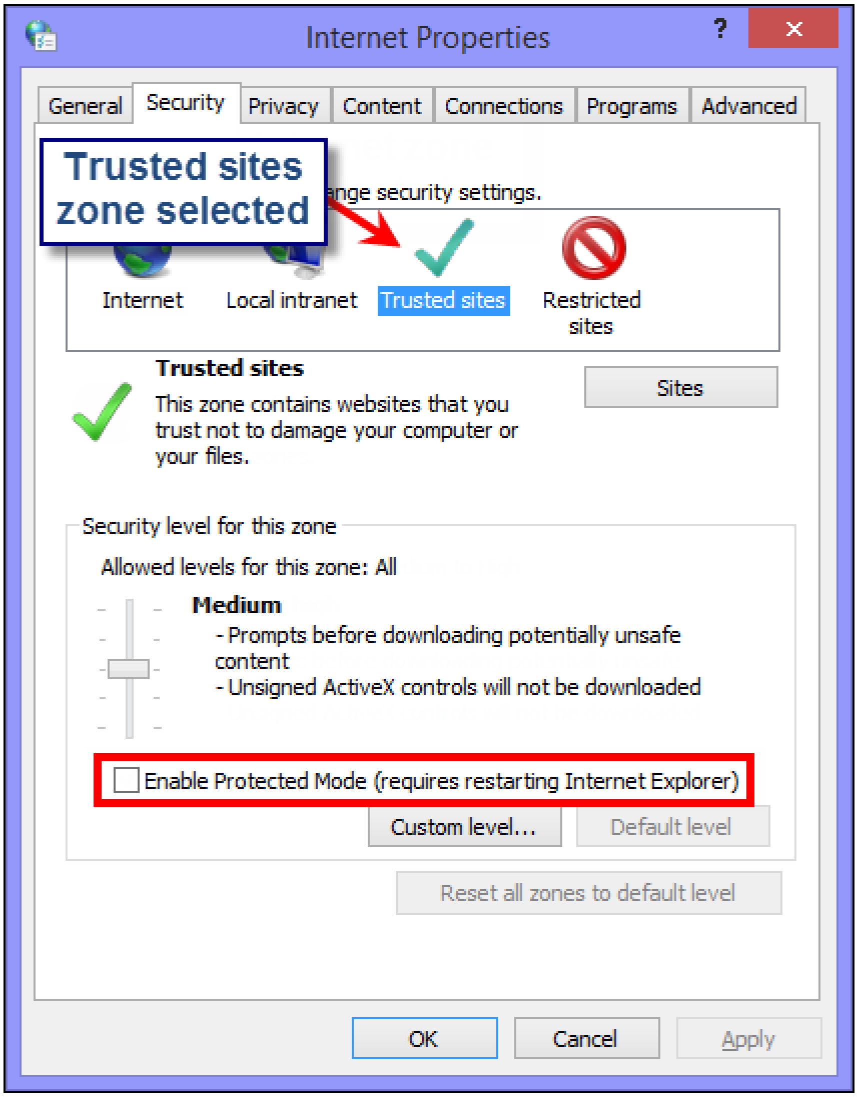
Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

3. Click the **Trusted sites** icon.
4. With the **Trusted sites zone options** displayed, deselect **Enable Protected Mode** if it is selected.



Trusted sites zone selected

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

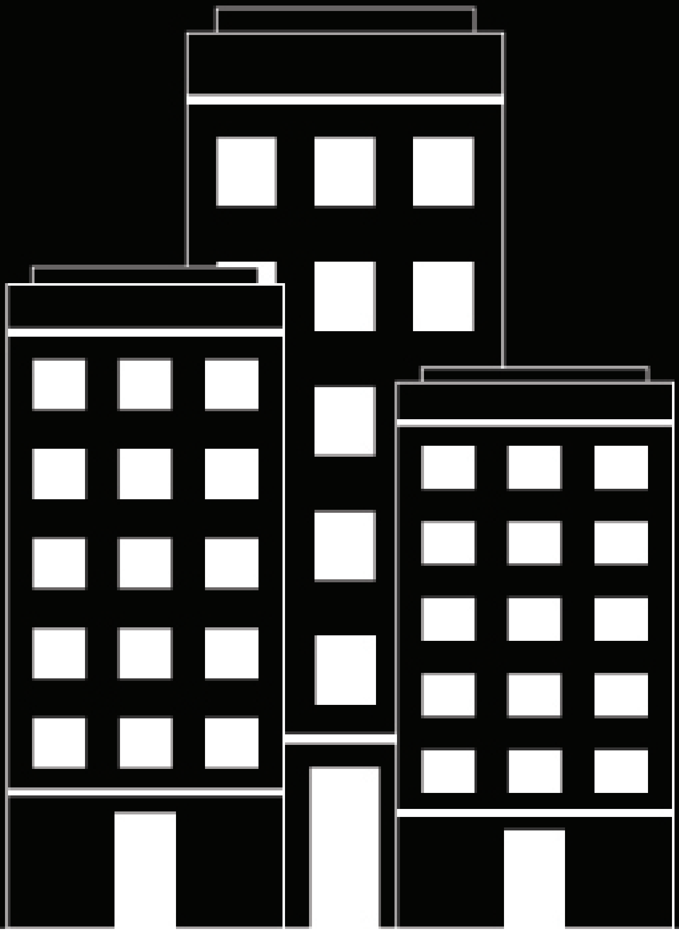
Allowed levels for this zone: All

Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

5. Click **Sites**.
6. On the **Trusted sites** screen, enter the BlackBerry AtHoc website address in the **Add this website to the zone** field.
7. Click **Close**.
8. If the Self Service screen is blocked by Active X (indicated by a yellow bar at the top of the screen requesting permission to display images), click **Yes** to unblock it and allow Active X to display the Self Service screen.



BlackBerry AtHoc

Mobile App User Guide

4.11

Contents

What is the BlackBerry AtHoc mobile app?

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

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

Supported OS versions

- Android: 13.0, 12.0, 11.0, 10.0, and 9.0
- iOS: iOS 16, iOS 15, iOS 14
- iPadOS: with iOS 14

App version support

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

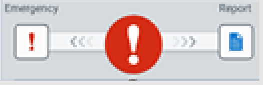
- 3.5.x
- 4.0
- 4.1.x

Home screen

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

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

Item	Name	Description
≡	Menu	Opens the navigation menu.
➤	Track Me	Periodically sends your location to your organization for the duration you choose.
📍 / 📍	Check In/Check Out	Sends your location and timestamp to the server.
+	Alert Publishing	Displays the login screen on tapping the icon. After logging in the alert template screen appears that has the list of alert templates to publish alerts.

Item	Name	Description
	Change view	**All**: Displays all activities including reports, tracking, and registration. **Inbox**: Displays all alerts that have been sent to you.
You are connected to *organization-name*	Organization settings	Displays information about the organization you are currently connected to. For more information, see Organization settings.
💬	Alerts	Displays the number of unread alerts as a badge on the icon.
	Red knob	Slide the red knob to view the following options: • **Report**: Sends information to the central operations center of an organization. Users can select a template to send a report. • **Emergency**: Sends duress messages.
👥	Collaborate	Displays a list of collaborations that you are involved in.

Menu

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

Name	Description
My Organization	Displays the name and logo of the organization you are connected to.
Switch Organization	Changes organizations to receive alerts from different organizations.
Personal Alert Button	Displays details about paired bluetooth buttons. Provides features to pair, test, and unpair a bluetooth device.
My Profile	Displays your user information including name, email, and phone numbers.
Subscriptions	Displays your organization subscriptions.
FAQs	Displays the list of frequently asked questions.
Send Feedback	Opens the email client to send feedback or suggestions.

Name	Description
Send Admin Log	Opens the email client to send a log file to report issues. The default email address, `support@athoc.com` is removed from sending Admin logs flow. When user taps on Send Log button, in the compose email screen, the "To" field is blank.
About Us	Displays the build version number.
Logout	Logs you out of the app. You must have the Alert Publishing or Accountability Manager permission. This option displays only if the user is authenticated and logged in to an organization
Terms of Use	Displays the BlackBerry Solution License Agreement.

Organization settings

Tap your organization name on the home screen to open the Organization settings screen. From the Organization settings screen you can access the following items:

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

Location services

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

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

VPN requirement

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

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

Set up the BlackBerry AtHoc mobile app

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

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

Install the BlackBerry AtHoc mobile app

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

Google Play Store

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

1. On your Android device, tap ▶.

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

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

Apple App Store

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

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

- If scheduled location access is enabled for your organization, on the **"AtHoc" Would Like to Access Your Location** dialog, tap **Continue**.

  a. On the **Allow AtHoc to access this device's location?** dialog, tap **While using the app**.
  b. On the **Location permission** screen, tap **Allow While Using App** or **Allow Once**.

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

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

Register the mobile app

Prerequisites

- Download and install the BlackBerry AtHoc mobile app from the Google Play or Apple App store.
- Before you register the BlackBerry AtHoc mobile app on your device, you may need the organization code provided by your BlackBerry AtHoc administrator. If your organization has a mapped email domain, you can register using your work email address without providing an organization code.
- If the BlackBerry AtHoc mobile app is pushed by UEM/MDM and you belong to the same organization configured in the UEM/MDM, then you only have to verify your email address when registering for the first time and are directed to the home screen. In this case, you do not have to enter the organization code. You must enter the organization code if you switch organizations after registering for the first time. You may have to enter the organization code when registering for the first time if the organization you belong to is not configured in UEM/MDM, or there is no organization code configured in UEM/MDM.

1. Tap the BlackBerry AtHoc app icon on your device.
2. Tap **Continue**.
3. On the **Register for Alerts** screen, if it is not displayed, enter the email address that is associated with your BlackBerry AtHoc user profile. If you do not already have a BlackBerry AtHoc user profile, one will be created for you automatically.
4. Tap **Send** or ➤. A verification page with a confirmation message is displayed.
5. Check your email for a verification email from BlackBerry AtHoc with a link to activate your account to your registered email address.
6. On the verification email, click **Verify Now**.
7. After the email address is verified, do one of the following:

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

Update your user profile

1. Tap ≡ at the top left corner of the home screen to open the menu.
2. Tap **My Profile**.
3. On the **My Profile** page, tap to update any of the following fields:
   - First Name
   - Last Name
   - Email
   - Work Phone
   - Mobile Phone
   - Text Messaging
   - Preferred Alert Language
4. Tap **Save**.

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

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

Before you begin:

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

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

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

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

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

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

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

Test the V.ALRT personal alert button

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

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

Publish a V.ALRT emergency alert

Before you begin:

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

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

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

Unpair your Bluetooth alert button

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

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

Respond to alerts

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

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

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

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

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

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

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

Alert icons

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

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

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

View alert responses

1. To view the alert response delivery summary, tap **Alert Name**.
2. Do one of the following:

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

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

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

   When authentication is successful, the following statuses are displayed:

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

   - Tap **Call** to call the user.
   - Tap **Message** to send a message to the user.
   - Tap **Email address** to send an email message to the user.

Update the status of an accountability event

This section describes how to respond to accountability events.

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

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

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

Check Accountability Officer availability

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

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

1. Tap on your device.
2. Tap the accountability event.
3. Optionally, if your administrator has enabled smart card authentication, a certificate selection window opens on your device. Tap a valid certificate and then tap **Continue**.
4. Tap **Reply**. The response options are displayed.
5. Tap one of the following options depending on your availability:
   - **I am available to update user status**
   - **I am not available to update user status**
6. If you tap **I am available to update user status**, complete the following steps:
   a. Tap **I am available to update user status**. A pop-up message with options is displayed.
   b. Tap **Manage Users' status** to update the users' status or tap **Close** to close the message window.
   c. When you tap **Manage Users' status**, the Manage Users status screen opens.
   d. From the list of users, tap **Manage** to update the status of the user you want.
   e. From the **Status** list, select a status.
   f. Optionally, in the **Comments** text box, add a comment.
   g. Tap ✓.
7. If you tap **I am not available to update user status**, your status gets updated.

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

Accountability event icons

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

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

Manage organizations

This section describes how you can change the organization you are connected to. You can connect to and receive alerts from one organization at a time.

Add a new organization

An existing user can be registered with one or more organizations. This section describes how an existing user can add a new organization.

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

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

You are now connected to the new organization.

Switch organizations

This sections describes how to switch from the organization you are currently connected to, to another organization you have already registered with.

1. Tap ≡.
2. Tap **Switch Organization**.
3. On the **Switch Organization** screen, tap the organization name you want to switch to. A confirmation message is displayed.
4. Tap **Switch**.

You can see an entry on your home screen with the name of the new organization you are connected to.

Subscribe to organizations

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

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

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

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

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

Disconnect from an organization

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

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

Enable or disable biometric authentication

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

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

Before you begin:

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

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

Advanced features

This section describes the advance features a user can use on the mobile app. The advanced features that you can see on your mobile app depends on the distribution list selected by the BlackBerry AtHoc administrator. Each feature in the Advanced Features section on the Mobile App settings page includes its own menu to select a distribution list.

Publish an alert

Alerts are communications sent to your organization, to mobile users, or to outside organizations. A user with BlackBerry AtHoc operator permissions can publish alerts using predefined alert templates. If the management system operator selects the "Available for mobile publishing" check box in the alert template, then that alert template appears in the alert publisher template list in the mobile app. Alert templates define the types of alerts that can occur within an alert folder, enabling operators to quickly publish the appropriate alert during an emergency.

Note: You must have alert publishing permissions.

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

   Tip: You can also press and hold the BlackBerry AtHoc mobile app icon to open the alert template screen.
3. Do one of the following:
   - If smart card authentication is enabled, a certificate selection window opens on your device. Tap a valid certificate and then tap **Continue**.
   - If smart card authentication is not enabled, click **OK** on the **Enable biometric authentication** window. The Face ID or Touch ID screen opens. Touch the fingerprint sensor or use Face ID to authenticate.

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

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

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

Edit the alert template

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

   a. From the **Severity** list, select a severity.
   b. From the **Type** list, select a type.
   c. In the **Title** field, enter a name.
   d. In the **Body** field, enter the content of the alert.

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

2. In the **Response Option** section, tap ✏ and do the following:
    a. Tap **Add Response Option** to add response options.
    b. Tap ✕ to remove a response option.
    c. Tap ✓ to save the changes.

    The Response Options section displays the response options.
3. In the **Target Users** section, tap ✏ and do the following:
    a. Tap the distribution list you want to edit. The following options are displayed:
        - **Targeted**: All users in that distribution list are selected.
        - **None**: No user is selected.
        - **Blocked**: All users in that distribution list are blocked.

    b. Tap an option.
    c. Tap ✓ to save the changes.
4. In the **Personal Devices** section, tap ✏ and do the following:
    a. Tap the device you want to target.
    b. Tap ✓ to save the changes.

Send an emergency

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

Note: Ensure that your device location services are enabled.

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

1. Open the BlackBerry AtHoc mobile app on your device.
2. On the home screen, slide the ❗ to the left to create an emergency.
3. A dialog appears with a countdown of 5 seconds with the options **Cancel** and **Send Now**. Choosing **Cancel** cancels the report. **Send Now** sends a duress message immediately. If the countdown reaches zero without you choosing either option, the emergency is reported and your location is sent. A screen is displayed where you can enter messages.
4. Optionally, tap ☎ to make a call, add a message with additional information, or tap 📷 to attach a video or photo.

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

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

Send an emergency using the Top key on Samsung Knox devices

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

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

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

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

Send a report

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

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

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

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

Tracking

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

Note: Ensure that your device location services are enabled.

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

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

Scheduled location access

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

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

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

Check In/Check Out

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

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

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

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

Prerequisites

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

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

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

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

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

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

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

Collaboration

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

When you upgrade your BlackBerry AtHoc mobile app, or install a new version of the app on Android or iOS smartphones, you are automatically enrolled for Collaboration, if your organization has configured the feature. When you tap ☰ > **Collaborate** in the menu, the list of collaborations that you are a part of displays in descending order of the creation date. Collaborations that have unread messages are displayed on the top of the list.

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

View collaborations

To view a collaboration, do one of the following:

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

Working with collaborations

1. Tap 👥 on the bottom right corner of home screen. The list of collaboration messages displays.
2. To participate in a collaboration, tap on the group icon you wish to participate in, type your message in the message box, and tap ➤ .
3. In a collaboration you can perform the following actions:
   - **Quote**: Respond to specific messages.
   - **Edit**: Edit your sent messages.
   - **Retract**: Retract a sent message. When you retract a message, the app displays a message to other users that the message was retracted.
   - **Delete**: Delete a specific sent message.
4. To add an attachment to a collaboration, click 🗋, and browse to the file that you want to attach.
5. To send a high priority message, click (!).

View the delivery status of messages

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

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

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

Log out of the mobile app

Before you begin:

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

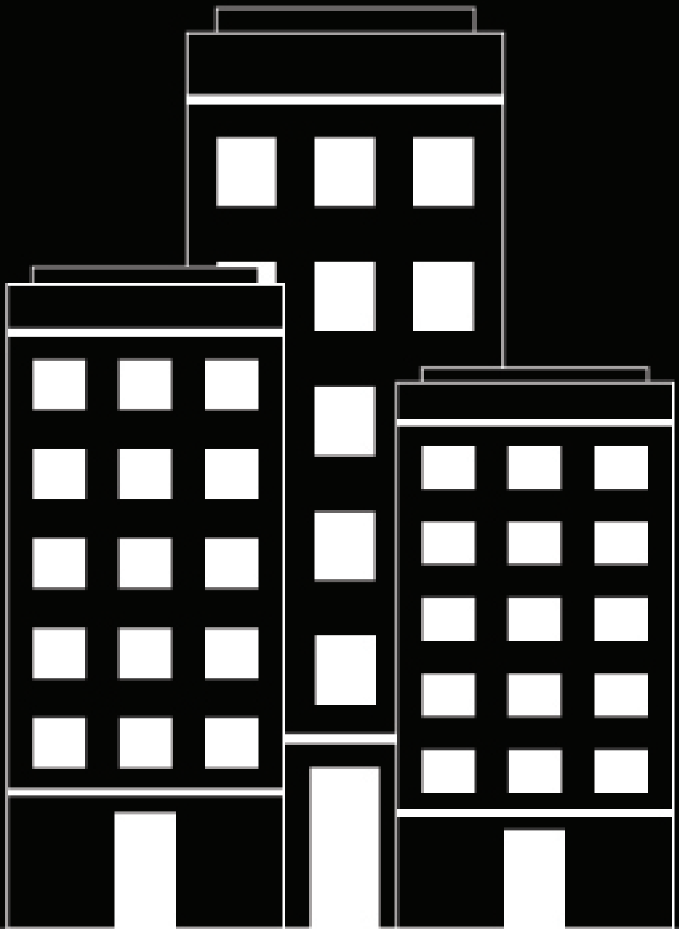
1. Tap ≡ > **Logout**.
2. Tap **OK**.

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

Smart card authentication error codes

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

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



BlackBerry AtHoc

Desktop App User Guide

7.3 (Windows), 2.4.1 (Mac)

Contents

BlackBerry AtHoc Desktop App

The BlackBerry® AtHoc® desktop app is a small desktop application that continuously runs on your computer. When a new alert targeted at user desktops is published in the BlackBerry AtHoc system, a notification screen pops up on your desktop, accompanied by an audio notification.

You can then close the pop-up or click a link to obtain additional information about the alert. For emergency alerts, the pop-up screen might contain response options that you must select from in order to acknowledge receipt of the alert.

Note: BlackBerry AtHoc desktop app release 7.1 or later is compatible with BlackBerry AtHoc release 7.9 (OnPrem) and 7.14 or later release.

Install the desktop app

Note: Installing and setting up the desktop app is relevant only to the Administrator or other authorized users of the BlackBerry AtHoc system. If you are a regular user, the app should already be installed on your computer. For detailed information about how to install and configure the BlackBerry AtHoc desktop app, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

The BlackBerry AtHoc management system provides authorized users with the ability to quickly notify large numbers of people in widely dispersed locations during emergencies and other critical situations. BlackBerry AtHoc also helps those users monitor alerts for threat conditions while also providing basic notifications services for non-emergency situations.

In order to join a notification system, every desktop must have the desktop app installed so that personnel are able to receive and respond to alert messages.

In most setups, your IT group pushes the app to user desktops during off hours using an SMS package that includes the app MSI, the SMS script, and a run.bat file. Depending on the input parameters set by your IT group, the app usually runs immediately after the install or at the next start up. The MSI can also be run manually, if your IT group prefers to do it that way.

In some setups, your IT group may require you to register with a validation code before you can use the desktop app. If your system is configured for manual desktop app registration, see Register the desktop app (Windows only).

Register the desktop app (Windows only)

When the desktop app is installed on your system, if your organization is configured to use the Defer to Self Service authentication method, the BlackBerry AtHoc Desktop App Registration form opens.

This section applies only to the Windows version of the BlackBerry AtHoc desktop app.

1. Click the link on the BlackBerry AtHoc Desktop App Registration form. You are redirected to Self Service.
2. Log in to Self Service:
    - If you have a Self Service account, log in to Self Service using your organization's authentication method (for example, user a smart card or enter your username and password.)
    - If you do not have a Self Service account, the Registration form opens. Complete all required fields and click **Continue**. For detailed instructions, see Register for Self Service in the *BlackBerry AtHoc Self Service User Guide*.
3. On the **My Profile** page, in the **BlackBerry AtHoc Apps** section, click **Generate Code**.

4. On the **Desktop App Registration Code** pop-up window, copy the registration code. The code is valid for 5 minutes.
5. Paste the registration code in the BlackBerry AtHoc Desktop App Registration form.
6. Click **Submit**.

After the registration is successful, it may take up to 2 minutes for the desktop app to connect.

Sign in to the desktop app

If your BlackBerry AtHoc administrator has configured automatic sign in, you do not have to sign in to the desktop app.

If you receive a Sign In pop-up screen, follow the prompts to sign in. The desktop app remains disconnected until you sign in. If you close the Sign In pop-up screen without signing in, you can click the 🌐 (Globe) icon and click **Sign In**.

The Sign In pop-up screen appears each time your start up your computer.

Launch the desktop app menu

You can access the BlackBerry AtHoc desktop app at any time by clicking the 🌐 (Globe) icon that appears on your screen. On Windows platforms, the icon is located in the bottom right corner of the screen. For the Macintosh platform, the icon appears in the top right menu bar.

As soon as you click 🌐, a pop-up menu appears, allowing you to check for new alerts, dismiss all pop-ups that are currently on your desktop, and access the Self Service application.

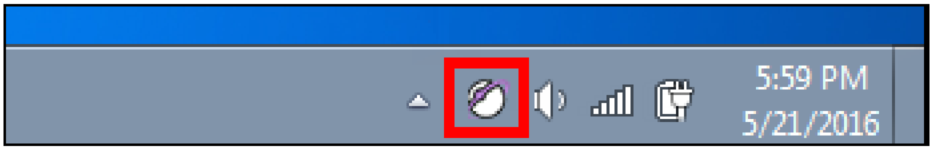
When multiple desktop app editions are running on the same computer, you must close the browser window for one edition before you can launch a browser window with a different desktop app edition.

Manage desktop alerts

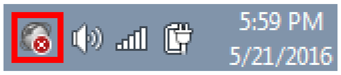
Important: All actions and operations carried out within the BlackBerry AtHoc desktop app are common to both Macintosh and Windows platforms.

Check your ability to receive alerts

After the desktop app launches successfully, the appears on your screen, indicating that you are connected to the BlackBerry AtHoc server and are ready to receive alerts.



If the desktop app has been installed but it is disconnected from the BlackBerry AtHoc server, the icon is grayed-out with a red circle with a white "x".



When the desktop app is disconnected, the app cannot receive alerts.

Windows: If your account has been disabled, the icon appears in gray with a yellow circle () and you cannot receive alerts.

Manually check for new alerts

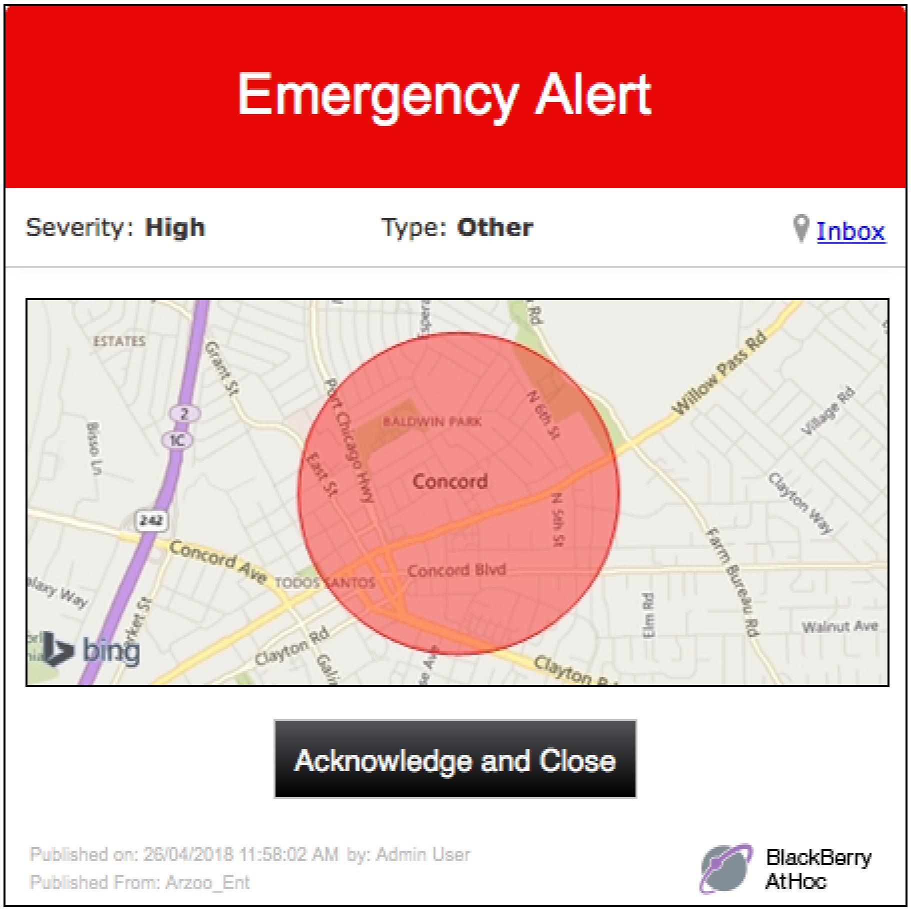
The BlackBerry AtHoc desktop app automatically checks for new alerts at an interval that is configured when the app is set up. The default interval is every 120 seconds. It is possible, however, to check for new alerts manually at any time by completing the following steps:

1. Right-click the (Globe) icon.
2. In the menu that appears, select the **Check for New Alerts** option.

The desktop app then polls the BlackBerry AtHoc server asking for new alerts or updates. If there are new alerts, each will appear as a separate pop-up on your desktop.

Respond to alerts

Desktop alerts display as popup windows. After reading the alert, click the **Acknowledge and Close** button. Click **Acknowledge and Close** to send a response to the BlackBerry AtHoc system, which tracks, compiles, and reports all recipient responses.



Emergency Alert

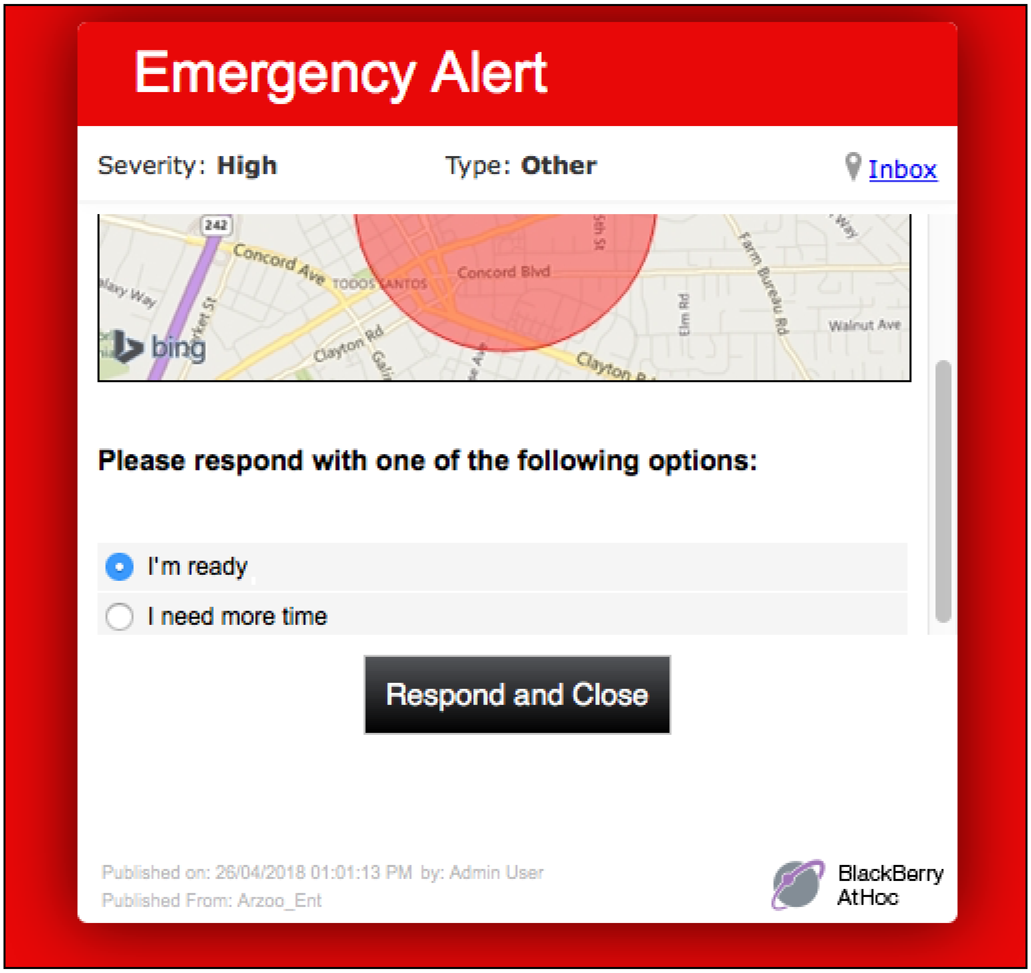
Severity: **High** Type: **Other** Inbox

Published on: 26/04/2018 11:58:02 AM by: Admin User
Published From: Arzoo_Ent

You can also click the **Inbox** link to go to Self Service to view and respond to the alert.

If the alert includes response options, select an option and then click **Respond and Close**.

If the alert includes a map, clicking on the map takes you to an interactive map in the alert in Self Service.



Emergency Alert

Severity: High Type: Other Inbox

Please respond with one of the following options:

● I'm ready

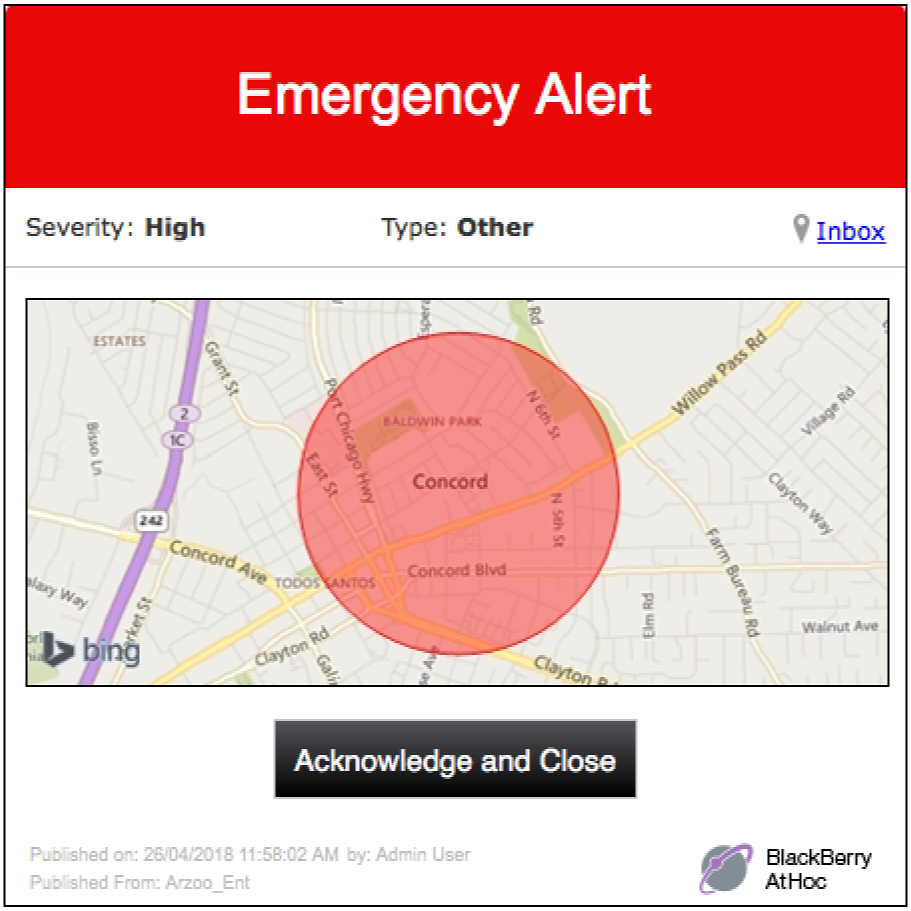
○ I need more time

Published on: 26/04/2018 01:01:13 PM by: Admin User
Published From: Arzoo_Ent

Close alerts

Desktop alerts display as popup windows. After reading the alert, click the **Close** button (for informational alerts) or the **Acknowledge and Close** button (for emergency alerts).

In the following example, clicking the Acknowledge and Close button sends a response to the BlackBerry AtHoc system, which tracks, compiles, and reports all recipient responses.



Emergency Alert

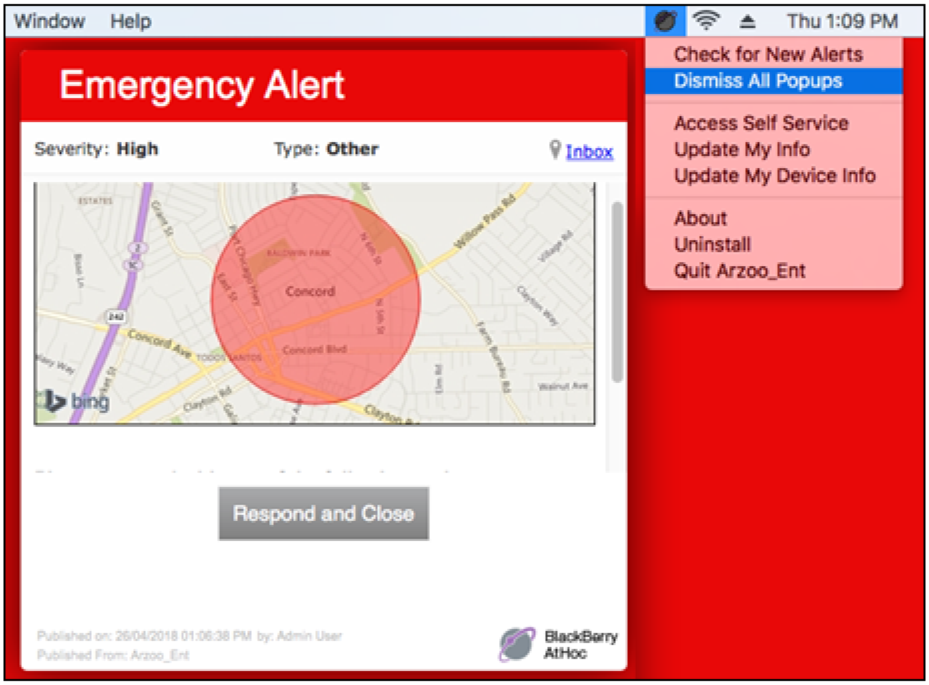
Severity: **High** Type: **Other**

Published on: 26/04/2018 11:58:02 AM by: Admin User
Published From: Arzoo_Ent

Close full screen pop-ups

When you receive a full screen pop-up, you can close it in any of the following ways:

- Respond to the alert by selecting a response option, then click **Respond and Close**.
- If your BlackBerry AtHoc administrator has enabled this capability, right-click the pop-up to close it.
- Right-click the (Globe) icon, then select **Dismiss All Popups** in the menu that appears. The following image shows how this would be done in a Mac environment:



Severity: **High** Type: **Other**

Published on: 26/04/2018 01:06:38 PM by: Admin User
Published From: Arzoo_Ent

Close multiple pop-ups

It is possible to close multiple pop-ups at once by completing the following steps:

1. Right-click .
2. In the menu that appears, click **Dismiss All Popups**.

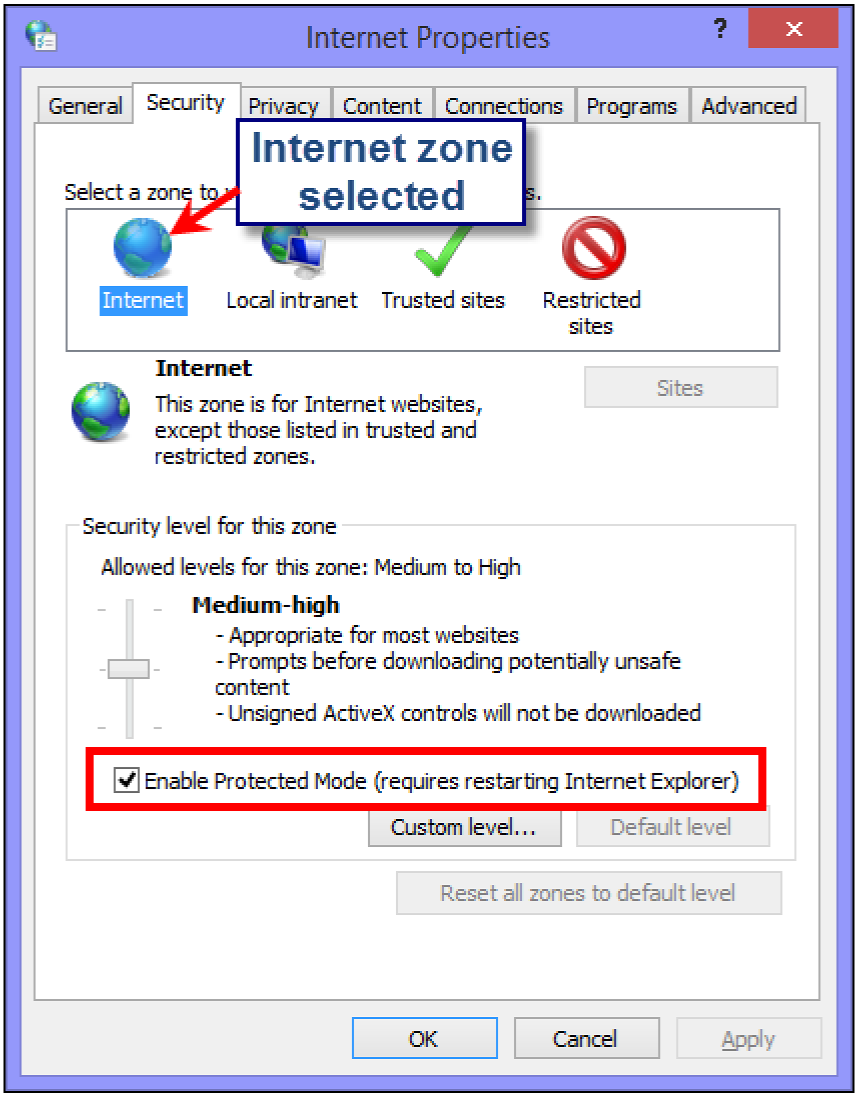
Troubleshoot desktop client issues

This section describes issues you might encounter after installing the BlackBerry AtHoc client on users' desktops. In most cases, the solutions provided in this chapter will resolve these problems. If they do not, contact BlackBerry AtHoc customer support.

Workaround for the Self Service validation error

If you are using Internet Explorer (IE) 10 or newer with Windows 7 or newer, you might receive a validation error when you try to view the Self Service screen. To fix this error, complete the following steps:

1. Go to **Control Panel** > **Internet Options** and click the **Security** tab.
2. With the Internet zone options displayed, select the **Enable Protected Mode** checkbox.



Internet zone selected

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

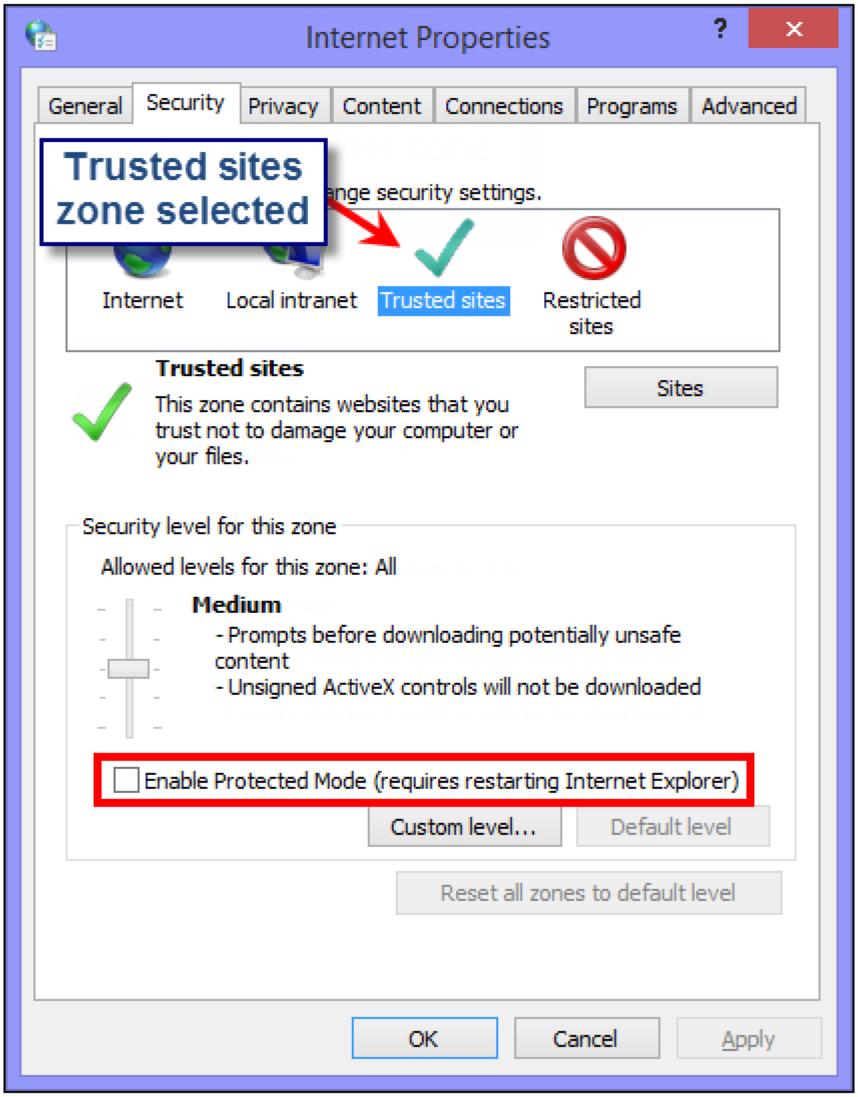
Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

3. Click the **Trusted sites** icon.
4. With the Trusted sites zone options displayed, deselect the **Enable Protected Mode** checkbox if it is selected.



nge security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☐ Enable Protected Mode (requires restarting Internet Explorer)

5. Click **Sites**.
6. On the Trusted sites screen that appears, enter the BlackBerry AtHoc website address in the **Add this website to the zone** field.
7. Click **Close**.
8. If the Self Service screen is blocked by Active X—indicated by a yellow bar at the top of the screen requesting permission to display images—click **Yes** to unblock it and allow Active X to display the Self Service screen.

Access desktop app details

Before contacting BlackBerry AtHoc customer support for help with problems you are having with the BlackBerry AtHoc desktop app, you should open the application details screens for the particular version of the application that you are running. The information contained on these screens will be useful for the Support team as they work to diagnose and fix the problem you are encountering.

The application details screens can be accessed by right-clicking and selecting **About** from the menu that appears.

The **System Information** tab allows you to see if the app is currently connected to a BlackBerry AtHoc server and the server URL. The **Connection Status** field displays Connected if you have a connection and the **Server Base URL** field displays the URL of the server to which you are connected.

The **Connection Settings** tab, which appears only on Windows platforms, provides options for automatic configuration and use of a proxy server. Because these settings are not used for most installations, it is unlikely you will need to review this information.

The **About** tab displays the version of the desktop app that is installed on your machine. If the Support team requests that you send them your system details, you can export that information by clicking the **Export System Information** button on the screen. You can also open your log file or copy and mail your log file path by clicking the corresponding button on the screen.

Incorrect or missing software on your computer

In order for the BlackBerry AtHoc desktop app to work correctly, the following software must be installed on your computer:

- **BlackBerry AtHoc release**: Desktop app release 7.0 or later is compatible only with BlackBerry AtHoc release 7.14 or later releases.
- **Windows**: The desktop app software supports Windows 7 (32-bit and 64-bit) and above.
- **Supported browsers**:
    - **Internet Explorer**: The 7.0 desktop app supports Internet Explorer versions 10 and above.
    - **Safari**: The Macintosh client supports Safari versions 6.x and above.
    - **Microsoft Edge**
    - **Firefox**
    - **Chrome**
- **Macintosh**: The desktop app software supports Mac OS X 10.8 Mountain Lion and above.
- **Installation files**: BlackBerry AtHoc provides the installation files required for the app.

Desktop app does not connect

The 🌐 (Globe - connected) icon displays when it is connected to the BlackBerry AtHoc server.

The 🌐 (Globe - disconnected) icon displays when the desktop app is disconnected.

Windows: The 🌐 (Globe - disabled) icon displays when the user account is disabled in the BlackBerry AtHoc system.

The app might not connect to the BlackBerry AtHoc server due to the network configuration. To resolve the problem, do the following:

- Ensure the app workstation is connected to the network.
- Verify that proxy and firewall settings are not blocking access in your browser and the Connection Settings for the app.

To verify that your app is connected to the correct server, complete the following steps:

1. Click 🌐.
2. In the menu that appears, click **About**.
3. On the **About** screen, click the **System Information** tab if it is not already open.

The **Connection Status** should be Connected and the **Server Base URL** should point to the BlackBerry AtHoc server. If the base URL is wrong, the usual fix is to uninstall the app and then install it, inputting the correct set of input parameters, which includes the base URL for the server.

Validation error message (Macintosh only)

If your account has been disabled, the following error message appears when you click the Desktop App icon and select **Access Self Service** from the drop-down menu that appears: `Error: Error encountered retrieving User Attributes Info.`

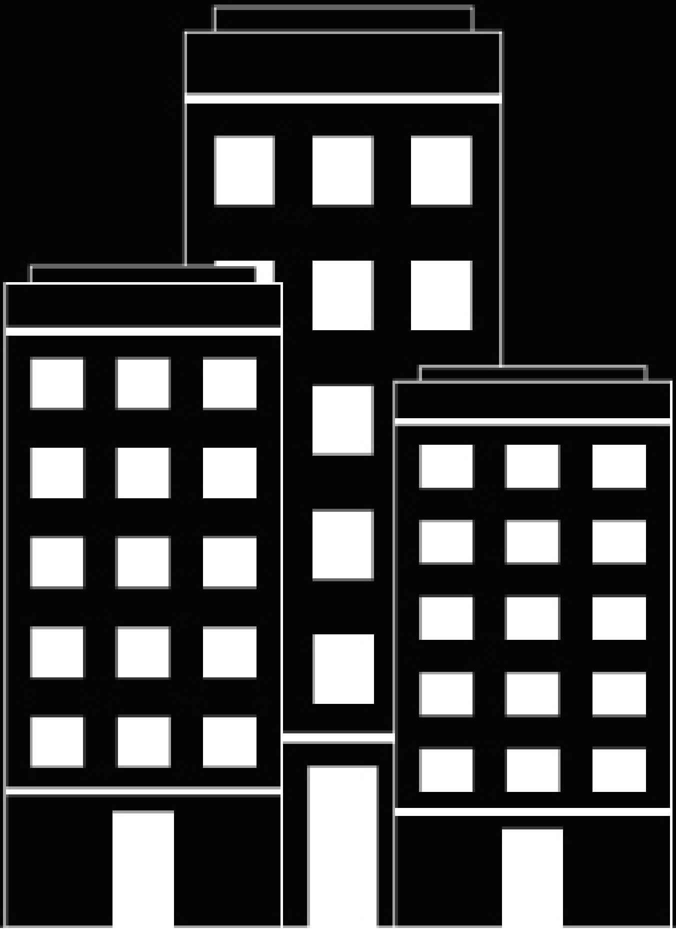
To correct this problem, contact your BlackBerry AtHoc administrator and have them re-enable your user account.

Desktop app is not receiving alerts

If you do not receive any alerts after installing the desktop app, check the following:

- Was your User ID targeted? To find out if it was, contact the Operator who created the alert and ask them to confirm that your User ID was part of the target group. You can find your User ID by clicking and selecting **About** from the menu that appears. Your User ID is listed at the top of the Value column on the System Information tab.
- Is your BlackBerry AtHoc desktop app connected to a server? Is it the correct server?
- Was your account enabled in the BlackBerry AtHoc system? If the desktop app icon appears in gray with a yellow circle (), your account is not enabled.

To view the server settings, follow the steps in Desktop app does not connect.



BlackBerry AtHoc

Operator Quick Start

7.16

Contents

Getting started

This guide provides basic information for operators to get started using the BlackBerry® AtHoc® management system.

For detailed information about creating and publishing alerts, see *BlackBerry AtHoc Create and Publish Alerts*.

For detailed information about operator roles and permissions, see the *BlackBerry AtHoc Operators Roles and Permissions* document or the *BlackBerry AtHoc Operator Roles and Permissions Matrix*.

For detailed information about creating alert templates, see *BlackBerry AtHoc Alert Templates*.

Quick Action Guides

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

View all Quick Action Guides

Alerts

- Create and publish an AtHoc alert
- Send an alert with fill count
- Send an alert with escalation
- End a sent alert
- View alerts in the Inbox
- Create a weather alert rule

Alert templates

- Create an alert template
- Organize your alert templates

Operators and users

- Manage operator roles and permissions
- Create a user
- Create a static distribution list
- Create a dynamic distribution list

Self Service

- Register for Self Service
- Move to an organization
- Subscribe to organizations
- Prioritize your personal devices
- Add a dependent

Account

- Create a new accountability event

- Generate an accountability report
- Report on behalf of users

Activity log

- Create an activity log entry

Log in and out of BlackBerry AtHoc

There are two general types of users that access the BlackBerry AtHoc management system: operators and administrators. Administrators have system, organization, and user management type roles and operators have publishing-related roles.

Log in

An online user session lasts until the administrator or operator logs out or the session times out. Administrators can configure the timeout interval using the System Policy screen. For more information, see "Set session timeout" in the *BlackBerry AtHoc System Settings and Configuration* guide.

Before logging in to BlackBerry AtHoc, verify that the following are all true:

- The BlackBerry AtHoc server is installed on a server connected to the network and is accessible to you.
- The system has Internet Explorer version 10 or higher, or any version of the following browsers: Microsoft Edge, Firefox, Chrome, or Safari.
- The BlackBerry AtHoc administrator has provided you with the following:
    - The URL (an Internet address) for accessing the BlackBerry AtHoc management system
    - A BlackBerry AtHoc username and password, or a smart card

Note: Log in will not occur on Internet Explorer when the Content Advisor filter in IE is set to specific values.

1. Contact your administrator to get the BlackBerry AtHoc management system address.
2. Open a web browser and navigate to the BlackBerry AtHoc URL.
3. Click **Accept** to agree to the terms of the Security Disclaimer. Note that if you select **Decline**, you cannot use BlackBerry AtHoc.
4. After you accept the security policy, the login screen fields become accessible. Do one of the following:
    - Log in Manually:
        a. Enter your username and password, which are case sensitive.
        b. Click **Log In**.
    - Insert your smart card and click **Access Smart Card**.
5. If a disclaimer screen displays immediately after you click **Log In**, read it, then click **OK**.

The BlackBerry AtHoc management system homepage displays.

Change organization

An organization is the logical grouping of operators and alert recipients. The members of the organization can send and receive alerts. Depending on the type of system you use, you might have access to more than one organization.

If you have access to multiple organizations, you can change between them.

1. In the navigation bar, click your username.
2. Click **Change Organization**.
3. Select an organization and click **OK**.

The homepage for the selected organization opens.

Log out

1. In the navigation bar, click your username.
2. Click **Log Out**.
3. Click **OK**.

Reset your forgotten password

Note: The information in the following topic is relevant only if you log in to Self Service manually using a username and password.

1. On the login screen, click **Forgot Password?** under the **Password** field.
2. On the **Reset Password** screen, from the **Select Verification Method** list, select **Email** or **Text Message**.
3. Enter the email address or text-messaging number associated with your BlackBerry AtHoc account.
4. If your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
5. Click **Submit**. If your email address or text-messaging number is found in the BlackBerry AtHoc system, a message is displayed instructing you to check your email or text for instructions. If your email or text-messaging number is not found in the BlackBerry AtHoc system, a message is displayed.
6. Open the email or text message, then click the **Create/reset your password here** link embedded in the body of the message.
7. On the **Create/Reset Password** screen, enter your username.
8. Click **Next**.
9. On the **Create/Reset Password** screen, enter and re-enter your new password.
10. Click **Next**. If your password meets the length and complexity requirements set by your administrator, a confirmation screen appears.
11. Click **Go to Login** to log in.

Recover your forgotten username

Note: The information in the following topic is relevant only if you log in to Self Service manually using a username and password.

1. On the **login** screen, click **Forgot Username?** under the **Username** field.
2. On the **Retrieve Username** screen, from the **Select Verification Method** list, select **Email** or **Text Message**.
3. Enter the email or text-messaging number associated with your BlackBerry AtHoc account.
4. If your system has reCAPTCHA enabled for user verification, select the **I'm not a robot** check box.
5. Click **Submit**. If your email address or text-messaging number is found in the BlackBerry AtHoc system, a message is displayed instructing you to check for your username in your email or text. If your email or text-messaging number is not found in the BlackBerry AtHoc system, a message is displayed.
6. Log in to Self Service using the username that appears in the email or text message.

Change your login password

1. In the navigation bar, click your username.
2. Click **My Profile**. Your user details page opens.
3. In the **Password** section, click **Edit**.
4. On the **Password** screen, enter your current password.
5. Enter your new password.
6. Re-enter your new password to confirm it.

   Note: Any password rules that your organization has created will appear on the screen under the Confirm New Password field. If you do not follow the rules, an error message will appear and your password will not be accepted.
7. Click **Update**.

Subscribe to organizations

If your administrator has configured the ability for users to subscribe to different suborganizations and has configured organizations for subscription, you can subscribe users to those organizations from the BlackBerry AtHoc management system or by using the .csv user import process.

You can also subscribe to any suborganization that has been configured for subscription from the My Profile screen in Self Service. For more information, see the *BlackBerry AtHoc Self Service User Guide*.

To subscribe multiple users to organizations using the .csv user import process, see "Manage organization subscriptions" in the *BlackBerry AtHoc Manage Users* guide.

When you subscribe users to other organizations, they can be targeted in alerts and accountability events from both their home and subscribed organizations. You can subscribe a user to a maximum of 10 organizations.

Dependent users cannot be subscribed to organizations. If you subscribe a user to an organization, their dependents remain in their home organization and are still targetable in alerts and events from the home organization. They cannot be targeted from any subscribed organizations.

You can cancel organization subscriptions at any time from the Organization Subscriptions section of the user profile screen.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select a user from the list.
4. On the user profile screen, click **Edit User**.
5. On the user profile screen, in the **Organization Subscriptions** section, click **Add Subscription**.
6. On the **Subscribe Organization** screen, select an organization from the list.
7. Click **Apply**.
8. In the **Organization Subscriptions** section, enter a date or click 📅 to select a start date for the subscription.
9. Optionally, in the **Organization Subscriptions** section, click 📅 next to the subscribed organization to set an end date for the subscription.
10. Optionally, in the **Basic Info** section, enter an address in the **Temporary work location** field.
11. Click **Save**.

BlackBerry AtHoc homepage components

The buttons and links that appear on the BlackBerry AtHoc homepage vary depending on the role you have been assigned in the system, so some of the components discussed below may not be visible.

The BlackBerry AtHoc system does not support use of the Web browser **Back** button. Clicking the **Back** button can produce unexpected results so it should not be used. Use the navigation bar or buttons on the screen to navigate from screen to screen within the application.

The BlackBerry AtHoc homepage is divided into two main sections: the Main area fields and the Sidebar fields.

Quick Action Guides

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

View all Quick Action Guides

Alerts

- Create and publish an AtHoc alert
- Send an alert with fill count
- Send an alert with escalation
- End a sent alert
- View alerts in the Inbox
- Create a weather alert rule

Alert templates

- Create an alert template
- Organize your alert templates

Operators and users

- Manage operator roles and permissions
- Create a user
- Create a static distribution list
- Create a dynamic distribution list

Self Service

- Register for Self Service
- Move to an organization
- Subscribe to organizations
- Prioritize your personal devices
- Add a dependent

Account

- Create a new accountability event
- Generate an accountability report

- Report on behalf of users

Activity log

- Create an activity log entry

Main area fields

The following fields appear in the main area of the homepage and may vary depending on your permissions in the BlackBerry AtHoc system.

Branding area: Displays the logo of the company or organization of the user and any customized welcome message that has been created by the company or organization.

Live alerts: Displays a summary of all live alerts in the system, including the following information:

- The title of the alert
- The time the alert was published
- The time remaining in the alert. Note that this information is visible only in the tooltip field that appears when you hover your cursor over an alert title.
- The number of users targeted by the alert
- The number of users the alert was sent to
- The number of users who responded to the alert

Note: To view complete details about any of the alerts in the list, click the alert name in the Alert Title column. To view a list of scheduled alerts, click the corresponding link at the top of the section.

Quick publish: Displays all alert templates that have the "Available for quick publish" option enabled on the alert template details screen. Note that a template can appear in this Quick Publish field even if its details are incomplete.

- If the alert template details are complete, a **Publish...** button appears beside its name in the **Ready to Publish** column. Click this button to go to the **Review and Publish** screen.
- If the alert template details are not complete or if you want to make edits to it before publishing, click **Edit** to go to the **Edit & Publish** screen.
- If the alert template you want to access is not listed, click **All Alert Templates >>** to go to the **Select from Alert Templates** screen.
- To create a new alert, click **Create a Blank Alert**.

Live accountability events: Displays all live accountability events in the system. The following information is provided for each event: event name, start time, number of affected users, number of affected users who have provided a status. Click **All Events >>** to view a list of ended accountability events.

Recently received alerts: Displays all live inbound alerts that have been recorded for the company or organization. The title, time, source, and type is displayed for each alert. Titles of alerts that have not yet been reviewed appear in bold font. Titles of reviewed alerts appear in plain font. All live alerts that appear in this section also appear on the map. When there are no recently received alerts, the map displays the default map view configured for your organization. Click **Inbox** to view incoming events in the Inbox.

Sidebar fields

The following fields appear in the sidebar and vary depending on your permissions in the BlackBerry AtHoc system.

Updated: Refreshes all data on the screen.

View Live Map: Provides a map that displays active alerts and events.

Quick Links: Provides links to screens in the BlackBerry AtHoc application that users frequently need to access, including *Publish Alert*, *Start Accountability Event*, *Manage Users*, *Connect to Organizations*, and *Request Support*.

System status:

- If no errors have been reported, displays a green circle and the message, "System is Healthy."
- If warnings have been reported, the field displays a yellow circle and the message, "System is Unhealthy" with a **More** link. Click the link to view information about the warnings.
- If errors have been reported, the field displays a red circle and the message, "System is Unhealthy" with a **More** link. Click the link to view information about the errors.

Note: If warnings and errors occur at the same time, the red icon displays and the errors appear first in the list when the **More** link is clicked.

Situation response: Displays any Plans that are waiting for your review or approval. Click the link to go to the Plan Manager, filtered to display only the Plans that require your review or approval.

Organizations and users: Displays the total number of organizations and enabled users. This section displays how many of the total users are currently online with a desktop or mobile device and how many users do not have an active device. If you have been invited to join an organization, a **View** link appears below the Organizations title, taking you to a screen where you can respond. If dependents are enabled for your organization, the number of dependents is displayed.

Login and password information: Displays the date and time you last logged in and the date and time you last changed your password. The **Last Login** field also lists the number of failed attempts and provides a link to the **My Profile** screen where you can change your password if necessary.

View your account details

When you are logged in to an organization, you can view detailed information about your account such as your login information, contact information, memberships, and subscriptions.

1. In the navigation bar, click your username.
2. Click **My Profile**.

   Your user details screen opens, displaying all of your profile information divided into the following sections:

   - **Basic Information**: Username, first name, last name, display name, creation date, organizational hierarchy, temporary work location, and user ID
   - **Numbers:** Home and mobile numbers
   - **Online Addresses**: Personal email, work email, and text messaging number
   - **Physical Addresses**: Home and work addresses
   - **Subscriptions**: Any distribution list
   - **Password**: Displays black dots to represent your password in the system and the date your password was last changed. Click the **Edit** link to change your password.

     Note: This is the only field on the screen that is editable by all operators.
   - **Organization Subscriptions**: This section appears only if organization subscriptions are enabled for your organization and if your administrator has configured organizations for subscription. This section displays your organization subscriptions, the start and end date, and the assigner for each subscription.
   - **BlackBerry AtHoc Apps**: This section shows whether any desktop or mobile apps are connected using your account.

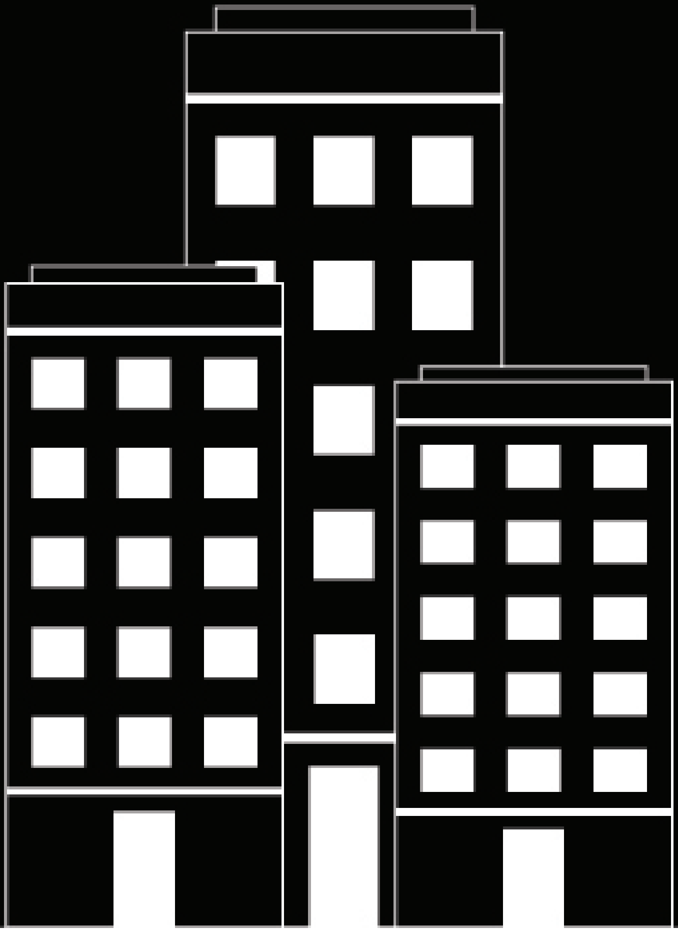
     - Desktop App:

       - Active: The desktop client for this user is currently connected.
       - Inactive: The desktop client has not been seen for at least 30 days.
       - Not Available: No desktop client for this user has ever been connected.
     - Mobile App:

       - If any mobile clients are connected, the number of users logged in with your ID for each mobile client is displayed.
       - Not Available: No mobile clients are logged in.

       Tip: Click **Active** (*x*) beside **Mobile App** to delete an unused mobile device. On the **User Mobile Devices** window, click ✖ beside the mobile device you want to delete.
   - **Permissions**: Displays your login history and the roles you have been granted in BlackBerry AtHoc. This field also displays the permissions you have been given for each of the following items:

     - Folder management and publishing
     - Distribution list management and publishing
     - User base access
     - Dependents management and publishing
   - **Advanced Information**: Any user attributes defined by your system administrator



BlackBerry AtHoc

Create and Publish Alerts

7.16

Contents

Create and publish alerts

Alerts are communications sent to your organization, to mobile users, or to outside organizations. A BlackBerry® AtHoc® operator creates alerts and targets users, distribution lists, mobile users, and organizations through IPAWS or AtHoc Connect. Operators publish alerts from the alerts menu in the BlackBerry AtHoc management system or from the mobile app.

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

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

View all Quick Action Guides

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

Publish an alert from an existing alert template

Important: Before you create and publish a new alert, go to the BlackBerry AtHoc home page and check the list of all alerts that are currently live, scheduled, and recurring in the system. This will help you avoid creating a duplicate alert.

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

Publish a blank alert

Important: Before you create and publish a new alert, go to the BlackBerry AtHoc home page and check the list of all alerts that are currently live, scheduled, and recurring in the system. This will help you avoid creating a duplicate alert.

If you have operator permissions, you can create a new alert without any predefined content or targeted users.

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

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

Publish a geofence alert

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

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

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

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

Limitations

- If you enable fill count, geofence targeting is disabled and cannot be enabled.
- If you enable geofence targeting, fill count is disabled and cannot be enabled.
- Operator and distribution list user base restrictions apply for alerts that use geofence targeting. If a user enters the defined alert perimeter, and that user is outside the operator's user base, that user is not targeted.

For more information, see Enable geofence targeting.

Preview and publish an alert

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

1. On the **Review and Publish** screen, click **Preview and Publish**.
2. On the preview screen, in the **Original Content** section, review the title, body, response options, location, more info links, attachments, and targeted users, groups, and organizations in the original alert template content.
3. In the **Device Summary** section, review the selected devices. This section displays the percentage of targeted users that are reachable by each selected device. This section also displays any selected device delivery preferences and mass devices.
4. If Email is a targeted device, in the **Email Preview** section, review and edit how the email alert will appear to end users.

    - Optionally, select the **Include Map** option to include the selected location as a map in the alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map. This option is available only when a location is selected in the Content section.
    - Optionally, select a custom delivery template from the **Custom Template** pull-down menu. BlackBerry AtHoc provides default templates for each alert severity: High, Moderate, Low, Informational, and Unknown. By default, the custom delivery template associated with the selected alert severity is used.

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

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

Search for an alert

The alert search engine matches any set of letters or numbers anywhere in an alert title, folder name, or publisher name and is not case-sensitive.

Wildcards are not supported in searches.

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

Filter the alert list

You can filter the alert list by any combination of the following attributes: title, status, folder, start time, and publisher.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Click **Advanced** to open the advanced filtering options.
3. Optionally, in the **Severity** drop-down list, select the severity you want to use as a filter: **High**, **Moderate**, **Low**, **Informational**, or **Unknown**.
4. Optionally, in the **Type** drop-down list, select the type of alert you want to use as a filter. The options displayed in the list are configurable and vary depending on the setup of your organization.
5. Optionally, in the **Status** drop-down list, select the status you want to use as a filter. The following options appear in the list: **Select All**, **Ended**, **Draft**, **Scheduled**, **Live**. You can select multiple status values.
6. Optionally, in the **Publisher** drop-down list, select the name of the alert publisher you want to use as a filter.
7. Optionally, in the **Folder** drop-down list, select the name of a folder to limit the search to only alerts within that folder.
8. Optionally, in the **Start Date** and **to** fields, select the beginning and end dates of the date range that you want to use as a filter. The alert list then displays only those alerts that have a start date that falls within the range you specified.
9. Click **Search**. The alert list displays all alerts that match the filter criteria.

Remove filters from the alert list

After you have filtered the alert list, you can do any of the following to filters:

- To remove all filters and return to the default alert list, click **Clear all** below the **Search** button.
- To remove a **Severity** filter, select the **Select All** option in the **Severity** drop-down list then deselect it to remove all selected options.
- To remove a **Type** filter, select the **Select All** option in the **Type** drop-down list then deselect it to remove all selected options.
- To remove a **Status** filter, select the **Select All** option in the **Status** drop-down list then deselect it to remove all selected options.
- To remove a **Publisher** filter, select the **Any Publisher** option in the **Publisher** drop-down list then deselect it to remove all selected options.
- To remove a **Folder** filter, select the **All Folders** option in the **Folder** drop-down list then deselect it to remove all selected options.
- To remove a **Date** filter, highlight the date in the field, then press **Delete**.

Sort the alert list

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

View a quick summary of an alert

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

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

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, use the search field or scroll down to locate the alert that you want to view. You can also click a column header to sort the sent alerts list.
3. Hover your cursor over the title of the alert. A tooltip is displayed, providing the following information:
   - **Alert Title**
   - **Alert ID**
   - **Body**
   - **Severity**
   - **Type**
   - **Time Left**: This field appears only if the alert has a Live status.
   - **Response Options**: If the alert has a Scheduled or Draft status, the response options appear by themselves. If the status is either Live or Ended, each response option is followed by a number that indicates how many respondents have chosen that option.
4. Click anywhere in an alert line to open the **Users** screen for the alert. The Users screen provides information about the targeted users and response details for the alert. The **Sent Details** section displays the number of targeted users. The **Response Details** section displays the number of users with each status. If dependents are enabled for your organization and in the alert template, the number of users displayed in the tool tip includes the number of sponsors and dependents.
5. Click the **Details** tab to view details of the content of the alert, including response options, severity, type, location, alert time and targeted users.

   If attachments are included in the alert, they are displayed. Click the attachment to open a preview window. In the preview window, click **Download** to download the attachment.

   The details screen is identical for both Live and Ended alerts except that the **Scheduled** section of a Live alert is editable, allowing you to change the end time.

   - If the alert has a status of **Draft** or **Scheduled**, you can edit the details of the alert.
   - If the alert has a status of **Live**, you can end the alert. You can edit the end time of the alert if there are five or more minutes remaining before the alert end time.
   - If the alert has a status of **Ended**, you cannot edit it.

View the details of a sent alert

After you click the **Publish** button to send an alert, you can click the **Alert Summary** button at the bottom of the **Review and Publish** screen.

The Alert Summary screen lists the current status of the alert: Live or Ended. For live alerts, the information on the page updates automatically every minute. Click ⟳ to update the screen manually.

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

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

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

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

Users tab

The Users tab provides statistics on the number of users who were targeted by the alert and the kinds of responses that were recorded from users who received the alert.

The **Sent Details** section contains statistics on the number of users targeted by the alert, the number of users the alert was sent to, and the number of users the system is still trying to contact, or the system failed to contact. For each of these options, a menu next to the number contains the following options:

- **Export Delivery Summary (CSV)**: Click this option to create an exportable .csv file that contains the names of all users belonging to the category you clicked: Targeted, Sent , or In Progress or Failed. Where applicable, the .csv file also contains the alert sent time, responded time, user response, and error time recorded for each user in the list.

  Tip: To view phone error codes, see "Unified telephony tracking codes" in the *BlackBerry AtHoc Alert Tracking* guide.
- **Send alert to these users**: Click this option to open a duplicate of the original alert that you can modify and send out again. For the "In Progress or Failed" category, this option is a quick way of adding more personal devices and delivery methods to the alert to try to contact alert targets who were unaware of or unable to respond to the original alert.
- **User List**: Click this option to open a User Tracking Report. The report opens in a new browser window.

The **Response Details** section of the Users tab displays the possible alert response options, each assigned a different color. The total number of alert recipients who have selected that option is displayed beside each option. This information is also represented in a pie chart. Hover over the pie chart to display a tool tip that shows the number of users in each category. If dependents are enabled for your organization and in the alert template, the number of sponsors and dependents is displayed.

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

- **Export Delivery Summary (CSV)** : Click this option to create an exportable .csv file containing the names of all recipients who chose the corresponding response option. Where applicable, the .csv file also contains the alert sent time, responded time, user response, and work related details for each recipient.
- **Send Alert to These Users**: Click this option to open a duplicate of the original alert that you can modify and send out again. For the "Not Responded" category, this option is a quick way of adding more personal devices

and delivery methods to the alert to try to contact alert targets who were unaware of or unable to respond to the original alert. For other options, it is a way to provide specific additional instructions to a highly targeted group.
- **User List**: Click this option to open a User Tracking Report. The report opens in a new browser window.

Organizations tab

The Organizations tab provides statistics on the number of organizations that were targeted by the alert and the types of responses that were recorded from those organizations.

Each list on the Organizations tab contains an **Export Delivery Summary** option. There is no option to resend the alert to the selected organizations.

Mass Devices tab

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

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

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

Advanced Reports button

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

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

Details tab

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

The Total Users field in the Target Users section displays the total number of users targeted in the alert. Click the number to open a Users screen that displays the names and user details of each of the targeted users. The Target Users section also displays the Fill Count, if enabled, response options, targeted personal devices, and the device delivery preference (System defined, Organization defined, or User preferred.)

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

For live alerts, you can change the alert end time in the Alert Timing section of the Schedule section if there are five or more minutes remaining before the alert end time. Click **Save** to save your changes.

Change the number of alerts listed on the Sent Alerts screen

To make it easier to locate alerts on the Sent Alerts screen, you can change the number of alerts that appear on each page.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Scroll to the bottom of the alert list.
3. Click the list that appears next to the phrase **items per page**.
4. Select the number of alerts you want to display per page.

The screen refreshes and displays the total number of results you specified.

Edit an alert

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

- If the alert has a **Draft** or **Scheduled** status, you can edit any of the details.
- If the alert has a **Live** status, you can edit the end time for the alert if there are five or more minutes remaining before the alert end time.
- If the alert has an **Ended** status, you cannot make any changes to it.

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Use the search field or scroll down in the alerts table to locate the alert you want to edit.
3. Select the check box next to the alert name.
4. At the top of the screen, click the **More Actions** > **Edit**.
5. Make any changes you want to the unlocked fields.
6. Click **Save**.

Define alert template details

The Alert Template section is used to establish the identifying characteristics of the alert template in the system.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Click **New**.
3. On the **New Alert Template** screen, in the **Name** field of the **Alert Template** section, enter a name and description for the alert template. The name and description display in BlackBerry AtHoc only; they are not displayed to end users. The name and description should make it easy to help publishers identify the alert template. For example, Tornado Warning.
4. In the **Description** field, provide details about the alert template purpose or content. For example, “Send out when there has been a tornado sighted within 5 miles of the facility.” This description is not seen by end users. It is only visible within the application.
5. In the **Folder** field, select the alert folder that you want to add the alert template to.
6. Optionally, select **Available for quick publish** if you want to make the new alert template available through all quick publish links in the application.
7. Optionally, select **Available for mobile publishing** if you want to make the new alert template available for publishing from the mobile app.
8. When you are done, configure the Content section.

Writing effective alert messages

Use the following hints and best practices to publish successful alerts.

Content and message

- Keep the title and body brief and simple.
- If the alert is an Exercise or Test, clearly put the text “Exercise” or “Test” in the title and message. This practice ensures that everyone responds appropriately and no one mistakenly takes your exercise message for a real-world event.
- Use the five W’s: who, what, when, where, why, and how if needed.
- If you use acronyms or unique words, remember that text-to-speech may mispronounce your message or make it hard to understand. Add spaces or periods after each letter of the acronym.
- If you include a phone number, remember that the text-to-speech reads the number in this order: nation number, regional number, telephone exchange number, subscriber number, and extension number. Phone numbers are read digit by digit. If you include a regional number (area code) in parentheses, text to speech will not read the number correctly. For example: (xxx)-xxx-xxxx. To ensure that text to speech reads the regional number correctly, use one of the following formats:

  - xxx-xxx-xxxx
  - xxx xxx xxxx
  - xxx.xxx.xxxx

  The following table lists supported phone number formats:

Example phone number	Text to speech expansion
1 800 123 4567	one, eight hundred, one two three, four five six seven
01.1234.5678	zero one, one two three four, five six seven eight
01.1234.5678 Ext. 15	zero one, one two three four, five six seven eight, extension one five
Call me at 123-4567	Call me at one two three, four five six seven

- Placeholders can be very useful when using alert templates. Don’t forget to select the values if they are included.
- Use the **More Info Link** field to add a web page or Dropbox attachment URL.
- Include response options. They are a powerful tool to see who has responded to your alert and can provide valuable accountability information from your users.

Devices and coverage

- Use the devices that will most likely reach your users at the time of the alert.
- Target your Connect organizations if you want them to receive your alert.
- When sending a desktop pop-up, ensure that you choose the template and audio that best corresponds to your alert.
- The Phone is the only device that you can establish a delivery order for. When selecting multiple telephony devices, prioritize the devices your recipients are most likely to use.

- Use the device options to ensure your message is effectively communicated. For example, some devices have shorter message requirements. Or, a message that goes to the phones of individuals might be different than a message that goes to the general public over a loudspeaker.
- Use the options for (SMS) text messages to shorten the content to 160 characters or less. If you exceed the 160 characters allocated for the title, body, and response options, your message may be broken into several messages.
- When you use Twitter, use discretion because the message appears on social media, outside of your user base.

Publishing schedule

- Alerts can be scheduled to be published at a later date and time.
- Set the 'live' time for the time you want your users to be able to respond to your alert. You can estimate how long that they will receive the message and respond if they are away from their devices.

Review and publish

- If you have time, always test your messages before sending.
- Use Alert Folders to organize your alerts.
- Use spell checking for your Title and Content before publishing.
- Verify in the Targeting Summary that the correct individuals are receiving your alert.

Preview and publish (for email devices only)

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

Define content for an alert or alert template

The Content section is used to define the key parts of an alert or alert template in the system: title, body, type, response options, website links, locations, and attachments.

1. To create an alert or alert template in a language other than the default language displayed on the screen, click the button beside the Type field and select a language. This does not change the language displayed on the screen. Instead, it changes the language that the message is delivered in. If text-to-speech is enabled, the audio portion of the sent alert will be in the language you selected.
2. In the **Severity** field, select a severity level from the list.

   Important: High severity is reserved for extreme emergencies. On the mobile app, it overrides the device sound settings to play any sounds associated with the alert or alert template.
3. In the **Title** field, enter a one-line summary that communicates the purpose of the alert or alert template. The maximum number of characters is 100. The title is required and displays at the top of the recipients' screen when the alert is sent out.
4. Optionally, to insert a placeholder into the alert or alert template title, click ⊞ and select the placeholder from the list.
5. In the **Body** field, enter up to 4000 characters of text that communicate why the alert has been sent and provide instructions to the target audience. For more details on what to include in the Body field, see Writing effective alert messages.
6. In the **Type** field, select the type that fits with the alert or alert template you are creating.
7. In the **Response Options** field, do one of the following:
   - Click **Custom Response Options** to view and select from a list of pre-set responses.
   - Click **Add Response Option** to define one or more responses that alert recipients can send to let you know that they have received the message. To add a call bridge to a response option, see Configure a call bridge for a response option.

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

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

   For more information, see Add a bilingual alert.
9. Optionally, in the **More Info Link** field, enter one of the following:
   - A URL that opens a webpage where users can get more details about the alert. When users receive the alert, a **For more info** link in it will take them to the webpage.
   - A URL that opens an attachment (media or documents) stored on Dropbox. For details on how to store an attachment on Dropbox, see Add an attachment using Dropbox.

   Note: To include the URL in SMS alerts, the SMS alert template must contain a [TargetUrl] placeholder. For more information, see "Configure the hosted gateway for cloud services" in the *BlackBerry AtHoc System Settings and Configuration* guide.
10. If you entered a URL in the previous step, click **Test URL** to verify that the link works correctly.
11. Optionally, in the **Location** section, click **Add** to access a map where you can select a geographic area for the alert or alert template. For more information, see Select an alert location. This location can also be used to target users by location. For more information, see Target users by location.

12. Optionally, in the **Location** section, if you have selected a location, select **Enable Geofence Targeting** to target users who enter the location after the alert is sent. For more information, see Enable geofence targeting.
13. Optionally, in the **Attachments** section, drag and drop or click **Browse** to select files to include as attachments in the alert. For more information, see Add attachments.
14. Configure the Target users section.

Configure a call bridge for a response option

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

1. In the **Response Options** section, select the **Call Bridge** option beside a response option.
2. In the **Call Bridge #** field, enter the conference call number.
3. In the **Pass Code** field, enter the pass code users will use to dial in to the conference call. To add pauses before or in the middle of the code (for the operator to speak), add a comma for each second of pause time.
4. Optionally, in the **Conference URL** field, enter a call bridge URL. The URL address must begin with one of the following:
    - http:// – for standard web addresses
    - https:// – for secured web addresses
    - sip:// – for conference device addresses

Add a bilingual alert

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

Before you begin:

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

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

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

Select an alert or event location

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

- Define custom locations using the drawing tools available on the map.

- Select geographic areas from a list of locations that were predefined by a BlackBerry AtHoc administrator.

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

1. In the **Content** section, click **Add** in the **Location** section. The publisher map opens.

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

   Note: Uploading multiple layers with different sets of predefined locations is recommended to improve usability and system performance. Map layers are configured on the Map Settings screen. Administrators can access them at **Settings** > **Basic** > **Map Settings**.
4. Select one or more predefined locations in the layer by clicking them on the map or selecting them in the drop-down menu. As you make selections, the locations are highlighted on the map.
5. To create a custom location, click **Create Custom Locations** to display the drawing tools for creating shapes.
6. In the **Create Custom Locations** section, click a shape button and click and drag on the screen to select the location to use in the alert or event.
7. To view the size of a custom location, click the shape on the map. A black box appears next to the Create Custom Locations section, listing the total area of the custom location in square miles or square kilometers, depending on which unit of measurement your system uses.
8. To edit a custom location, click the shape and then click and drag on any of the circles that appear around the edge of the shape.
9. To scale new shapes up and down while preserving their dimensions, complete the following steps:

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

   As you create shapes and select predefined locations on the map, the **Location Summary** field in the bottom-right corner updates to provide you with an overview of the total number of locations that are displayed on the map and the locations that will be included in the alert or event.
10. To delete a custom location, in the **Location Summary** field, click the **X** beside each location you want to remove. If you have created more than one custom location, they are combined in the list and cannot be deleted individually. To delete individual custom locations, click the border of the location shape on the map to select it, then click 🗑 on the Create Custom Locations toolbar.
11. To view the total number of users and organizations that are located within the selected map locations, click **Calculate** next to the **Select By Location** field.

    Important: Users and organizations listed in the Select By Location field are automatically added to the alert or event target list. To remove them as targets, you can deselect the **Target Users** or **Target Organizations** options.
12. Optionally, in the **Select by Location** section, click **Export** to export the targeted users.

    a. On the **Export Options** screen, select the columns to export in the left column and click **Add**.
    b. Optionally, use the control buttons on the right to order the selected columns.
    c. Click **Export PDF** or **Export CSV**. The .pdf or .csv file downloads to your system.
    d. Click **Cancel** to close the **Export Options** screen.

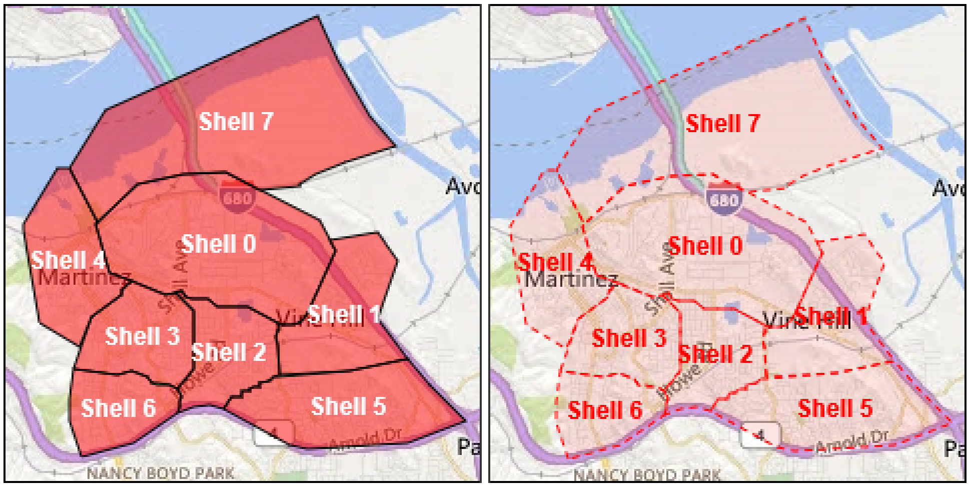
13. Click **Apply**.

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

View multiple information layers on a map

To enable operators to view multiple layers simultaneously, the Map screen includes a Layers (◈) icon. Selecting layers from this list adds them to the map for informational purposes: they can be viewed, but not clicked. In contrast, the Select Predefined Location button (available only on the publisher map) allows operators to select a location from a single layer at any given time.

1. Open the map.
2. In the bottom left corner of the screen, click ◈.
3. Select the layers you want to view from the **Show Layers** panel.
4. Click the check box next to any of the **Show Layers** items to see it displayed on the map. The difference between selecting a predefined location in the **Select Predefined Locations** drop-down list and doing so in the Show Layers panel is that the location is not interactive when selected in the Layers panel. This non-clickable status is indicated by the use of lighter shading and dotted lines around the edges of the locations, as shown on the right in the following image:



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

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

Change the map type

To change the map style in an alert or alert template, click 🗺 in the bottom left corner of the screen and then click to select the map you want to use. The following options are available:

- **Bing Road**: Microsoft's standard drawing map with streets and major landmarks labeled.
- **Bing Aerial**: Microsoft's standard aerial photograph of the map area.
- **Imagery**: Aerial photograph of the map area.
- **Imagery with Labels**: Aerial photograph of the map area with major landmarks labeled.
- **Streets**: Traditional drawing map with streets and major landmarks labeled.
- **Topographic**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Dark Gray Canvas**: Dark drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.

- **Light Gray Canvas**: Light drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.
- **National Geographic**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Oceans**: Traditional drawing map with topographical land features displayed and underwater topography labeled.
- **Terrain with Labels**: Traditional drawing map with topographical features displayed and cities and major roads labeled.
- **OpenStreetMap**: Traditional drawing map with streets and major landmarks labeled.

Note: OpenStreetMap is provided by OpenStreetMap (www.openstreetmap.org.) All other map types, except for Bing maps, are provided by ESRI (www.esri.com.)

Add attachments

If attachments are enabled for your organization and in the alert template, you can include text, audio, and video files as attachments in your alerts. You can add a maximum of 5 files totaling up to 5 MB.

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

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

The following file types are supported:

- Adobe Acrobat document (.pdf)
- Microsoft Word document (.doc, .docx)
- Microsoft Excel document (.xls, .xlsx)
- Text document (.txt)
- Image files (.jpeg, .jpg, .bmp, .png, .gif)
- Audio and video files (.mp3, .mp4)
- Markup language files (.html, .xml, .kml)

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

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

Enable geofence targeting

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

Before you begin:

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

- The By Location option must be selected on the Target Users tab of the alert template settings.

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

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

Add an attachment using Dropbox

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

If you want to include an attachment in an alert, alert template, event, or event template, you can upload media or documents on Dropbox and then include a link to that attachment within the alert, event, or template you are creating. To add a link to an attachment stored in Dropbox, complete the following steps:

1. In the **Content** section of the alert, event, or template, click **Choose from Dropbox**.
2. Enter your Dropbox username and password. If you do not have a Dropbox account, click **create an account** under the **Sign In** button to create one.

   Note: Although you need to set up an account in order to access Dropbox, you can use the **Choose from Dropbox** button to select files stored in the cloud or add files from your local drive without having to install the full Dropbox application on your computer.
3. Click **Upload**.
4. Click **Choose files**.
5. Navigate to the file you want to upload, then click **Open**.
6. Click **Done**.
7. Click the filename in your Dropbox homepage, then click the **Share** link that appears in the same row.
8. Copy the link location that appears in the **Link to file** field.

9. Paste the link location into the **More Info Link** field in the **Content** section of the alert, event, or template you are creating.

Configure a response option as a user attribute

Response options can be either of the following types:

- **Custom**: Defined during the creation of an alert or alert template. This is the most common type.
- **Preset**: Defined in advance as user attributes. The preset options have a feature that is not available in custom responses. When a user responds to the alert using a preset option, the response value is copied to their user record as a user attribute that can later be the subject of a query. The user attribute must be a single-select picklist, status attribute, or check box type. Use the single-select picklist type when you want to customize the response options. Use the check box attribute type if you require only a "Yes" or "No" response. Status attributes are used primarily as a single-select picklist for accountability events, but are also available as preset response options.

  Note: Single-select picklist, and status attributes can have a maximum of 9 values when used as response options.

When a user responds to an alert on multiple devices, only the response on the first device updates the alert summary. A user can update the user attribute from the response options one time for each device that received the alert. For example, if email is used to update a response option, and more than one email address is targeted, only the first email address the user responds from will update the attribute. Each subsequent response is ignored in alert reports. The user can update the attribute value by using another device, such as Phone or SMS, each device can update one time per alert.

If an attribute is used as a response option in an alert, the last response from a single device is the response that updates the user attribute value. If the attribute needs to be updated again after the alert, the user must access Self Service to make the update. Additionally, operators and administrators can update the attribute in the BlackBerry AtHoc management system.

If an attribute is used as a response option in an accountability event, each device can update the event if there are changes to the user's status. Only a single device can be used to update the status attribute value.

Benefits of using a preset response option

Preset response options created as user attributes are appropriate in the following situations:

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

1. In the navigation bar, click ⚙.
2. Click **Users** > **User Attributes**.
3. On the **User Attributes** screen, click **New** > **Single-select Picklist**.

   Note: If you require only a "Yes" or "No" response, select **New** > **Checkbox**.

   Note: Single-select Picklist attributes can have a maximum of 9 values when used as response options.
4. In the **Basic** section, in the **Name** field, enter a name for the attribute.
5. In the **Basic** section, select **Use as a Response Option**.
6. For a Single-select Picklist attribute, in the **Values** section, add the response options for each picklist option. The recommended number of response options is 3 to 5. Do not use more than 9 response options.

7. In the **Page Layout** section, leave all drop-down lists set to **Do not show**.
8. Optionally, to track the responses:
    a. In the **Personnel Reports** section, select the Enabled **Yes** option.
    b. In the **Name** field, enter the same name you entered in Step 4.
9. Click **Save**.

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

If you selected the **Enable** check box in Step 8, each time an operator publishes an alert with the response options you created, the option value each respondent selects is added to their user record. To view a summary of responses to each option, go to **Reports** > **Personnel Reports** and click **Summary** beside the name you gave the report in Step 8. A list of attributes and users who have selected the values are listed. A pie chart of the selected values is displayed.

For the attribute to show as a response option, at least one user must make a selection in the attribute. You may need to log out and log in to see the new attribute as a response option.

Target users

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

Targeting basics

The following general targeting information can be used to plan how to target recipients for different types of alerts.

- User-based targeting provides one or a combination of ways to select users:
  - **By Groups**: Target users who belong to one or more groups selected by the operator. Groups can be defined as organizations, shared attributes, or distribution lists. For more information, see Target groups in alerts or alert templates. You can also block groups from receiving the alert. For more information, see Block groups and distribution lists from receiving a notification.
  - **By Users**: Target individual users. You can also target dependents of sponsor users. Operators can also block specific individuals within a group from receiving the alert. For more information, see Block a user from receiving a notification.
  - **By Advanced Query**: Target users based on standard or user attributes or delivery devices. Select this option to perform customized targeting for an alert. For more information, see Target or block users by advanced query.
  - **By Location**: Target users based on their geographical location. For more information, see Target by location.

The administrator can restrict the organizational nodes and distribution lists that each publisher can access. As a result, a publisher might be able to target only a fraction of the total available organizations and distribution lists.

- Use Fill Count to specify a certain number of responses before ending an alert. This option is useful when you need confirmation that the alert has been received by a certain number of users.
- Enable Escalation to control the order in which users are contacted. Use escalation options to control the delivery order by groups or specific individuals.
- You can add a group escalation path based on user attribute values and priority. You can also specify a sequence that targets individuals, one-by-one, until enough users respond. After the fill count is met, the alert is ended.
- Blocking a recipient always takes priority during targeting. If a user is excluded, they *will not* receive an alert, even if they belong to a group, organization, geographical area, or distribution list that has been targeted to receive the alert.

Define fill counts and escalation

Use Fill Count to specify a certain number of responses before ending an alert. This option is useful when you need confirmation that the alert has been received by a certain number of users. For example, if you need ten emergency responders to report to an event, you can request this many responses before the alert ends.

Additionally, you can enable Escalation to control the order in which groups or individuals are contacted. For example, you might want a high priority group of users to be contacted before another group of users. To control the order, you use an attribute to target groups or users.

Note: If dependents are targeted in the alert template, Fill Count is not available. If Fill Count is enabled in the alert template, dependents cannot be targeted.

Example: Emergency notification with fill count and escalation

You need to set up an alert template to contact the appropriate teams during a chemical spill. You select a user attribute named EC_ChemSpill. The values of EC_ChemSpill include Chemical Facility, Supervisors, and Executives.

The creation and execution of this hypothetical alert would take place in the following stages:

1. You specify the number of “I can help” responses that must be sent before the alert can end. In this example, that number is 10.
2. You enable alert escalation by choosing a user attribute with groups that are contacted one at a time until the fill count is satisfied.
3. You set the sort order from lowest to highest to ensure that if 10 Chemical Facility team members do not select the "I can help" response option within the time frame, the alert escalates to the Supervisors team.
4. You enter an interval of 6 minutes for each team to respond before the alert escalates to the next team.
5. The first group, the Chemical Facility team, gets the alert immediately.
6. Only seven members respond within the six-minute interval for that part of the alert.
7. The alert then escalates automatically to the next team: the Supervisors.
8. Three members of the Supervisors team respond within the next six-minute interval. The fill count is met so the alert ends.
9. The Executive team is not contacted because the alert ended before it escalated to them.

Prerequisites

- The alert template must have the Fill Count setting enabled. See "Manage visibility options for Target Users fields in an alert template" in the *Alert Templates*guide.
- The user attribute that will be used to target groups and users must be created:
  - It can be any attribute type other than Memo or Geolocation.
  - (Recommended) For escalations, you should use a single- or multi-select picklist that targets the groups of users needed to meet the fill count.
- Users must have the selected user attribute as part of their profile.
- Response options must be defined in the Content section of the alert.

1. In the **Target Users** section, click **Fill Count and Escalation**.
2. On the **Fill Count and Escalation** window, in the **Required Response(s)** field, enter the number of responses needed to end the alert. This number can be changed when the alert is actually published.
3. Select a **Response Option** for the fill count.
4. Optionally, select the **Enable Escalation** option to define the order in which groups of users are contacted.
5. In the **Escalate By** list, select any user attribute with a type other than *memo* or *geo location*.

   The attribute should target the users you want to deliver the alert to. If the attribute is a picklist, ensure that the sort order is correct.
6. Specify the **Escalate Priority** method for the escalation or delivery method.

   Select **Top to Bottom** to start with the first value in the attribute list or **Bottom to Top** to start with the last value in the list. For example, in planning for a chemical spill, you could select top to bottom to ensure that HazMat personnel are sent the notification before it is escalated to higher levels of authority.
7. Optionally, to enable controlled delivery, select **One User at a Time** as a Delivery Method.
8. In the **Interval** field, specify how much time will be given to a group to respond before the next group or user is contacted. If the first group does not send enough responses to meet the fill count during the interval, alerts go out to the next group in the sort order.
9. Click **Apply**. Your choices are displayed at the top of the Target Users section. These choices can be edited before publishing.

10. To view the order users will be alerted in, click the number next to Total Users in the **Targeting Summary** section. The list of users is displayed in the order of escalation priority.
11. Publish the alert.
12. Monitor the status of the fill count with the Alert Summary Report. As the users respond, the fill count increases.

Target groups in alerts or alert templates

Using the By Groups tab, publishers can target groups of users based on their memberships in organizational hierarchical nodes or distribution lists. The alert is sent to users within the selected groups. Users who belong to multiple targeted groups receive a single alert.

The publisher can also block recipient groups (exclude them from alert delivery.)

The Group target categories displayed are:

- **Organizational Hierarchy**: If your system is set up for them
- **Distribution Lists**: Static and dynamic
- **Targetable Attributes**: Any attributes that have been selected as targeting criteria

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

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

   If you select a group or distribution list that contains sub groups or sub distribution lists, those are also automatically selected. Click the check box next to a selected sub group or sub distribution list to name to deselect it. If you select all sub groups or sub distribution lists manually, the parent group or distribution list is not selected automatically.

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

Block groups and distribution lists from receiving an alert

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

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

   Note: Even if a top-level group or distribution list is selected for inclusion, you can still block a sub group or sub distribution list underneath it. Blocking takes precedence over inclusion, so blocked sub groups and sub distribution lists will not be targeted even if their parent groups or distribution lists are targeted.

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

   Note: If you block a group or distribution list that contains sub groups or sub distribution lists, those are also automatically blocked. To unblock any of the sub groups or sub distribution lists, you must manually unblock the parent group or distribution list first. If you manually block all sub groups or sub distribution lists, the parent group or distribution list will not display a blocked icon.

Target individual users

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

Note: If dependents are enabled for your organization and enabled in the alert template settings, the Target Users section displays separate tabs for sponsors and dependents.

1. In the **Target Users** section, click **By Users**.
2. In the **Users** field, click **Add/Block Users**.
3. On the **Add/Block Users** screen, select the check box next to each user that you want to target in the alert. Click **Block**in the row for any user you want to block from receiving the alert.

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

   As you select and block users, the total number selected updates automatically at the top of the screen. The total number of targeted and blocked users appears below the search field.
4. Click **Apply**. The users you added are displayed in the Users field with a ✓ beside their name. Blocked users appear with a ⊘.

   Note: To remove a targeted user from the alert recipient list, click ✖ beside their name.
5. Optionally, to target dependents, click the **Dependents** tab and then select **Include all dependents of targeted sponsors**.

Target dependents

If dependents are enabled for your organization, you can target them on the Dependents tab in the Target Users section.

1. In the **Target Users** section, click **Sponsors**.
2. Select one or more sponsor users.
3. In the **Target Users** section, click **Dependents**.
4. Select **Include all dependents of targeted sponsors**.

Target subscribed users

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

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

Subscribed users can be targeted on their subscribed organization using email, SMS, phone, and mobile app devices and can be targeted using any criteria such as location, groups, or attributes. Targeted devices must be enabled on both the home and subscribed organizations. When targeting subscribed users by attributes, those attributes must be enterprise-level attributes.

1. In the **Target Users** section, click **By Advanced Query**.
2. Click the **Select Attribute** list, and then scroll down and click **Subscribed Organizations** in the **Attribute** section.
3. In the **Select Operation** field, select the **equals** operator. In the field that appears, select your organization.

4. Optionally, in the **Targeting Summary** section, click the number beside the **Advanced Query** field to view a pop-up screen that displays the attributes you have selected as targeting criteria for the alert.

Block a user from receiving an alert

You can block (exclude) specific users from receiving an alert. Individual alert settings take precedence over group settings, so if a user is blocked, they will not receive an alert even if a group they belong to is targeted in the alert.

1. In the **Target Users** section, click **By Users**.
2. In the **Users** field, click **Add/Block Users**.
3. On the **Add/Block Users** screen, click **Block** beside each user you want to block from receiving the alert.

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

   When you block a user, the Block link becomes an Unblock link and a 🚫 appears beside their name.
4. Click **Apply**.

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

Target or block users by advanced query

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

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

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

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

   Tip: For multi-select picklist, single-select picklist, geo-aware multi-select picklist, and status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.
7. Optionally, click **Add Condition** and then repeat steps 3 through 6 for each additional condition you want to add.

   The Targeting Summary field at the bottom of the Target Users section updates automatically to display the total number of users who match the query conditions you have created.

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

9. Optionally, modify the query conditions as needed to isolate the exact user group that you want to send the alert to. Click **Add Condition** to add more conditions. Click ⊟ beside a condition to remove it.

Target or block users with the User Last Updated Source attribute

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

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

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

Target users by role

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

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

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

   The Targeting Summary field at the bottom of the Target Users section updates automatically to display the total number of users who match the query conditions you have created.
7. Optionally, click the number in the **By Advanced Query** field to view a pop-up screen that lists the operator roles you have selected as targeting criteria for the alert.

Target users by location

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

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

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

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

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

Review the targeting summary

The Targeting Summary section of the Target Users section displays the total number of groups and users that have been selected and blocked, and the number of targeted locations and personal devices included in the alert.

As additional groups, users, and devices are added to or removed from the target group, the section updates automatically.

Click the numbered links in the Targeting Summary field to open a pop-up screen that provides a list of the users, devices, or search conditions related to the selected target.

By Groups

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

By Groups-Blocked

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

By Users

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

By Users-Blocked

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

By Location

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

By Advanced Query

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

Personal Devices

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

Select personal devices for an alert or alert template

After selecting the users or groups you want to include in the alert or alert template, you must select the personal and mass devices to use to contact the target group.

1. In the **Target Users** section, click **Select Personal Devices**.

A list of available personal devices appears, including the percentage of selected users who can be reached by each device type.

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

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

Specify personal device options for an alert or alert template

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

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

   The Personal Devices Options screen opens, displaying separate tabs and separate options for each device you selected in Step 2.
4. After selecting options, click **Apply**.

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

Device Type	Options	Description
Desktop Popup	App Template	• All desktop pop-up alerts display the alert severity and type, and, if available, a link to the alert location. BlackBerry AtHoc provides default templates, one for each severity: High, Moderate, Low, Informational, and Unknown. • Specify the desktop delivery template, either the default template or a custom template. • If you choose **Use Custom Template**, you can pick from any existing templates. • **Best Practice**: Click **Preview** to preview the custom template. **Important:** If your operating system has been magnified to 150% or higher, reduce the amount of text in the alert. If the alert exceeds the size of the alert dialog, the scroll bars might be unavailable.
	App Audio	• Select whether to use the default or a custom audio sound. The default audio is predefined by your organization. • If you choose **Use Custom Audio**, you can pick from any existing audio sound. • **Best Practice**: Click ► to preview audio selections.

Device Type	Options	Description
	Map Image in Alert	• Select **Enable** to include the location set in an alert template as a map in an alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map.
Email (for non-bilingual alerts)	—	• The device options for Email devices are set on the preview screen. For more information, see Preview and publish an alert.
Email (for bilingual alerts)	Email Template	• Specify the email template, either the default template or a custom template. BlackBerry AtHoc provides default templates for each severity: High, Moderate, Low, Informational, and Forgot Password. **Note:** If you select a custom template and your email delivery system does not support it, the default template is used.
	Email Message Content	• Select **Alert Title and Body** to use the information in the alert title and body fields as the email message content. • Select **Custom Text** to enter a custom title and message body as the email message content.
	Map Image in Alert	• Select **Enable** to include the location set in an alert template as a map in an alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map.

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

Device Type	Options	Description
	Audio Broadcast	• Select **No audio message** if you want no audio to play when the alert is received. • Select **Audio - Title and Body** if you want the alert title and body to play when the alert is received. If you select this option, you can specify the number of times to replay the alert. • Select **Audio - Title Only** if you want the alert title to play when the alert is received. If you select this option, you can specify the number of times to replay the alert. • Select **Audio - Body Only** if you want the alert body to play when the alert is received. If you select this option, you can specify the number of times to replay the alert. • Select **Custom** if you want to enter custom text for the alert. If you select this option, you can specify the number of times to replay the alert.
Phone	Phone Message Content	• Select **Send Alert Title and Body** to use the information in the alert title and body fields as the phone message content. • Select **Send Custom Text** to enter a custom title and message body as the phone message content. • Select **Send Recorded Message** to create and upload a custom recorded message that will be played for the alert recipients. For complete details on creating a recorded message, see Create a custom recorded message for an alert or alert template. For complete details on uploading a recorded message, see Upload a custom recorded message for an alert or alert template.
	Recipient Answers the Call	Select what happens after the recipient answers the call: • Deliver alert without any authentication. • Deliver alert only after the provided PIN is entered. • Deliver alert only after user validation.
	Recipient Does Not Answer the Call	Select what happens if the call is not answered: • Deliver alert as voice mail. • Leave callback information in the voicemail. **Note:** If this option is selected, the end user must have a PIN associated with their account to retrieve the alert message from a phone number other than the phone number targeted in the alert. • No voice mail.

Device Type	Options	Description
	Requires Acknowledgment	Select if the alert has no response options. The acknowledgment steps are provided at the end of the alert.
	Stop Calling Options	Select the criteria that stop calls from being made to the alert recipient: • Recipient acknowledged the message. • Recipient listened to entire message. • Entire message left on voicemail.
	Call Attempts	Enter the number of attempts the system makes to contact each recipient.
	Retry Interval	Enter the amount of time that must elapse before the system tries again to contact the recipient.

Device Type	Options	Description
BlackBerry AtHoc Mobile App	Repeat Notification	Each alert is only sent once. This option specifies if and how often notifications about the alert are repeated on a mobile device. • **None**: Send the alert notification once. • **Default**: Use the default time that has been defined for the selected severity. ◦ For **High** severity alerts, the default is one notification a minute for 10 minutes. ◦ For **Moderate**, **Low**, **Informational**, or **Unknown** severity alerts, the default is one notification a minute for 2 minutes. • **Custom** : ◦ Select how long to repeat the notification if the user does not respond. ◦ Select how long to pause between each repetition. **Note:** Ensure that the pause time is smaller than the repetition timeframe. For example, if you set the **Stop Repetition After** value for 5 minutes, and the **Pause between Notifications** value to 30 seconds, the notification can be repeated up to 9 times. However, if the **Stop Repetition After** value is 5 minutes, but the **Pause between Notifications** value is 6 minutes, the notification is repeated only once. Alert notifications repeat until one of the following actions occur: • The recipient responds to the alert from any of the mobile apps on which the same recipient is registered. Responses sent from other devices such as email, phone, or SMS, do not stop the notification. • The defined timeframe for repeat notifications elapses. • The alert ends.
	Deliver Alert with Sound	• Select **Yes** if you want the mobile device to play a sound according to the alert severity and device settings. For High severity alerts, this setting overrides the device settings and plays a sound when an alert is delivered. For all non high-severity alerts, the sound setting on the mobile device takes precedence. This is the default. • Select **No** to prevent the mobile device from playing any sounds. Alerts of any severity are delivered silently.

Create a custom recorded message for an alert or alert template

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

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

1. In the **Target Users** section, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the check boxes beside the phone devices to use as targeting methods.
3. Click **Options**.
4. On the **Personal Devices Options** screen, click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Record New Message**.
7. On the **Record New Message** window, click **Record** and then start speaking.

   Note: As you speak, the timer on the screen counts down, showing you how many more seconds you can record. By default, the timer is set to 1 minute.
8. When you have finished recording the message, click **Stop**.
9. Optionally, click ▶ to listen to your message.
10. Optionally, if you want to re-record the message, click **Record**.
11. When you are satisfied with the recording, click **Use Recording**.

    The Personal Devices Options screen appears, with the Phone tab displayed and the filename field populated with a system-generated name for your recording.
12. Optionally, click ⬇ to download your message as a .wav file.
13. Optionally, make selections in the other fields on the **Phone** tab.
14. Click **Apply**.

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

Upload a custom recorded message for an alert or alert template

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

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

1. In the **Target Users** field of the alert or alert template, click the **Select Personal Devices** tab.
2. In the **Personal Devices** section, select the check boxes beside the phone devices to use as targeting methods.
3. Click **Options**.
4. On the **Personal Devices Options** screen, click the **Phone** tab.
5. In the **Phone Message Content** section, select **Send Recorded Message**.
6. Click **Browse** and navigate to the location where the custom recorded message is stored.
7. Click the filename and then click **Open**. The name of the file appears in the filename field.
8. Optionally, click **Play** to hear the message before attaching it to the alert or alert template.
9. Optionally, make selections in the other fields on the **Phone** tab.
10. Click **Apply**.

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

Preview a desktop alert template

1. In the **Target Users** section, click **Select Personal Devices**.
2. In the **Personal Devices** field, select **Desktop App**.

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

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

Select the device delivery preference

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

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

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

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

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

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

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

Before you begin:

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

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

Target AtHoc Connect organizations

Note: You must have the Connect Publisher, Organization Administrator, or Enterprise Administrator role to target AtHoc Connect organizations in alerts or alert templates or to respond to alerts from these organizations.

1. Create or open the alert or alert template you want to add organizations to.
2. In the **Target Organizations** section, select each organization you want to target or select **Include all connected organizations** at the top of the section to target all organizations that you are connected to.

Select and configure mass devices for an alert or alert template

Note: This feature is not available for non-English alert templates.

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

1. In the **Mass Devices** section, select the check box beside each mass device you want to use to broadcast alerts.
2. Optionally, click **Options** at the top of the **Mass Devices** section.

   Each of the mass devices you selected in Step 1 appears as a separate tab on the Mass Devices Options screen that opens. The contents of each tab vary depending on the type of mass device selected.
3. Click each tab on the screen and then configure each mass device by selecting from the range of options that appear.
4. Click **Apply**.

Review an alert

When you click **Review and Publish** after creating an alert, the **Review and Publish** screen opens.

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

The Alert Summary screen appears, displaying the alert details and targeting information. Click the **Advanced Reports** button to view detailed tracking reports for the alert.

Test an alert

The BlackBerry AtHoc system allows you to test any alert from the Edit Alert screen. When you test the alert, it is sent only to you.

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

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

Set an alert to draft mode

Alerts are sometimes created in advance or created by operators who do not have the necessary permissions to publish them. BlackBerry AtHoc allows the alert creator to set the alert to Draft mode, which retains the details of the alert. The draft alert is saved in the Sent Alerts screen as a draft.

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

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

Publish a draft alert

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

Quick publish an alert

When time is critical and you want to publish an alert where only the Title and Body content needs to be changed, you can edit only those sections without the need to wait for the entire Review and Publish page to load.

Before you can quick publish an alert, the alert template must be in a Ready state.

1. Access an alert template from any of the following locations:

    - The Quick Publish section on the BlackBerry AtHoc management system home page
    - The Alert Templates page
    - The Sent Alerts page. Select an alert, and then select **More Actions** > **Publish**.

    The Review and Publish page opens. The Title and Body fields in the Content section of the alert template appear in a white box at the top of the page.
2. On the **Review and Publish** page, click✏.
3. On the **Edit Title and Body** window, update the title and body text as needed. The title must be between 3 and 100 characters. The body must be fewer than 4000 characters.
4. Click **Apply**. You are returned to the Review and Publish page. If you click **Edit** at the bottom of the **Review and Publish** page to edit other sections of the alert template, any changes you made in the Edit Title and Body window are not retained.
5. Click **Publish**.

Resend an alert

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

1. the navigation bar, click **Alerts** > **Sent Alerts**.
2. On the **Sent Alerts** screen, click the alert that you want to resend.
3. On the alert details screen, click the **Users** tab.
4. In the **Sent Details** section, click the drop-down menu in the **Targeted**, **Sent**, or **In Progress or Failed** row.
5. Select **Send Alert to These Users**.
6. Optionally, on the alert details page, update the details of the alert.
7. Click **Review and Publish**.
8. On the **Review and Publish** page, click **Publish**.

Track alerts with advanced reports

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

View advanced reports

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

To view advanced reports from the Advanced Reports screen, complete the following steps:

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

   The report opens in a new browser screen.

To view an advanced report for a specific set of users from the Sent Alerts screen, complete the following steps:

1. In the navigation bar, click **Alerts** > **Sent Alerts**.
2. Click a live alert or ended alert.
3. Click the **Users** tab.
4. Do one of the following:
   - In the **Sent Details** section, select **User List** from the drop-down menu next to **Targeted**, **Sent**, or **In Progress or Failed** to go directly to an Advanced Report that lists users in that category.
   - In the **Response Details** section, select **User List** from the drop-down menu next to **Responded** or **Not Responded** to go directly to an Advanced Report that lists users who have responded or have not responded to the alert.

Advanced report types

The following reports provide advanced tracking information about the alert delivery process, including the number of alerts sent compared to the delivery devices used and the responses received.

Report name	Description
Organizational Report	Displays the alert progress for recipients grouped by Organizational Hierarchy.
Distribution List Report	Displays the alert's progress for recipients divided by targeted distribution lists.
Delivery Distribution by Devices (Chart)	Displays a group bar chart that tracks, for each device used, the number of targeted alerts, the number of alerts sent, and the number of responses received.

Report name	Description
Delivery Distribution by Devices	Displays a tabular report that tracks the number of targeted alerts, the number of alerts sent, and the number of responses received for each device used. The report can include all devices or only the devices used for targeted recipients. You can click any user count in the report, such as the number of targeted users, to open a detailed user tracking report that identifies individual users and provides their names, device addresses, and responses. This information is useful for evaluating the effectiveness of the delivery devices used for the alert. **Note:** If device delivery preference is set to Organization defined, the number in the Sent column of the report is updated incrementally as different personal devices are targeted.
User Tracking Reports	Displays user tracking information and user response data. The User Tracking with Devices report tracks which users were targeted by device and which device users responded on. The User Tracking with Alerts report tracks the delivery date and delivery status of the alert.

View alert lifecycle results

You can view the publishing lifecycle for an alert to trace the progress of the alert and determine how it was handled during delivery. The lifecycle shows information such as the following:

- When the alert went through the delivery gateway
- If a failure prevented the alert from being delivered
- If the alert needed to be redirected because of a gateway failover

You can also check the batch process to determine if the alert was delivered.

To view the publishing lifecycle events, complete the following steps:

1. Open the alert summary and do one of the following:
    - After sending the alert, click **Alert Summary** in the completed alert, then click **Advanced Reports** at the top of the screen.
    - In the navigation bar, click **Alerts** > **Sent Alerts**.

        a. On the **Sent Alerts** screen, click the live or ended alert you want to see lifecycle results for.
        b. Click **Advanced Reports**.
2. On the report screen, scroll to the **Publishing Lifecycle** section.
3. Check to see that the alert was marked as Live.
4. In the **Publish Alert messages** field, check for batch reports, and then click **Show Details** to see a detailed log.

    A batch contains the alerts for each targeted user and is sent to a delivery gateway corresponding to the personal or mass devices targeted in the alert. The batch report tracks the delivery of the batch to the gateway and whether it was successful.

    It shows if there was a problem with the batch and whether it had to be sent to another gateway for delivery. This is called batch recovery.
5. Check to see that the recipients were populated.

    Note: If you have specified backup delivery gateways for the targeted devices, you might see additional batch reports if messages were redirected to a backup gateway because of a failover.

Alert partial batch recovery

BlackBerry AtHoc Cloud Delivery Services performs partial batch recovery when a subset of a batch of alerts cannot be successfully delivered to email, SMS, or telephony devices. Batch recovery occurs when delivery errors in the batch reach 20% of users, or more.

If there is a complete batch failure (100%), BlackBerry AtHoc tries to recover immediately.

For example, an operator publishes an alert that targets 50 users. Thirty-five users receive their alerts, however, message error codes were received for the other 15 users, exceeding the 20% recovery threshold. After 5 minutes, BlackBerry AtHoc sends a termination request to the primary gateway. It then creates a recovery batch only for the users that got errors for the next available gateway.

BlackBerry AtHoc cancels the current batch delivery and creates a new batch to be sent to another gateway, if the alert batch meets the following conditions:

- The network is up and BlackBerry AtHoc Cloud Delivery Service is available.
- Gateway reporting succeeds for the batch.
- The percentage of "No activity" plus "Error" messages reaches the recovery threshold within the batch. The default is 20%. Alerts that have received responses are not counted.

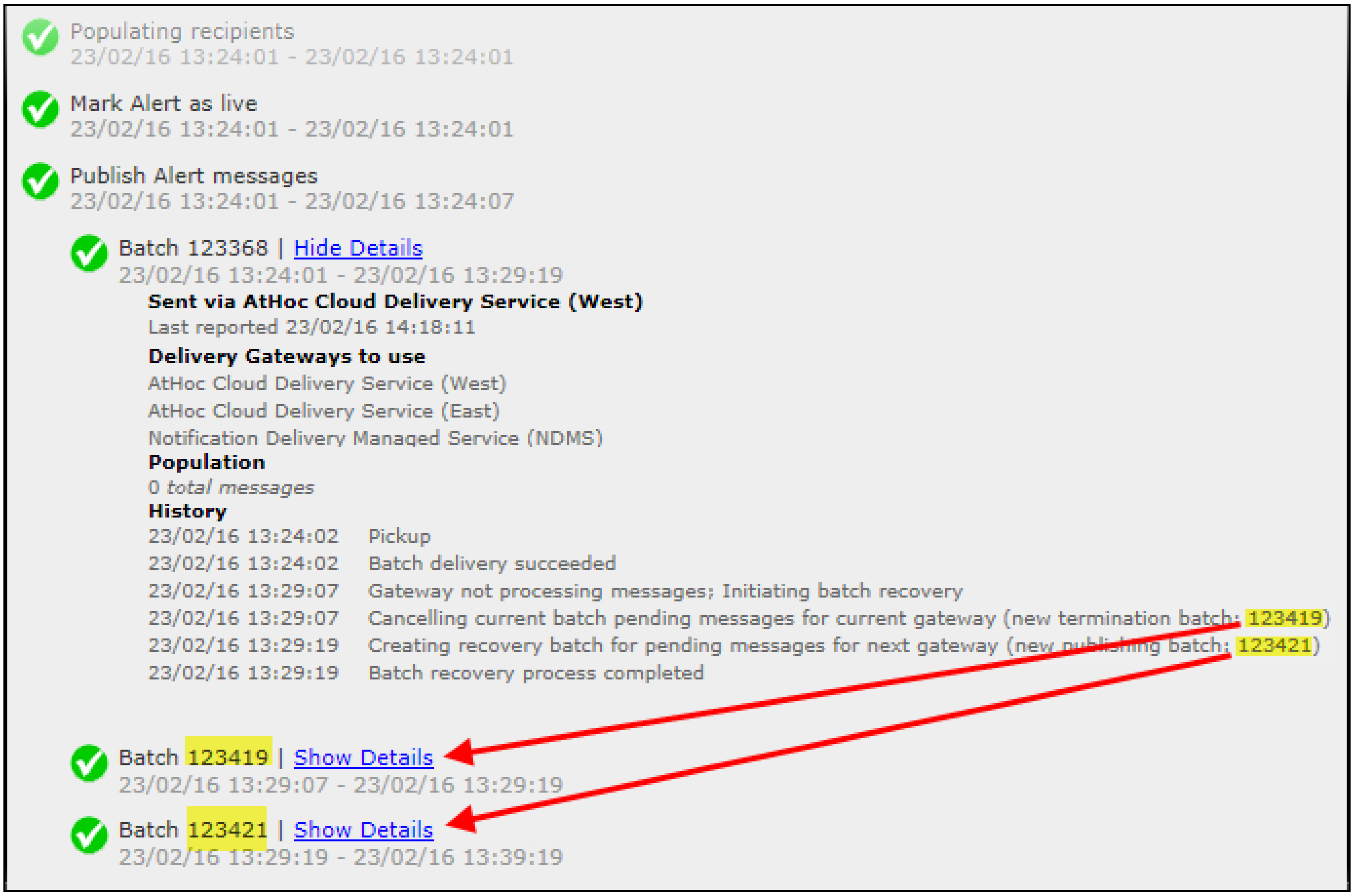
After a specified time (the default is five minutes), BlackBerry AtHoc resends any alert that was not sent or does not have a response. Users that have responded to the alert do not receive another alert.

The new alert batch contains the following information:

- All alert messages that had delivery errors
- All alert messages that had no delivery tracking information (inactivity)
- Relevant phone messages that had MSG-SENT codes, when the contact cycle value is greater than “1”
- Excludes all messages that already have acknowledgments coming from any devices

To view delivery information, check the Publishing Lifecycle section of the Alert Summary. The Batch details show how many alerts, whether the batch was sent successfully, and if it had to be redirected. You can also check user delivery reports for more information.

The following figure shows the history of the alert delivery and the recovery process.



✓ Populating recipients
23/02/16 13:24:01 - 23/02/16 13:24:01

✓ Mark Alert as live
23/02/16 13:24:01 - 23/02/16 13:24:01

✓ Publish Alert messages
23/02/16 13:24:01 - 23/02/16 13:24:07

✓ Batch 123368 | Hide Details
23/02/16 13:24:01 - 23/02/16 13:29:19

Sent via AtHoc Cloud Delivery Service (West)
Last reported 23/02/16 14:18:11

Delivery Gateways to use
AtHoc Cloud Delivery Service (West)
AtHoc Cloud Delivery Service (East)
Notification Delivery Managed Service (NDMS)

Population
0 *total messages*

History

23/02/16 13:24:02	Pickup
23/02/16 13:24:02	Batch delivery succeeded
23/02/16 13:29:07	Gateway not processing messages; Initiating batch recovery
23/02/16 13:29:07	Cancelling current batch pending messages for current gateway (new termination batch: 123419)
23/02/16 13:29:19	Creating recovery batch for pending messages for next gateway (new publishing batch: 123421)
23/02/16 13:29:19	Batch recovery process completed

✓ Batch 123419 | Show Details
23/02/16 13:29:07 - 23/02/16 13:29:19

✓ Batch 123421 | Show Details
23/02/16 13:29:19 - 23/02/16 13:39:19

As you can see, the initial alert batch was terminated (Batch:123419) for the current gateway, and a second publishing batch was created (Batch: 123421). You can click on the details for the additional batch reports to see if the batch was successfully sent. The batch can be sent to additional gateways if there are problems with second batch.

Export alert tracking reports

You can export alert tracking reports to a .csv file to view the full detailed report or for other tracking reasons.

1. Send an alert.
2. Click **Alert Summary** from the completed alert or open the alert from the **Sent Alerts** list.
3. On the **Alert Summary** screen, click **Advanced Reports**.
4. Hover over the **Export** link and then select **Export Full Report**.

The report is exported to a .csv file.

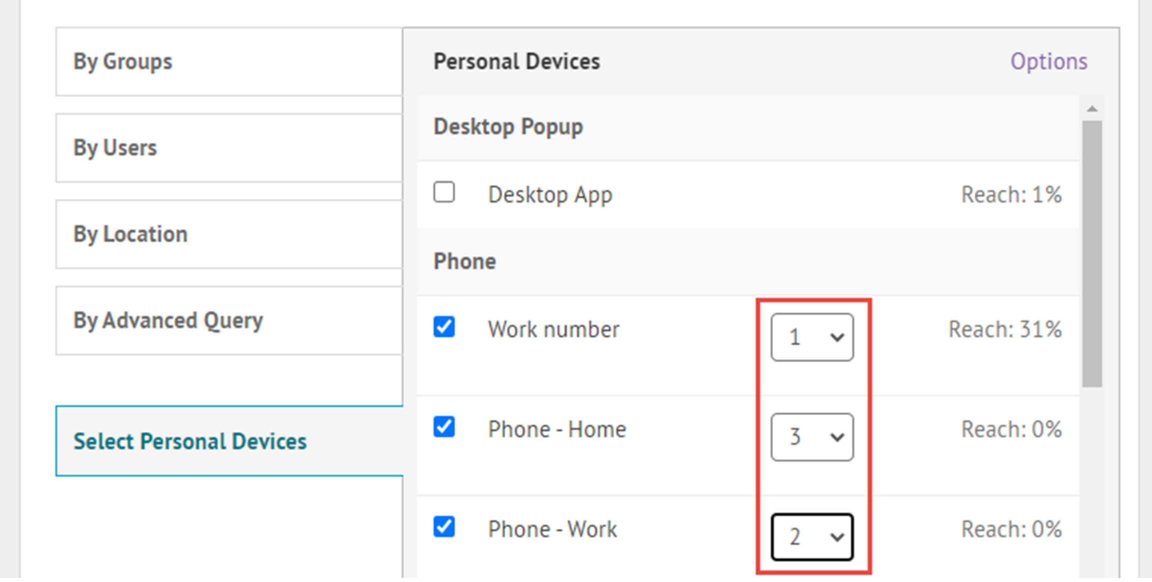
Message termination

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

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

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

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



☐ Desktop App Reach: 1%

☑ Work number 1 Reach: 31%

☑ Phone - Home 3 Reach: 0%

☑ Phone - Work 2 Reach: 0%

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

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

Disable message termination

Message termination is enabled by default.

1. Start **Internet Information Services** (IIS.)
2. In the **Connections** panel, expand the **Sites** folder.
3. Expand **IWS Services**.
4. Click **User Termination Coordinator**.
5. In the **Actions** panel, click **Stop Application**.
6. In the **Connections** panel, click **Application Pools**.
7. In the **Application Pools** pane, click **AtHoc User Termination Coordinator Pool**.
8. In the **Actions** panel, in the **Application Pool Tasks** section, click **Stop**.

   Note: If the Application Pool task indicates that it is already stopped, you can stop the process using the task manager.
9. Reset IIS.

Redundant message stop

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

Redundant message stop is enabled when:

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

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

Redundant message stop is not supported on the desktop app.

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

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

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

Message consolidation

Message consolidation applies to phone and text messaging devices only. Consolidation occurs when multiple users have the same phone number. It does not occur when a user has entered the same phone number for multiple device addresses.

For example, an alert targets a work phone, mobile phone, and text messaging. One of the targeted users has entered the same phone number in the address field for each device. The system sends two phone calls and a text message to the same device.

When the same alert targets several users who share a phone, the system sends one phone call to the phone. Note that response options are disabled when message consolidation occurs.

End an alert

You can end alerts that currently have a Live status.

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

The alert status changes from Live to Ended.

Export an alert as a PDF

The BlackBerry AtHoc system allows you to export alerts as .pdf documents by clicking a button on the Review and Publish screen that appears when reviewing a new or draft alert.

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

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

The alert details are downloaded as a PDF file.

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

Export sent alerts

The BlackBerry AtHoc system enables you to export the details of sent alerts to a .csv file. The report contains the following columns: Alert ID, Alert Title, Alert Body, Start Time, Publisher, Severity, Type, Status, Targeted, Sent, Responded, and Error.

Note: You must have report manager operator permissions to export sent alerts.

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

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

The .csv file downloads to your computer.

Delete an alert

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

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

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

Duplicate an alert

Important: When you duplicate an alert, the Schedule section of the new alert reverts to the default settings for all new alerts, overriding any date and time parameters that are configured for the alert that you duplicated. For example, if you duplicate an alert that is set to begin at 12:30 PM on August 1, 2015 and your system default is to have all new alerts begin "As soon as I click the "Publish" button," your duplicated alert will begin as soon as you click **Publish** unless you manually change the Alert Timing setting beforehand.

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

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

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

Hosted SMS text messaging tracking codes

The following codes are used to track the status of SMS text messages. They appear in the full delivery report for an alert.

Code	Status	Message
3001	Sent	Invalid destination phone number
3002	Sent	The target user has unsubscribed from BlackBerry AtHoc alerts
3003	Not Sent	The target carrier has blocked BlackBerry AtHoc alerts
3006	Not Sent	Rejected by the SMS aggregator
3007	Not Sent	Rejected by target carrier
3900	Not Sent	Error in sending alert

Pager carrier IDs and names

The following table displays the name and ID of all of the pager carriers that are supported in BlackBerry AtHoc.

Pager Name	ID	Pager Name	ID
AAA	1	MetroCall National TAP (888)	164
Advanced Paging and Wireless	2	MetroCall National2 TAP (800)	165
Advantage Paging	41	MetroCall TAP (757)	166
Airtouch Paging	3	MetroCall TAP (904)	162
Airtouch TAP	84	Metrotel National TAP	167
AllCom	4	Metrotel TAP	100
ALLTEL PCS	42	Midwest Paging	39
Alpha Messaging Center TAP	103	Midwest Paging National TAP	123
AlphaNow	5	Minncomm	57
American Messaging	73	MinnComm National TAP	133
American Messaging National TAP	149	MinnComm TAP (763)	134
American Messaging Network	81	Mobilfone	94
American Messaging TAP	74	MultiComm Paging TAP	97
American Messaging TAP (305)	145	MultiComm SNPP	98
American Messaging TAP (520)	140	MWD TAP	72
American Messaging TAP (586)	146	National Communication TAP	102
American Messaging TAP (618)	139	Network Services	20
American Messaging TAP (714)	147	New SPN National TAP	189

Pager Name	ID	Pager Name	ID
American Messaging TAP (734)	138	New SPN TAP (252)	194
American Messaging TAP (734)	144	New SPN TAP (330)	197
American Messaging TAP (734)	142	New SPN TAP (406)	190
American Messaging TAP (818)	150	New SPN TAP (609)	191
American Messaging TAP (818)	148	New SPN TAP (612)	193
American Messaging TAP (904)	141	New SPN TAP (626)	192
American Page Network	52	New SPN TAP (626)	195
Ameritech	6	Nextel	21
Ameritech 001 TAP	106	Nextel 2 Way	22
Ameritech TAP (314)	108	Northeast Paging	23
Ameritech TAP (573)	107	Omni-com Paging	24
Aquis SNPP	210	Omnicomm TAP (406)	110
Aquis TAP (615)	200	One Source	203
Arch National TAP	158	Other	40
Arch Wireless (USA Mobility)	38	Page 1	78
Arch Wireless 1-way (USA Mobility)	61	Page One TAP (304)	187
arch1way (USA Mobility)	18	Page Plus TAP (918)	153
AT&T Wireless	58	PageMart Canada	25
ATS National TAP	161	PageMe Inc	55
ATS Paging	83	PageNet - Canada	53
ATS TAP (402)	160	Pagenet Pro TAP	66

Pager Name	ID	Pager Name	ID
ATT Tap	208	PageOne - TX	215
Bailys Comm.	43	PageOne UK	92
Baystar	7	PagePlus	90
beepers.com	60	Pager People TAP	101
Bell Mobility (US)	8	Personal Page	214
Bell Mobility TAP (416 / Walkerton, ONT)	205	Porta-Phone Paging	26
Bell Mobility TAP (519 / Walkerton, ONT)	206	Priority Communications	27
BELL SNPP	204	ProPage	28
Cap Communications TAP (231)	175	RAM-Page	62
Carolina Wireless TAP	99	Range Paging	196
Carolina Wireless TAP (843)	172	Range Telecommunications	185
CellularPage	88	Range Telecommunications (TAP 512)	211
Central Vermont Comm.	45	Range Telecommunications TAP	209
Chariton Valley National TAP	199	RCS Wireless	77
Cingular	64	Rogers Two Way	48
Comm Special TAP (910)	109	RSC COMM National TAP	151
Communications Specialists	9	Satellink	29
Contact Communications	82	Satellink TAP (615)	111
Contact Paging	10	SBC National TAP (800.250)	129

Pager Name	ID	Pager Name	ID
Contact Wireless	207	SBC National TAP (800.864)	132
Cook Paging	37	SBC National TAP (877.802)	130
DataComm	11	SBC Paging	56
DataPage	12	SBC TAP	85
Dial A Page TAP (479)	186	SBC TAP (313)	131
Digi-Page/ Kansas	13	SBC TAP (573)	127
Edge Wireless	79	SBC TAP (763)	128
Electronic Engineering TAP (319.362)	181	Schuylkill Mobile	93
Electronic Engineering TAP (319.833)	180	Schuylkill TAP (570)	154
Electronic Engineering TAP (515)	179	Schuylkill TAP (717)	155
Extel Mobile	14	Sharp TAP (256)	176
GrayLink	15	Skytel	30
Highland Paging, Inc.	16	SkyTel National TAP	173
Illinois Signal	46	Skytel Talkabout	63
IM Cingular	76	Skytel TAP	67
Indiana Paging SNPP	44	Sprint SNPP	89
Indiana Paging TAP (219.756)	126	Stenocall TAP (806)	174
Indiana Paging TAP (219.928)	124	Teleone TAP	104
Indiana Paging TAP (317)	125	Teleone TAP (903)	178
Infopage Systems	17	Telepage TAP	105
Intelliguard Systems	95	TeleTouch (TeleOne) SNPP	202

Pager Name	ID	Pager Name	ID
Intelliguard Systems (TSU/Raven)	96	Teletouch TAP (501)	171
Island Page	68	Teletouch1 National TAP	168
JSM Comm TAP (414)	137	Teletouch2 National TAP	169
JSM Comm TAP (608)	136	Teletouch3 National TAP	170
JSMCOM 1-way	65	Tele-Trak	31
KP In-House	213	Telus Vancouver TAP	91
KPN TAP	212	Texas Communications	198
Lauttamus 2 TAP (304)	183	TSCNet	32
Lauttamus Communications SNPP	201	TWR TAP (301)	184
Lauttamus TAP (304)	182	UCOM	50
Maximum Communications	54	UCP	33
Metro Communication TAP	87	Unity Comm TAP (304)	135
Metrocall (USA Mobility)	19	Unity Communications	59
Metrocall 1-way (USA Mobility)	51	US Mobility TAP	75
MetroCall National TAP (800)	163	USA Mobility	80

Phone number validation

An Emergency Mass Notification System is only as effective as the contact information it contains. For this reason, BlackBerry AtHoc provides a phone number validation feature that applies to all phone numbers, no matter which country they belong to. It also enforces clean data wherever data can be entered.

The validation feature gives operators higher confidence before an alert is sent that end users with phone numbers are reachable. One way it does this is by ensuring that end users completing Self Service profiles enter actual phone numbers, instead of invalid data such as “No Phone” or “N/A.” Validating phone numbers when they are created in the system makes the alerting process more rapid and efficient by preventing the Telephony Delivery Service from wasting time trying to send telephone notifications to invalid numbers.

BlackBerry AtHoc provides this feature for customers operating outside or calling users who are outside the United States. Validated phone numbers can be stored in the internationally recognized E.164 format, ensuring that alerts sent by delivery services deployed throughout the world will reach their destinations. BlackBerry AtHoc uses a third-party library to validate phone numbers.

BlackBerry AtHoc works with customers to make sure that automated data imports, including Active Directory sync, .csv imports, and direct SDK integrations, will send phone numbers to the server in the correct format. The following sections provide the validation rules and best practices for getting the most out of this feature.

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

For BlackBerry AtHoc release 6.1.8.88 and earlier releases, you must continue to use 011 instead of + at the beginning of all international phone numbers.

BlackBerry AtHoc release 6.1.8.89 and later releases fully support the leading + method. Dialing 011 will continue to be supported after upgrade to 6.1.8.89 for organizations with a U.S. country code since 001 is the U.S. exit code.

Areas of the system that validate phone numbers

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

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

Validation rules

The following validation rules are delivered by a third-party open source component. For more information, see: https://github.com/googlei18n/libphonenumber.

- E.164 international format is preferred and is always accepted. The number should start with + followed by the country code and then the full number to call. A maximum of 15 digits can be used. For example: +18884628462.
- Numbers can have an extension. The user interface has a separate field for telephone extensions. When importing numbers, an x should be used to separate the main number from the extension. When dialing, the Telephony Delivery Service will wait for the call to connect before dialing the extension. For example: +18884628462x1340. Unlike the phone number field, the extension field is not validated.

- Numbers not in E.164 are interpreted based on the Default Country Code for the Organization.
  - The Default Country Code can be set on the General Settings screen in the Phone Call Settings section.
  - For example, for the Country Code "US," the following rules apply:
    - If the number starts with 011, which is the international exit code from within US, it will be replaced with +.
    - If the number contains only 10 digits, it will be stored as +1 followed by the number.
    - If the number contains 11 digits and starts with 1, it will be stored as +1 followed by the number.
    - For example: (888) 462-8462 will be interpreted as +18884628462
- Common formatting punctuation is ignored.
  - The following characters are removed: ().-_
  - For example: +1 (888) 462-8462 will be interpreted as +18884628462.
  - If you are using control characters such as , (comma) or # (pound sign), they must be in the extension field.
- If the number contains letters, they will be converted to numbers according to a standard keypad. For example: (888) Go AtHoc will be converted to +18884628462.
- If the number starts with +, it will be assumed to be an international number. For example: A number starting with +440 will dial the UK, even though 440 is a valid US area code.

Best practices

Send all numbers in E.164 format. Although E.164 format is not required, it is the best way to send a number to the system, especially if user data can contain numbers from different countries.

Make sure you set the correct Default Country Code in the Phone Call Settings section on the General Settings screen. This specifies what country is the default for user-entered phone numbers. This also is used to interpret phone numbers that are not in E.164 format.

If the number contains any special control characters that must be dialed, such as , (comma) ; (semicolon) * (asterisk) or # (pound sign), the characters must be part of the extension. This is especially important for numbers that connect to a conference bridge.

Email format validation

A critical event management system is only as effective as the contact information it contains. For this reason, BlackBerry AtHoc validates that email addresses are RFC-5322 compliant in the following areas:

- End User Manager in the management system
- Self Service My Profile page
- Forgot Username
- Forgot Password
- .CSV import
- User Sync Client
- AtHoc SDK
- Swagger

Email address syntax

The valid email address syntax is *local-part@domain*.

Local-part

The local-part of an email address can contain any of the following ASCII characters:

- Uppercase and lowercase Latin letters A to Z and a to z
- Digits 0 to 9
- The following printable characters: !#$%&'*+-/=?^_`{|}~

The following guidelines apply to the local-part of a valid email address:

- The dot (.) character is allowed but cannot be the first or last character and cannot appear consecutively.
- Spaces are not allowed.
- The length is not validated.

Domain

The domain of an email address can contain any of the following ASCII characters:

- Uppercase and lowercase Latin letters A to Z and a to z
- Digits 0 to 9

The following guidelines apply to the domain of a valid email address:

- The domain must match the requirements for a hostname, and include a list of dot (.) separated DNS labels.
- The dot (.) character is allowed but cannot be the first or last character and cannot appear consecutively.
- No digits are allowed in the top-level domain (TLD). The TLD is the portion of the domain after the dot (.).
- The TLD must contain a minimum of 2 and a maximum of 15 characters.
- Spaces are not allowed.
- The length is not validated.

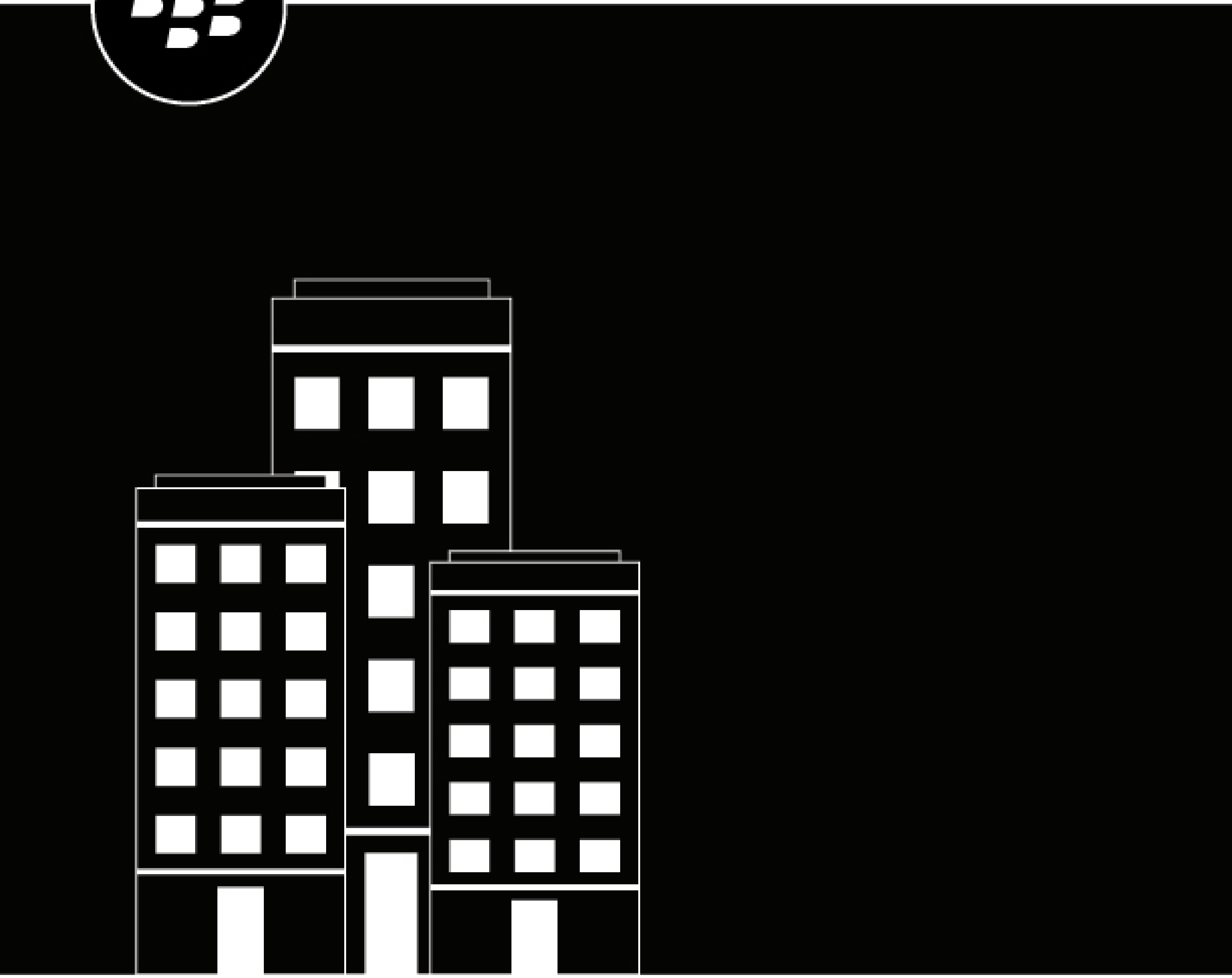
Valid email address examples

- simple@example.com

- very.common@example.com
- abc@example.co.uk
- disposable.style.email.with+symbol@example.com
- other.email-with-hyphen@example.com
- fully-qualified-domain@example.com
- user.name+tag+sorting@example.com
- example-indeed@strange-example.com
- example-indeed@strange-example.inininini
- 1234567890123456789012345678901234567890123456789012345678901234+x@example.com

Invalid email address examples

- Abc.example.com (No @ character.)
- A@b@c@example.com (Only one @ is allowed outside quotation marks.)
- a"b(c)d,e:f;g<h>i[j\k]l@example.com (None of the special characters in the local-part are allowed.)
- just"not"right@example.com (Quoted strings are not supported.)
- this is"not\allowed@example.com (Spaces, quotes, and backslashes are not allowed.)
- this\ still\"notallowed@example.com



BlackBerry AtHoc

Incoming Alerts in the Inbox

7.16

Contents

Manage incoming alerts in the Inbox

The Inbox displays information about live and expired alerts from mobile users, Connect organizations, other agencies, and the Integrated Public Alert and Warning System (IPAWS). Alerts from mobile users and outside organizations are called incoming alerts. The Inbox provides organizations with a means of managing incoming alerts and monitoring what is happening in their system.

Updates to the Inbox are fully automated. When a new alert is received or an operator reviews or replies to an alert, the Inbox updates immediately to display the new item.

Access the Inbox

BlackBerry® AtHoc® administrators and operators must be members of the Emergency Community to see items in the Inbox.

1. In the navigation bar, click **Alerts** > **Inbox**. The Inbox opens, showing all incoming alerts in the system. Alerts that have not been reviewed appear in bold.

   In the left pane, the following items are displayed for each incoming alert in the Inbox:

   - **Severity icon**: Hover your cursor over the icon to display the severity level. Available severities are: High, Moderate, Low, Informational, or Unknown.
   - **Alert title**: Displays the subject of the alert.
   - **Source type icon**: Displays 👤 if the source is a person or 🏠 if the source is an organization.
   - **Source name**: Displays the name of the person or organization that created the alert.
   - **Creation date and time**: Displays the time and date stamp for the alert.
   - **Latitude, Longitude**: Displays GPS coordinates (for incoming live mobile alerts only). Displays only if a valid location is found.
   - **Alert type**: Displays the category of alert.
   - **Reply, Replied icon**: If an alert requires a response, a **Reply** icon appears next to the alert type. Clicking anywhere in the alert line opens the alert details field containing a Reply button. After you or another authorized user respond to an alert, a **Replied** icon replaces the Reply icon.
   - **Location icon**: Displays ➤ if the alert includes a map.
   - **Attachments icon**: Displays 📎 if the alert includes file, video, or image attachments.

View incoming alert details

1. In the navigation bar, click **Alerts** > **Inbox**. The Inbox opens, displaying all incoming alerts in the system.
2. In the **Inbox**, locate the alert you want to view.
3. Click anywhere in the alert row.

A detailed view of the alert appears in the right pane. The detailed view includes the following items:

- Alert title
- Severity
- Type
- Source
- Creation time
- Expiration time (if any)

- GPS coordinates (for incoming live mobile alerts only). This item is displayed only when a valid location is found.
- Body
- Review status (reviewed or not)
- Reviewer's name (if applicable)
- Review time (if applicable)
- Reply status (replied to or not, if applicable)
- Reply that was sent (if applicable)
- The name of the person who replied (if applicable)
- The time the event was replied to (if applicable)
- The location of the alert. Alerts with a location display ➤ in the alert row. To view a full-sized map of the incoming alert location, click ✎ next to the small map image.
- Any attachments to the alert. Incoming alerts with attachments have a 📎 in the alert row. To view an attached image, video, markup, or text file, click the thumbnail of the attachment to see it as a pop-up or click ⬇ to download it.

Reply to an incoming alert

Within the Inbox, *reviewing* refers to the action of looking at the details of an alert while *replying* refers to the action of responding to the alert by clicking a button and selecting a response option. You can reply to an alert if it meets all of the following criteria:

- It requires a reply
- It has not yet expired
- It has not yet been replied to
- It was sent from another organization

Note: Reviewing is a *per alert* action, not a *per person* action. Only one person must review an alert for it to be marked as reviewed in the system. If another operator reviews an alert, their review is reflected on your screen. If you mark an alert as reviewed, that action will be reflected on the screens of all operators.

There are two ways to reply to an incoming alert. The method you chose will depend on how much information you need prior to replying.

Reply directly from the Inbox list

Replying to an event directly from the Inbox list is a fast and easy way to reply to an alert that you either know about already or that is not complex or detailed.

1. In the navigation bar, click **Alerts** > **Inbox**.
2. In the **Inbox**, locate the alert that you want to reply to.
3. Click **Reply** at the end of the alert row.

   Note: The **Reply** button is disabled if the alert does not require a response, if it has expired, or if you have already responded to it.

   A pop-up screen appears listing the response options for the alert.
4. Select a response option and then click **Reply Now**.

Reply through the Alert Details section

Replying to an alert from the Alert Details section is more appropriate for alerts that contain attachments, maps, or complex or detailed responses.

1. In the navigation bar, click **Alerts** > **Inbox**.
2. In the **Inbox**, locate the alert that you want to reply to.
3. Click anywhere in the alert row. The details of the alert appear in the right pane.
4. Click **Reply** at the top of the details section.

   Note: The **Reply** button is disabled if the alert does not require a response, if it has expired, or if you have already responded to it.

   A pop-up screen appears listing the response options for the alert with the first option already selected by default.
5. Select a response option, and then click **Reply Now**.

Forward an incoming alert

1. In the navigation bar, click **Alerts** > **Inbox**.
2. In the **Inbox**, locate the alert that you want to forward.
3. Click anywhere in the alert row. The details of the alert appear in the right pane.
4. Click **Forward Alert** at the top of the details section.
5. Optionally, if attachments are included in the alert, the **Select Attachments** window opens. Select the attachments that you want to include in the forwarded alert and click **Close**.

   The Alert Details screen appears, displaying the title, message body, attachments, and the default response options for the alert.
6. Optionally, in the **Content** section, modify the title and message body if necessary.
7. Optionally, in the **Attachments** field, drag and drop or click **Browse** to include additional attachments.
8. Optionally, add more response options if the current options do not include all of the possible responses that you want to make available to recipients.
9. In the **Target Users** section, select the people and organizations to forward the alert to.
10. In the **Target Users** section, click **Select Personal Devices** and select the check box beside each personal device you want to include.
11. Click **Review and Publish**.
12. On the **Review and Publish** screen, review the content of the alert.
13. Optionally, click **Preview and Publish** to preview how the forwarded alert will appear to end users.
14. Click **Publish**.

Note: For an alert triggered due to a connect rule based on a selected condition, the severity and type values are retained from the original alert. The application overwrites the severity and type values selected in the alert template with the values from the alert forwarded from the Inbox.

Mark alerts as reviewed or not reviewed

Reviewing is a *per alert* action, not a *per person* action. Only one person needs to review an alert for it to be marked as reviewed in the system. If another operator reviews an alert, their review is reflected on your screen. If you mark an alert as reviewed, that action will be reflected on the screens of the other operators.

1. In the navigation bar, click **Alerts** > **Inbox**. The Inbox opens, showing all incoming alerts in the system.
2. In the **Inbox**, locate the alert whose review status you want to change. If the list is extensive, you can narrow it down by filtering for alerts that are not reviewed yet or that have been reviewed already. For details on how to filter the list, see Run an advanced search for an incoming alert.
3. Click the name of the alert. The details of the alert appear in the right pane.
4. Click **Mark as Reviewed** or **Mark as Not Reviewed** at the top of the details section.

The review status of the event is updated. Your identity and the time you made the update are recorded and displayed in the event details section below the source name field.

View details about an alert creator

1. In the navigation bar, click **Alerts** > **Inbox**. The Inbox opens, showing all incoming alerts in the system.
2. In the **Inbox**, locate the alert whose creator details you want to view.
3. Click the name of the alert. The details of the alert appear in the right pane.
4. Under the alert title, click the name of the alert creator.

If the creator is a person, the screen that opens displays the contact details of the person, any information in the system that relates to the teams, communities, and lists they belong to and their mobile app details.

If the creator is an organization, the screen that opens displays a description of the organization, the organization type, and the Website URL (if available.) The screen also displays points of contact within the organization, the address of the organization, and a map that displays where the organization is located (if appropriate.)

View live and incoming alerts on a map

For information about viewing live and incoming alerts on a map, see the *BlackBerry AtHoc Live and Publisher Maps* guide.

Update the Inbox manually

The Inbox updates automatically as new alerts are added and existing alerts are updated. Click ↻ in the top corner of the screen to manually update the contents of the Inbox.

Manage Connect requests and updates from the Inbox

You can view and respond to AtHoc Connect requests from the Inbox.

All requests, responses, and updates appear in the list and are labeled as Connect Update. Accept or Decline updates for invitations to outside organizations also appear in the Inbox.

To view invitations that you have sent to outside organizations, including the status, click **Organizations** > **Sent Invitations**.

Run a basic search for an alert

1. In the navigation bar, click **Alerts** > **Inbox**.
2. In the **Inbox**, in the search field, type or paste a word or phrase found in the alert title or alert contents.
3. Click **Search**.

Run an advanced search for an incoming alert

1. In the navigation bar, click **Alerts** > **Inbox**.

2. Optionally, in the search field, type or paste a word or phrase found in the alert title or alert contents.
3. Click **Advanced**. The search field expands to display additional search criteria.
4. Select from the criteria you want to use to find the event.
    - **Source Name**: The name of the person or organization that created the event.
    - **Alert Type**: To view a list of all available alert types, see Mobile alert types.
    - **Date**
    - **Severity**: Options include High, Moderate, Low, Informational, or Unknown.
    - **Reviewed**
    - **Pending Reply**: Select Yes or No.
    - **Status**: Select Live and Ended.
5. Click **Search**.

The screen refreshes to display the results of your search, with each of the search criteria you selected appearing as a separate pill under the search field.

Note: You can click **X** in any pill to remove it as a search criteria. If you do so, the search results field updates automatically.

Sort the Inbox

1. In the navigation bar, click **Alerts** > **Inbox**.
2. In the **Inbox**, at the top of the list, click the **Sort by** list and select one of the following options:
    - **Time**
    - **Severity**: Each incoming alert is assigned one of the following severity types: High, Moderate, Low, Informational, or Unknown. Select this option to sort the alerts by level of severity.
    - **Type**: Sorts the list by each of the available incoming alert types in the system. To view a list of the types, see Mobile alert types.
    - **Source**: Sorts the list based on the person or organization that created each incoming alert.
    - **Title**
3. Optionally, click **Ascending/Descending** next to the **Sort by** list to change the current sort order of the incoming alerts.

Export alerts from the Inbox

1. In the navigation bar, click **Alerts** > **Inbox**. The Inbox opens, displaying all incoming alerts in the system.
2. Optionally, run a basic or advanced search to filter the contents of the Inbox.
3. Click **Export to CSV**.

The .csv file downloads to your computer. The export .csv file includes the following details for each event: Event Title, Message, Timestamp, UserID, Display Name, Alert Type, Severity, Physical Address, Lat/Long address and Shape Layer Name.

Note: If multiple shapes overlap, and a user or event is in both shapes, BlackBerry Alert selects the smaller shape. The name of the smaller shape is displayed in the export .csv.

The export is recorded in the operator audit trail.

View external events in the Inbox

BlackBerry AtHoc improves emergency managers' situational awareness by providing alerts for external events that impact their organization and employees. External event categories include: Earthquake, Fire, Flood, Freeze, Heat, Hurricane, Storm, and Wind. To see the full list of supported external events, see Supported external event types.

BlackBerry AtHoc monitors external feeds and creates events that appear in the Inbox. System Administrators can enable the External Events feature in **Settings** > **Feature Enablement** in the BlackBerry AtHoc management system.

When external events are enabled, Organization Administrators can select the locations and external events to monitor. When an event occurs that impacts a selected location, it appears in the Inbox. Operators can also receive notifications on their chosen devices (email, SMS, and mobile app) when events that impact their selected locations appear in the Inbox. These notification events include a link to the event in the Inbox. In addition, when an external layer is enabled, the notification includes a link to the live map that displays the location of the event. For more information, see the *BlackBerry AtHoc External Events* guide.

External events that appear in the Inbox include the event title, description, event start time, expiration time, severity, map, and feed source (name and URL.) External events also include the event geolocation and the number of impacted users. Click the **View the Live Map...** link in the event details to open the live map. The live map opens with the triggering event type selected in the External Layers panel and the event highlighted in the event list and on the live map. After evaluating the external event and its impact, the operator can forward the event as an alert to impacted employees.

Forward an external event as an alert

You can forward external events from the Inbox in the BlackBerry AtHoc management system to users in the targeted event location.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Alerts** > **Inbox**.

   Tip: External events are marked with **Feed Service** in the Inbox.
3. In the left pane, select the external event to forward as an alert.
4. Review the details of the external event alert in the details pane.
5. Click **Forward Alert**. The following feed content is mapped to the forwarded alert: Severity, Title, Body, and Map. The Type is always Other.
6. On the **Forward Alert** page, review the alert details and make changes as needed.
7. In the **Target Users** section, click **By Advanced Query**. By default, if the forwarded alert has a selected location, all users in that location and users with a Last Known Location updated in the past 4 hours are targeted.
8. Optionally, enter a number and select **Hour(s)**, **Minute(s)**, or **Day(s)** to change the timeframe for targeting users with a Last Known Location attribute.
9. Click **Select Personal Devices** and select the personal devices to use to contact the targeted users.
10. Click **Review and Publish**.
11. Review the details of the alert.
12. Optionally, click **Preview and Publish** to preview how the forwarded alert will appear to end users.
13. Click **Publish**.

Supported external event types

The following external event types are supported:

Earthquake

- Earthquake

Fire

- Extreme Fire Danger
- Fire Warning
- Fire Weather Watch
- Red Flag Warning
- Wildfire

Flood

- Flash Flood
- Flood Advisory
- Flood Statement
- Flood Warning
- Flood Watch

Freeze

- Amber Warning Ice
- Amber Warning Snow
- Blizzard Warning
- Freeze Warning
- Freeze Watch
- Freezing Fog Advisory
- Frost Advisory
- Heavy Freezing Spray Warning
- Red Warning Ice
- Red Warning Snow
- Snow Squall Warning
- Winter Storm Watch
- Winter Weather Advisory
- Yellow Warning Ice
- Yellow Warning Snow

Heat

- Amber Warning Extreme Heat
- Excessive Heat Warning
- Excessive Heat Watch
- Heat Advisory
- Red Warning Extreme Heat
- Yellow Warning Extreme Heat

Hurricane

- Hurricane Force Wind Warning
- Hurricane Warning

- Hurricane Watch

Storm

- Amber Warning Lightning
- Amber Warning Rain
- Amber Warning Thunderstorms
- Red Warning Lightning
- Red Warning Rain
- Severe Thunderstorm Watch
- Severe Weather Warning
- Snow Squall Warning
- Storm Surge Warning
- Storm Surge Watch
- Storm Warning
- Storm Watch
- Tornado Warning
- Tornado Watch
- Tropical Cyclone Statement
- Tropical Storm Warning
- Tropical Storm Watch
- Winter Weather Advisory
- Yellow Warning Lightning
- Yellow Warning Rain
- Yellow Warning Thunderstorms

Wind

- Amber Warning Wind
- Gale Warning
- Gale Watch
- High Wind Warning
- High Wind Watch
- Red Warning Rain
- Wind Advisory
- Wind Chill Advisory
- Wind Chill Warning
- Wind Chill Watch
- Yellow Warning Wind

If you do not see the type of external event you need, you can submit a request to add it by submitting a request form at: https://www.blackberry.com/us/en/support/enterpriseapps/athoc/support-request. Include the event type and region. Include the source URL for a public feed source, when possible. For example: COVID-19, United States, https://tools.cdc.gov/api/v2/resources/media/404952.rss.

Note: RSS, Geo-JSON, CAP, and ATOM formats are supported. Each requested feed type must have consistent location data and event type information. Requested feed types should be applicable to a regional (for example U.S. West Coast), national, or international area.

Configure mobile alert settings

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

Note: To configure incoming alerts with standard types (such as geophysical, security, or fire), see Manage alert rules.

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

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

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

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

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

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

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

Mobile alert types

The following event types are available in the system:

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

Create a field report for the mobile app

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

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Mobile Alert Settings**.
3. On the **Mobile Alerts Settings** screen, on the **Event Rules** tab, click **New**.
4. On the **Event Rule details** screen, add or select values in the following fields:
    - **Title**: Enter a descriptive label that identifies the field report.
    - **Message**: Optionally, enter the default message you want to appear in the message field. This text can be edited by end users prior to them sending the field report.
    - **Icon**: Select the specific icon you want to use on maps to represent the event report.
    - **Default Severity**: Select the default severity of the field report. Severity options include High, Moderate, Low, Informational, or Unknown. End users can change the severity prior to sending the report.
    - **Run Alert Template**: Select an alert template to be published when a user sends the field report. Only alert templates that are ready to be published are displayed.
5. Click **Save**.
6. Optionally, repeat steps 3 through 5 to add additional report types that end users can access when preparing to send an event report.

Configure scheduled location access

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

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

Before you begin:

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

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Mobile Alert Settings**.
3. On the **Mobile Alert Settings** page, click **Scheduled Location Access**.
4. Click **New**.
5. On the **Schedule Location Access** screen, select a distribution list.
6. Optionally, select an **Interval**. The default is 24 hours.
7. Select one or more days of the week for the **Recurrence**. All days are selected by default.
8. From the **Start Date** and **Start Time** fields, select when to begin tracking.
9. From the **End Date** and **End Time** fields, select when to stop tracking, or select **No End Date**.

10. Optionally, select **Enforce geolocation (No Opt-out)**. If this option is selected, the end user does not receive the opt-out option on the mobile app when tracking begins.
11. Click **Save**.

Manage alert rules

Note: This section provides rules for Connect and weather alert types. To configure mobile alerts, see Configure mobile alert settings. You must have a Enterprise Administrator, System Administrator, or Basic Administrator role to access alert rules.

Alert rules help determine which alert templates to run when an alert arrives in the Inbox.

Note: For Connect alerts, the Alert Rule Manager supports a maximum 150 rules per organization.

Two connect rules are provided for your use:

- Urgent Alert Rule
- Informational Alert Rule

You can create alert rules to associate a condition and an action with an incoming alert. Each rule has one or more conditions specifying an alert attribute value, an operation, and the value of the attribute.

For example, an operator creates an alert rule for fire emergencies. The operator specifies two alert conditions for triggering an alert template:

- `Severity equals High`
- `Title contains “Fire”`

The operator then specifies the action to trigger an alert template called “Emergency: Fire” that publishes an alert to the Fire Department when the conditions are met.

View or edit alert rules

You can view the list of rules for processing alerts. You can create, edit, or delete existing rules, and define the processing order of the rules.

1. From the navigation bar, click **Alerts** or **Organization**.
2. Click **Alert Rules**. The Connect tab is open by default. To view or edit a Weather Alert rule, click the **Weather** tab.
3. Click the name of the rule that you want to view or edit.

   Important: Only alert templates that are ready are listed. Each rule has a field for the associated alert template.
4. Make changes to the rule and then click **Save**.

You can change the name and the conditions. You can also select a different alert template or change the processing actions.

Create a Connect alert rule

Add a new rule to specify what happens when a Connect alert is received in the Inbox.

1. From the navigation bar, click **Alerts** or **Organizations**.
2. Click **Alert Rules**. The Connect tab is open by default.
3. Click **New Rule**.
4. On the **New Rule** screen, in the **General** section, enter a rule name in the **Name**.
5. In the **Conditions** section, create a condition that triggers the rule:

   a. Click **Add Condition**.

  b. Select from the list of existing attributes:

     - **Severity**: The importance of the incoming alert (High, Moderate, Low, Informational or Unknown.)
     - **Source Organization**: The list of your existing connections (the organizations that can send alerts to your organization.)
     - **Title**: The title of the incoming alert.
     - **Type**: The type of alert, such as “Geophysical” or “Safety.”

     Note: In alerts triggered based on Connect rules, the severity and type is retained from the original alert. The severity and type in the selected template are overwritten.

  c. Select an operation that defines the relationship between the attribute and the value. For example, **equals** or **not equals**.

  d. Enter or select the value of the attribute, such as “Fire”.

     For example, the condition might look like the following:

     ```
     Type equals “Fire”
     ```

     Attribute values that contain multiple items are separated by commas. If one or more of the values is true, the condition is met.

6. In the **Actions** section, in the **Publish Alert** field, select an alert template to be published when the conditions of the rule are met.

   For example, if the title of the incoming alert contains the word “fire”, you might select a template called “Emergency: Fire” to publish an alert to the fire department.

7. To use the response options from the incoming alert, select **Use sender response options and return first response to sender**.

   When this option is selected, the response options from the incoming alert are copied to the triggered alert. Additionally, the first response that is received is sent to the sender of the incoming alert.

8. Select **Stop processing more rules** to prevent more rules from being processed after the current rule. This option prevents the processing of the next rule or rules that match the same incoming alert.
9. Click **Save**.

Note: When an incoming Connect or mobile app alert from a connected organization triggers another alert, any attachments in the incoming alert are not included in the triggered alert.

Configure the processing order of rules

Note: This section applies only to Connect alert rules.

More than one rule can be run on a Connect alert when it arrives in the Inbox. The rules run in the order in which they appear in the list. You can specify the order in which the rules are run, and can indicate when processing stops.

1. Using the drag icon ↕ to drag rules to the order in which they should run.
2. Ensure that the last rule has the **Stop processing more rules** check box selected.

Note: When a rule has the **Stop processing more rules** check box selected, the processing stops at that rule and others are ignored.

Create a weather alert rule

To begin processing Integrated Weather Alerts, you must create alert rules that are designed to trigger alert templates. Each weather alert rule must contain a selected county and an alert template before it can be enabled.

You must create weather alert rules for each organization you want to send integrated weather alerts from.

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Alerts** > **Alert Rules**.
3. On the **Alert Rules** page, click the **Weather** tab.
4. Click **New Rule**.
5. On the **New Rule** page, in the **General** section, enter a name for the rule and select the option to enable the rule.
6. In the **Condition** section, click **Select** beside **Counties**.
7. On the **Select Counties** window, on the **All Counties** tab, select one or more counties. You can click ⌄ **All States** to filter counties by state. You can also search for a specific zip code.
8. Optionally, click the **Selected Counties** tab to verify the counties you selected.
9. Optionally, click **Modify** to change your county selection.
10. Click **Apply**. You are returned to the New Rule page. The counties you selected appear in the Counties area.
11. Optionally, select a **Weather Severity**. The following severities are available: Extreme, Severe, Moderate, Minor, and Unknown. You can select one, multiple, or all severities.
12. Optionally, select a **Weather Type**. You can select one, multiple, or all weather types. See Weather types for the list of available weather types.
13. Optionally, select a **Message Type**. The following message types are available: Alert, Cancel, and Update. You can select one, multiple, or all message types. Select **Alert** to send an initial alert to targeted users. Select **Update** to update and replace an existing alert. Select **Cancel** to cancel an earlier alert.
14. In the **Action** section, select an alert template.
15. Optionally, select the **Override Geo Information** option. When selected, the map from the incoming weather feed overrides any map in the alert template. If the alert template has geo-targeting enabled, the alert is triggered for the location from the feed. If not selected, the map and geo-targeting from the original alert template is used in the triggered alert.
16. Click **Save**. The new weather alert rule is created and enabled by default.

One alert is generated per rule when an incoming feed matches the rule criteria. All conditions you specify must be met by a weather feed before an alert is triggered. For example, if you select Extreme for Weather Severity, and Coastal Flood Warning for Weather Type for San Mateo county, only weather feeds that are extreme severity coastal flood warnings that target San Mateo county trigger the selected alert template.

Weather types

The following weather types are available when creating a weather alert rule:

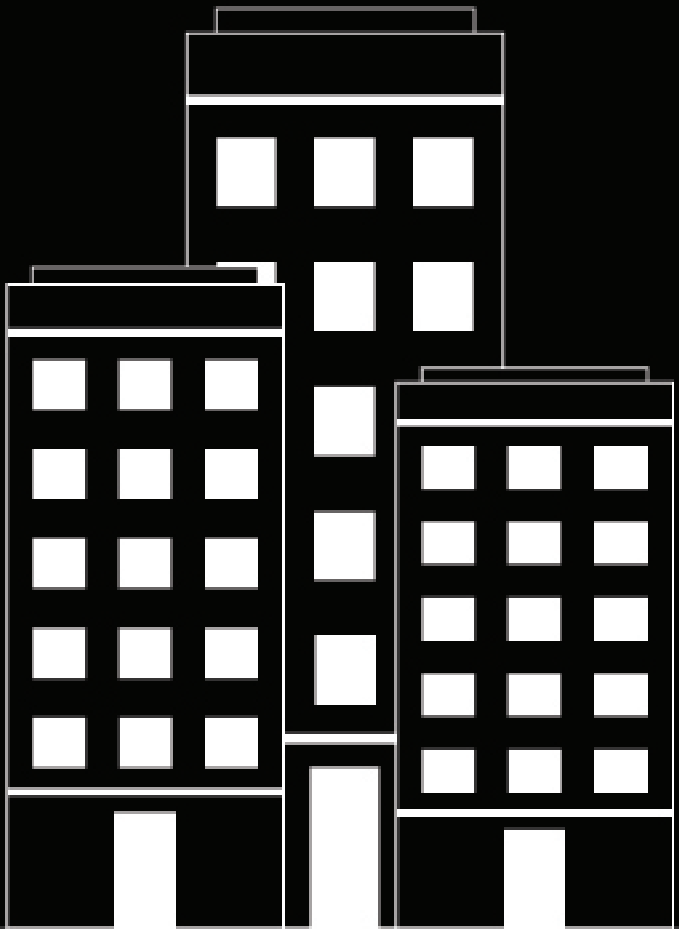
- Avalanche Warning
- Avalanche Watch
- Blizzard Warning
- Coastal Flood Warning
- Coastal Flood Watch
- Dust Storm Warning
- Earthquake Warning
- Extreme Wind Warning
- Fire Warning
- Flash Flood Statement
- Flash Flood Warning
- Flash Flood Watch
- Flood Statement
- Flood Warning
- Flood Watch
- High Wind Warning
- High Wind Watch
- Hurricane Statement
- Hurricane Warning
- Hurricane Watch
- Severe Thunderstorm Warning
- Severe Thunderstorm Watch
- Severe Weather Statement
- Snow Squall Warning
- Special Marine Warning
- Special Marine Statement
- Special Weather Statement
- Storm Surge Warning
- Storm Surge Watch
- Tornado Warning
- Tornado Watch
- Tropical Storm Warning
- Tropical Storm Watch
- Tsunami Warning
- Tsunami Watch
- Volcano Warning
- Winter Storm Watch
- Winter Storm Warning

Note: BlackBerry AtHoc supports weather types from the National Weather Service (NWS.) For more information, see https://www.weather.gov/nwr/eventcodes.

Delete an alert rule

When a rule becomes obsolete, you can delete it.

1. From the navigation bar, click **Alerts** or **Organization**.
2. Click **Alert Rules**. The Connect tab is open by default.
3. Click the **Weather** tab.
4. Select the check box next to the rule to delete. To delete all rules, click the global check box in the heading of the list.
5. Click **Delete**.
6. On the **Delete Weather Alert Rules** dialog, click **Delete**.



BlackBerry AtHoc

Live and Publisher Maps

7.16

Contents

Overview

BlackBerry® AtHoc® provides two types of maps; the publisher map and the live map. The publisher map is the map that appears when creating alerts or events. Use the publisher map to target users in a defined location and to define and communicate the affected area for an alert or event. Use the live map to view live alerts and events, incoming alerts, users, and external feeds. You can select an imported shape or draw a shape on the live map and send a quick alert to users in the shape.

Manage map settings

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

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

Tip: On the live map, you can also click ⚙ to access the map settings.

Shape layers

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

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

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

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

Only shape files that contain polygons and multipolygons can be imported. If your shape file contains point or polyline data, the file cannot be imported. If you need to display points on a map, you should use an external third party tool to create a polygon buffer around each point, and then import the buffer polygons.

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

- Well-known ID: 4326
- Name: GCS_WGS_1984
- GCS Data

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

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

Add a shape layer

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

   If your shape file cannot be loaded, validate your shape file using QGIS.

4. Select a shape layer name from the **Shape Display Name** pull-down menu. The values in this menu are attributes in the shape file that can be used as the shape display name when the shape layer is displayed on the map.
5. In the **Name** field, enter a name for the shape layer.
6. Optionally, select the check box to make the new shape selectable.

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

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

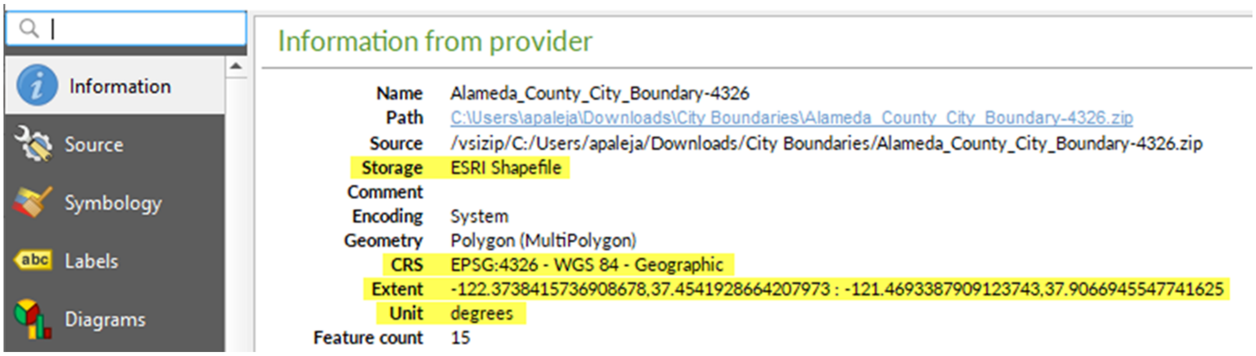
   Go to **Settings** > **User Attributes** > **Page Layout** to update the new attribute so that it is visible in user profiles. When the attribute is visible, users can subscribe to it as a location of interest from Self Service or in their user profile in the BlackBerry AtHoc management system. Users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

Validate your shape file using QGIS

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

1. Open QGIS.
2. Click **Layers** > **Add Layer** > **Add Vector Layer**.
3. Click **Source** and select the shape file or zipped shape file. The shape .zip file must contain the .shp, .dbf, and .prj files. The shape .zip file can also contain a .shx file that is used to increase the performance of the shape file, but it is not required. If the shape .zip file does not include the required files, the import stops and an error is displayed.
4. Select **file** for Source Type.
5. Select **UTF-8** for encoding.
6. Click **Add**.
7. Click **Layers**.
8. Right-click the new layer.
9. In the menu that appears, click **Properties**.
10. Click **Information**.
11. In the **Information from provider** section, verify the following values:
    - Storage: ESRI Shapefile

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



Information from provider

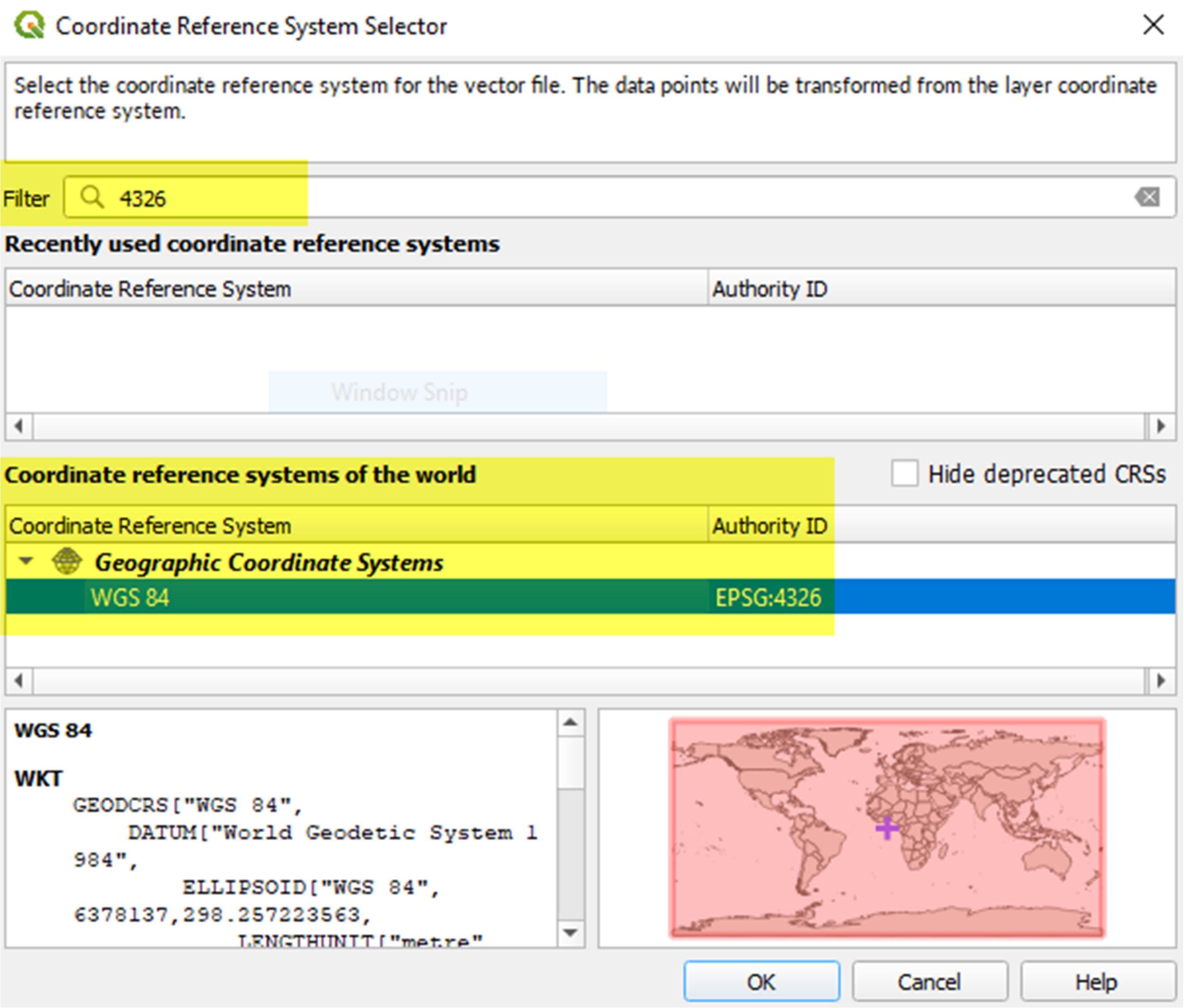
Name	Alameda_County_City_Boundary-4326
Path	C:\Users\apaleja\Downloads\City Boundaries\Alameda_County_City_Boundary-4326.zip
Source	/vsizip/C:/Users/apaleja/Downloads/City Boundaries/Alameda_County_City_Boundary-4326.zip
Storage	ESRI Shapefile
Comment	
Encoding	System
Geometry	Polygon (MultiPolygon)
CRS	EPSG:4326 - WGS 84 - Geographic
Extent	-122.3738415736908678,37.4541928664207973 : -121.4693387909123743,37.9066945547741625
Unit	degrees
Feature count	15

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

Convert projection of shape file using QGIS

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

1. Open QGIS.
2. Click **Layers** > **Add Layer** > **Add Vector Layer**.
3. Click **Source** and select the shape file or zipped shape file. The shape .zip file must contain the .shp, .dbf, and .prj files. The shape .zip file can also contain a .shx file that is used to increase the performance of the shape file. The .shx file is not required. If the shape .zip file does not include the required files, the import stops and an error is displayed.
4. Select **file** for Source Type.
5. Select **UTF-8** for encoding.
6. Click **Add**.
7. Click **Layers**.
8. Right-click the new layer.
9. Click **Export** > **Save Features As...**.
10. On the **Save Vector Layer as...** window, click **Browse**.
11. Navigate to the correct folder and specify the name of the new layer.
12. In the **Coordinate Reference System** section, click 🌐.
13. In the **CRS Selector** window, in the **Filter** field, enter **3426**.
14. From the search results list, select **WGS 84**. The Authority ID is **EPSG:4326**.
15. Click **OK**.
16. Compare the old and new projections of the layer and verify that they are in two different CRS but still overlap.



Coordinate Reference System Selector

Select the coordinate reference system for the vector file. The data points will be transformed from the layer coordinate reference system.

Filter 4326

Recently used coordinate reference systems

Coordinate Reference System	Authority ID

Coordinate reference systems of the world □ Hide deprecated CRSs

Coordinate Reference System	Authority ID
Geographic Coordinate Systems	
WGS 84	EPSG:4326

WGS 84

WKT

```
    GEODCRS["WGS 84",
        DATUM["World Geodetic System 1
    984",
            ELLIPSOID["WGS 84",
    6378137,298.257223563,
                LENGTHUNIT["metre"
```

External layers

The External Layers section of the Map Settings screen displays details about the external layers that appear on the live map.

The following types of external layers can be added: Feature, Image, and KML.

External layers update automatically on the live map when data from the source feed are updated.

Note: Data for external layers are obtained from the layer source. BlackBerry AtHoc does not modify or verify the accuracy of this data. If there is no source data for a selected external layer, no data appears on the live map. Go to the data source to verify that the feed has data.

You can add up to 30 external layers.

1. On the **Map Settings** screen, in the **External Layers** section, click **Add External Layer**.
2. On the **Add External Layer** dialog, in the **URL** field, enter a URL for the external layer. The read-only Layer Type field is populated automatically.
3. In the **Name** field, enter a name for the external layer. The name must be unique.
4. Click **Add**. You are returned to the Map Settings screen.

5. Optionally, click and drag ⇕ to change the order of the external layers. This order determines the display order of the external layers on the External Layers panel on the live map.
6. Optionally, click ✖ to remove an external layer.
7. Click **Save**.

The following external layers are available out of the box:

External layer name	**URL**
Floods – NDFD Rainfall Total Forecast	https://services9.arcgis.com/RHVPKKiFTONKtxq3/arcgis/rest/services/NDFD_Precipitation_v1/FeatureServer/2
Floods – Live Stream Gauges	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Live_Stream_Gauges_v1/FeatureServer/0
Floods – USA Flood Hazard Area	https://services.arcgis.com/P3ePLMYs2RVChkJx/ArcGIS/rest/services/USA_Flood_Hazard_Reduced_Set_gdb/FeatureServer/0
Hurricanes - Forecast Position	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/0
Hurricanes – Observed Position	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/1
Hurricanes – Forecast Track	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/2
Hurricanes – Observed Track	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/3
Hurricanes – Forecast Error Cone	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/4
Hurricanes – Watches and Warnings	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/5
Hurricanes – Hurricane Force	https://services9.arcgis.com/RHVPKKiFTONKtxq3/ArcGIS/rest/services/Active_Hurricanes_v1/FeatureServer/9

Distribution list layers

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

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

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

Configuration and Setup

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

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

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

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

1. On the **Map Settings** screen, in the **Configuration and Setup** section, click ✎ in the **Default Map View and Organizational Areas** section. An editable map screen opens.
2. Optionally, do any of the following:

   - Click 🗺 to select the type of map to display by default.
   - Click 👥 to display users from distribution lists on the map. You can select to display up to ten distribution lists.
   - Click ◈ to choose the layers to display on the map. You can select whether to view:
     - Live accountability events
     - Accountability events from suborganizations
     - Live sent alerts
     - Live incoming alerts
     - Shape layers
     - Organizations
   - In the **Find a place** field, enter an address and press **Enter** on your keyboard to zoom to that location on the map.

    Note: The location on the map you zoom to is configured as the default map view and organizational area. The default map view is displayed on the live and publisher maps and in the Recently Received Alerts section on the BlackBerry AtHoc management system home page.

3. Optionally, to select your organizational area for external events, do the following:

    - Click **Create Custom Locations**, and then select a shape from the shapes panel. Click and drag on the map to draw the shape.
    - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

    Note: You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
4. Click ↻ to refresh the map and review your changes.
5. Click **Apply**.
6. On the **Map Settings** screen, click **Save**.

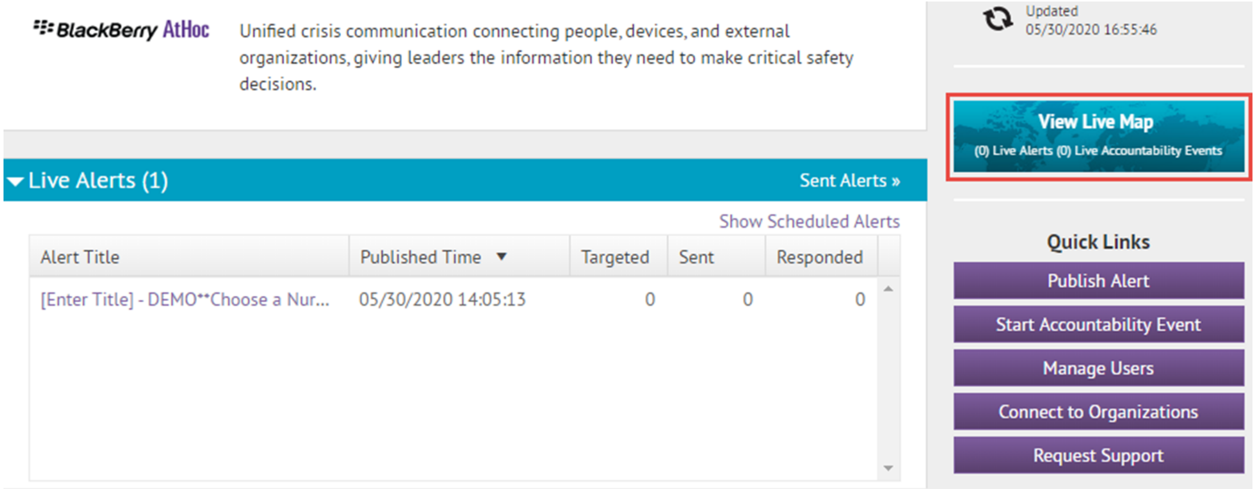
Live map

The live map displays live alerts and events, incoming alerts, external feeds, and users. You can select an imported shape layer or draw a shape on the live map and send a quick alert to users found in the shape.

Note: The live map is not supported on the Internet Explorer browser.

To view the live map, do any of the following:

- Click **View Live Map** on the BlackBerry AtHoc homepage:



BlackBerry AtHoc Unified crisis communication connecting people, devices, and external organizations, giving leaders the information they need to make critical safety decisions.

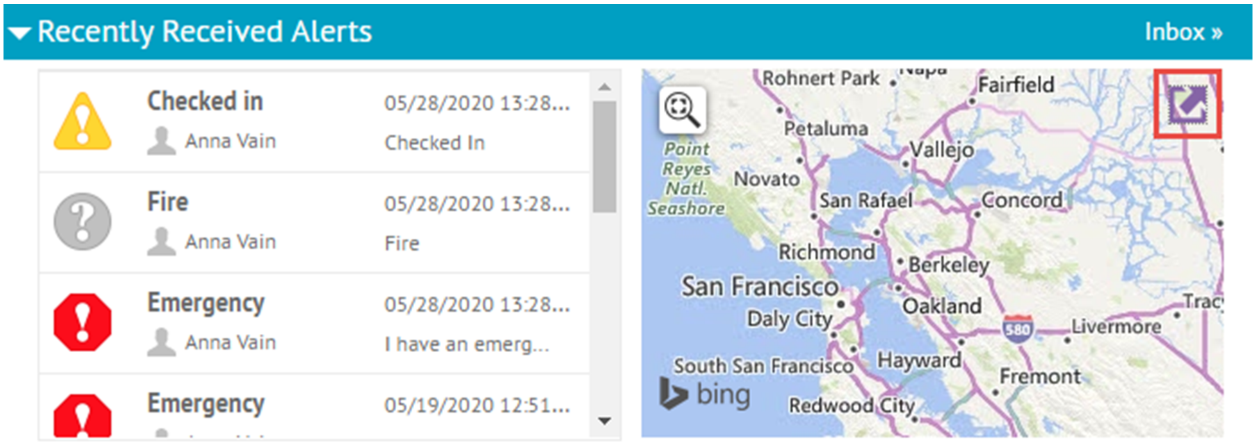
Updated 05/30/2020 16:55:46

Live Alerts (1) Sent Alerts »

Show Scheduled Alerts

Alert Title	Published Time ▼	Targeted	Sent	Responded
[Enter Title] - DEMO**Choose a Nur...	05/30/2020 14:05:13	0	0	0

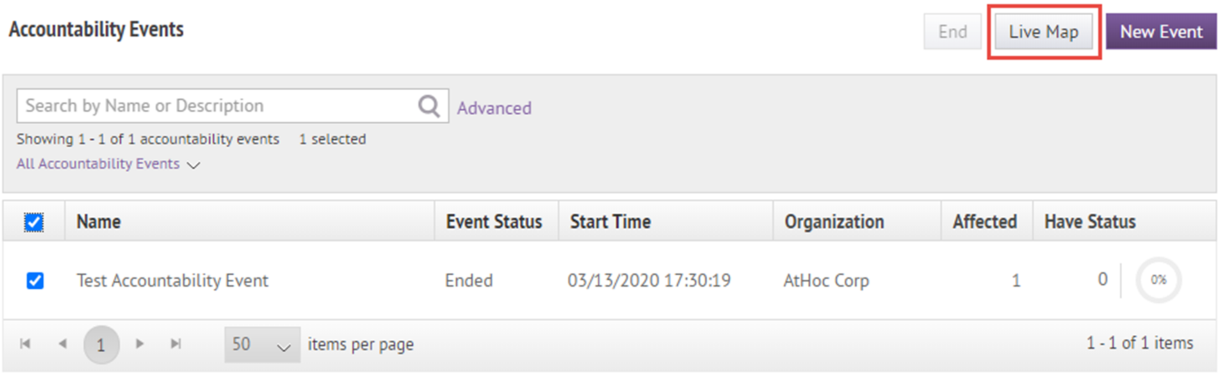
- Click ✎ in the **Recently Received Alerts** section on the BlackBerry AtHoc homepage:



Recently Received Alerts Inbox »

Checked in	05/28/2020 13:28...	
Anna Vain	Checked In	
Fire	05/28/2020 13:28...	
Anna Vain	Fire	
Emergency	05/28/2020 13:28...	
Anna Vain	I have an emerg...	
Emergency	05/19/2020 12:51...	

- Click **Live Map** on the Accountability Events page:



Showing 1 - 1 of 1 accountability events 1 selected

☑	Name	Event Status	Start Time	Organization	Affected	Have Status
☑	Test Accountability Event	Ended	03/13/2020 17:30:19	AtHoc Corp	1	0 0%

1 - 1 of 1 items

Map controls

The following control options are available on the live map:

- : Basemap Layers panel: Select the type of map you want to view.
- : BlackBerry AtHoc Layers panel: BlackBerry AtHoc layers include accountability events from enterprise and suborganizations, live sent alerts, live incoming alerts, and connected organizations. Live incoming alerts include Connect alerts and the following alerts from the mobile app:
    - Emergency
    - Check-in
    - Check-out
    - Report

  Select the check box beside an item to display it on the map. Click the name of a displayed item in the panel to zoom the map to its location.
- : Imported Shape Layers panel: Imported shape layers are also known as predefined zones. Select the check box beside an imported layer or shape file to display it on the map. Click the name of a displayed item in the panel to zoom the map to its location.
- : External Layers panel: Displays alerts from public external feeds.
    - ⌄ and ⌃: Expand or collapse the External Layers and External Events sections in the External Layers panel.
    - External Layers section:
        - : Adjust the transparency of an event layer on the live map.
        - : View the source of an external layer. Depending on the type of layer, the source will open in a new tab on your browser or will download a file to your computer.
    - External Events section:
        - and : Hide or show an external event on the live map.
        - : Zoom to a specific external event.
- : Distribution List Layers panel: Displays users from distribution lists. Click a selected distribution list to zoom the map out to display all users in the distribution list.
- **Find address or place** : Enter an address and press **Enter** on your keyboard to move the map view to that location. Click the **Find address or place** field to open the **Use current location** field. Click this field to move the map to your current location.
- : Close an open panel.

- ▣: Dock an open details pop-up to the right side of the screen.
- ⧉: Undock an open details pop-up.
- ⊕: Open the User Action panel.
- ⚙: Open the Map Settings screen in the BlackBerry AtHoc management system.
- **Shape Toolbox** :
  - ▣: Draw a polygon on the map.
  - □: Draw a rectangle on the map.
  - ○: Draw a circle on the map.
  - ▱: Draw a freehand polygon on the map.
  - ◉: Select or deselect an imported shape layer on the map.
  - 🗑: Delete a drawn shape from the map.
- +: Zoom in.
- ⌂: Move to the default view.
- −: Zoom out.
- ⟳: Refresh the map. The map updates automatically every sixty seconds.
- ≡: Display a legend for a selected external layer.
- ●○○: Switch to view the legend of another selected external layer.
- «: Close the Legend panel.

Change the map type

To change the map style displayed on the live map, click 🗺 in the top navigation bar. In the Basemap Layers panel, click to select the map you want to use. The following map types are available:

- **Bing Road**: Microsoft's standard drawing map with streets and major landmarks labeled.
- **Bing Aerial**: Microsoft's standard aerial photograph of the map area.
- **Imagery**: Aerial photograph of the map area.
- **Imagery Hybrid**: Aerial photograph of the map area with major landmarks labeled.
- **Streets**: Traditional drawing map with streets labeled.
- **Navigation**: Custom drawing map with streets and major landmarks labeled.
- **Dark Gray Canvas**: Dark drawing map with bodies of water, cities, and roads labeled.
- **Light Gray Canvas**: Light drawing map with bodies of water, cities, and roads labeled.
- **National Geographic Style**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Navigation (Dark Mode)**: Custom drawing map in dark mode with streets and major landmarks labeled.
- **Oceans**: Traditional drawing map with topographical land features displayed and underwater topography labeled.
- **OpenStreetMap**: Traditional drawing map with streets and major landmarks labeled.
- **Streets (Night)**: Traditional drawing map in night mode with streets labeled.
- **Terrain with Labels**: Traditional drawing map with topographical features displayed and cities and major roads labeled.
- **Topographic**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.

Note: OpenStreetMap is provided by OpenStreetMap (www.openstreetmap.org.) All other map types, except for Bing maps, are provided by ESRI (www.esri.com.)

Select external event types

When external events are enabled, you can define the locations and select the types of external events to monitor. When an external event occurs that impacts a selected location, it appears on the live map.

Before you begin:

- IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement**.
- You must be an Organization Administrator to select external event types.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **External Events**.
3. On the **External Events** screen, in the **Your Organizational Area** section, click ✎.

   If a default location has been set in the Map Settings, this location is displayed.
4. On the map, do any of the following:

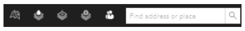
   - Click **Create Custom Locations**, and then select a shape. Click and drag on the map to draw a shape.
   - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

   You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
5. Click **Apply**.
6. In the **External Event Types** section, select the types of external events to view on the live map.

   If the external event type you need is not listed, you can submit a request to add it. Go to the BlackBerry AtHoc support portal at: https://www.blackberry.com/us/en/support/enterpriseapps/athoc/support-request. Include the Event Type keyword and region in the support request form. If available, provide the external event feed source. For example: COVID-19, United States, https://tools.cdc.gov/api/v2/resources/media/404952.rss.
7. Optionally, to send notifications to an operator when an external event occurs in the selected organizational area:
   a) In the **Setup Admin Notifications** section, click **Select Targets**.
   b) On the **Users** dialog, select the operators to notify when an external event occurs in the selected organizational areas. All external events that impact the organizational area appear on the live map. The operators you select will receive an alert about the event on the selected devices.
   c) Click **Apply**.
   d) From the **Devices** pull-down menu, select the devices (email, SMS, and mobile app) that the targeted operators will receive notifications on. You can select more than one device.
   e) From the **Frequency** pull-down menu, select the interval to send the event notifications at. Choose **24 Hrs** or **48 Hrs**. One notification is sent for each event category. For example, Earthquake.
8. Click **Save**.

View layers on the live map

To view layers on the live map, click the layer icons in the top navigation bar to open the layer panels:



In a layer panel, select the check box beside a layer to display it on the map. When a check box is selected, the name of the selected layer updates to include the number of items that are displayed on the map for the layer. Double-click the name of a selected layer to zoom the map to display the items in the layer.

You can view multiple layers at the same time. Layers on the live map are read-only.

The live map contains the following layer panels:

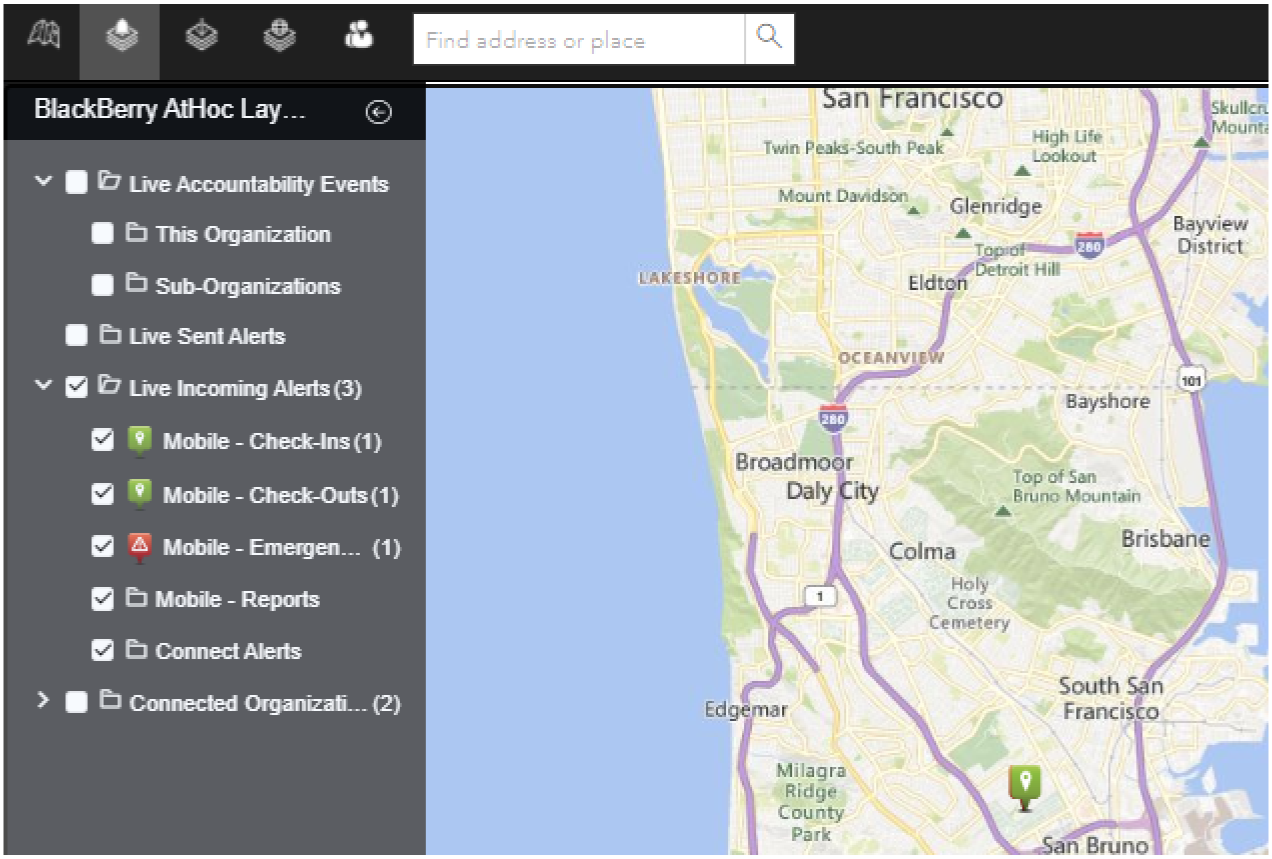
- : Basemap Layers. Select the type of map to display. For more information, see Change the map type.
- : BlackBerry AtHoc Layers.
  - **Live Accountability Events**: For more information, see View live alerts and events on the live map.
  - **Live Sent Alerts**: For more information, see View live alerts and events on the live map.
  - **Live Incoming Alerts**: This layer displays alerts from the mobile app and Connect alerts. For more information, see View incoming alerts on the live map.
  - **Connected Organizations**: This layer appears only when the Connect feature is enabled and there are connected organizations. To view the details for a connected organization, click the icon on the map.
- : Imported Shape Layers. Imported shape layers are added in the Map Settings page in the BlackBerry AtHoc management system. For more information, see Add a shape layer. Imported shape layers can be selected for alert targeting on the live map.
- : External Layers. External layers are layers from public feeds such as FEMA weather maps or ArcGIS. For more information, see View external layers on the live map.
- : Distribution List Layers. For more information, see View users on the live map.

View incoming alerts on the live map

Incoming alerts are alerts from the mobile app (check-ins, check-outs, emergencies, and reports) and from connected organizations. To view details about an incoming alert, click the corresponding alert icon on the map.

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

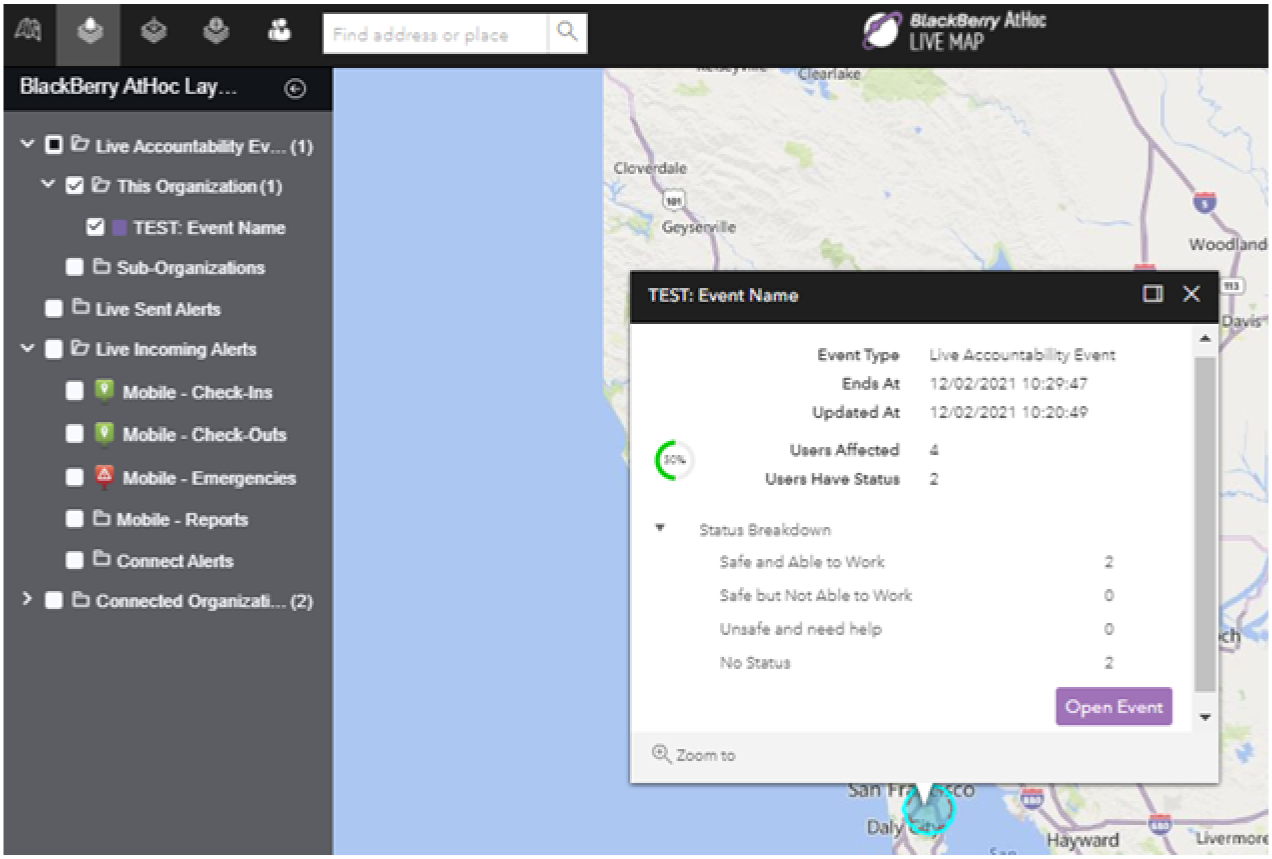
1. Click in the top navigation bar to open the BlackBerry AtHoc Layers panel.
2. On the **BlackBerry AtHoc Layers** panel, select the check box beside **Live Incoming Alerts** to display all incoming alerts on the map. You can also select individual alerts. When a check box is selected, the name of the selected incoming alert updates to include the number of alerts displayed on the map. You can select multiple incoming alerts.



BlackBerry AtHoc Lay...

- ☐ Live Accountability Events
  - ☐ This Organization
  - ☐ Sub-Organizations
- ☐ Live Sent Alerts
- ☑ Live Incoming Alerts (3)
  - ☑ Mobile - Check-Ins (1)
  - ☑ Mobile - Check-Outs (1)
  - ☑ Mobile - Emergen... (1)
  - ☑ Mobile - Reports
  - ☑ Connect Alerts
- ☐ Connected Organizati... (2)

3. Optionally, click the name of a selected incoming alert to zoom the map to display it.
4. Click the icon of the alert you want to view. The following information is displayed in the alert details pop-up:
   - Severity icon
   - Alert type
   - User display name
   - Date and timestamp
   - Sent location in latitude,longitude
5. Optionally, on the alert details pop-up, click **Zoom to** to move the map focus to the alert location.



BlackBerry AtHoc Lay...

- □ Live Accountability Ev... (1)
  - ☑ This Organization (1)
    - ☑ TEST: Event Name
  - □ Sub-Organizations
- □ Live Sent Alerts
- □ Live Incoming Alerts
  - □ Mobile - Check-Ins
  - □ Mobile - Check-Outs
  - □ Mobile - Emergencies
  - □ Mobile - Reports
  - □ Connect Alerts
- □ Connected Organizati... (2)

TEST: Event Name

Event Type Live Accountability Event
Ends At 12/02/2021 10:29:47
Updated At 12/02/2021 10:20:49
50% Users Affected 4
Users Have Status 2

Status Breakdown

Safe and Able to Work	2
Safe but Not Able to Work	0
Unsafe and need help	0
No Status	2

Open Event

Zoom to

6. Optionally, click ◘ to dock the alert or event pop-up to the right side of the map.

View live alerts and events on the live map

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

The live 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.

1. Click ◘ in the top navigation bar to open the BlackBerry AtHoc Layers panel.
2. On the **BlackBerry AtHoc Layers** panel, select the check box beside **Live Accountability Events** or **Live Sent Alerts** to display live alerts and events on the map. You can also select individual events and alerts. You can select multiple live events and alerts.
3. Click an event or alert on the map to open a pop-up window that displays detailed information for the live event or alert.

   The following information is displayed:

   - Name of the event or alert
   - Severity icon
   - Type of item: accountability event or alert
   - Organization name (for events from suborganizations)
   - Time the live alert or event ends
   - Last updated date and time
   - GPS coordinates in latitude,longitude (for incoming mobile alerts only)
   - Number of affected users
   - Number and percentage of users with a status

- Summary of user statuses by response option

4. Optionally, in an event pop-up, click **Open Event** to go to the Summary tab of the event in the event manager.
5. Optionally, in an alert pop-up, click **Open Alert** to go to the Users tab of the alert in the Sent Alerts screen.
6. Optionally, in an alert pop-up, click to expand **Response Breakdown** to view the number of responses.
7. Optionally, in an event pop-up, click to expand **Status Breakdown** to view the number of responses.
8. Optionally, click ▣ to dock the alert or event pop-up to the right side of the map.
9. Optionally, on the pop-up, click **Zoom to** to move the map focus to the alert or event location.
10. If there are multiple events or alerts in the same location on the map, click ▶ to scroll through the details for each alert or event.

View imported shape layers on the live map

Imported shape layers are also known as predefined zones. For more information, see Shape layers.

1. Click ◈ in the top navigation bar to open the Imported Shape Layers panel.
2. On the **Imported Shape Layers** panel, select the check box beside an imported shape layer to display it on the map.
3. Optionally, double-click the name of a selected imported shape layer to zoom the map to display it.

View external layers on the live map

External layers are layers from public sources such as FEMA, weather maps, or ArcGIS.

The External Layers section in the External Layers panel on the live map displays the external layers that are configured in Map Settings. For more information, see External layers.

Note: The data displayed for external layers are obtained from external sources. BlackBerry AtHoc does not modify or validate this data. If a selected external layer has no data from the external feed, no icons or shapes appear on the live map.

1. Click ◈ in the top navigation bar to open the External Layers panel.
2. On the **External Layers** panel, click ▼ to expand the **External Layers** section.
3. Select the check box beside a layer to display it on the map.
4. Optionally, click ▼ > 💧 **Transparency** to open the Layer Transparency slider and change the transparency of the layer.
5. Optionally, click ▼ > 🗀 **Source** to view the feed source. For KML layer types, a feed source file downloads to your computer. For other types of feeds, the feed source opens in a new tab on your browser.
6. Optionally, in the middle pane, click ≡ to display a legend that provides graphical information about the layer. The displayed legend information is obtained from the source of the layer. If a layer has no legend information, clicking the ≡ opens the Legend panel, but no data is displayed. You can display multiple legends. If multiple legends are selected, click ●○○ to switch between them on the Legend panel. Click « to close the Legend panel. Legends are supported only for Feature and Image layer types. KML type layers do not support displaying a legend.
7. Optionally, click the name of a selected external layer to zoom the map to display it.
8. Optionally, click the icon or shape for an external layer item on the map to open a details pop-up.
9. Optionally, on an external layer shape details pop-up, click **Zoom to** to move the map focus to the external layer shape location.
10. Optionally, click ▣ to dock the external layer shape pop-up to the right side of the map.

View external events on the live map

The External Events section of the External Layers panel on the live map displays the external events that are configured in the External Events settings. For more information, see Select external event types.

Note: IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement** for external events to be visible on the live map.

1. Click in the top navigation bar to open the External Layers panel.
2. On the **External Layers** panel, click to expand the **External Events** section.
3. In the **Event Types** section, select the event types to display from the pull-down list.
4. Optionally, in the **Time Filter** section, from the pull-down list, select the time period to display on the map. You can select from 30 minutes to 72 hours. The default is 2 hours. External events that occur in the selected time period are displayed under the Time Filter pull-down list and appear on the map. The severity and the time elapsed since the event occurred are displayed.
5. Optionally, in the **External Events** section, do any of the following:
    - Click an external event to highlight it in the panel. The shape associated with the event is highlighted on the map.
    - Click to hide an event on the map.
    - Click to display a hidden event.
    - Click to zoom the map to an event.
    - Select or deselect the **Show All** option to display or hide all events on the map. All events are displayed on the map by default.
6. Optionally, click an event on the map to display a pop-up with details about the event. The details pop-up includes the following information about the event:
    - Title
    - Source
    - Severity
    - Event Type
    - The date and time the event was published.
    - Description. This description is from the original feed source and is not modified by BlackBerry AtHoc.
    - The number of users who are impacted by the event, based on their geolocation.
7. Optionally, click to dock the external event pop-up to the right side of the map.

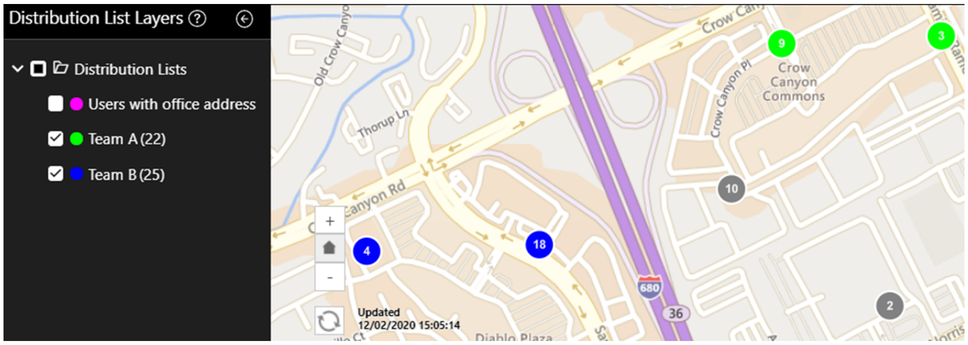
External events data are refreshed on the live map every 5 minutes. Click to refresh external events data manually.

View users on the live map

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

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

1. Click in the top navigation bar to open the Distribution List Layers panel. Distribution lists that are selected in the BlackBerry AtHoc management system under **Settings** > **Map Settings** appear on the panel. For more information, see Distribution list layers.
2. On the **Distribution List Layers** panel, select the check box beside a distribution list layer to display it on the map. When a check box is selected, the name of the selected distribution list updates to include the number of users that are displayed on the map for the distribution list. You can select multiple distribution lists.
3. Optionally, click the name of a selected distribution list to zoom the map to display the users in the distribution list on the map. The number of users is displayed in a circle with a color that matches the color designated for the distribution list.

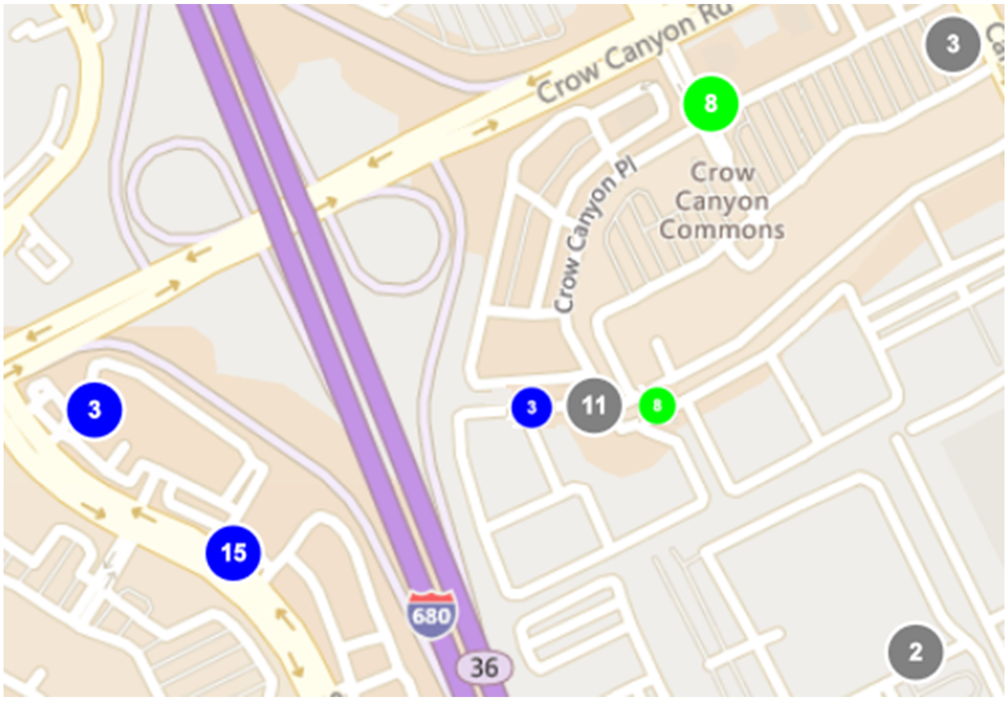


Distribution List Layers ⓘ

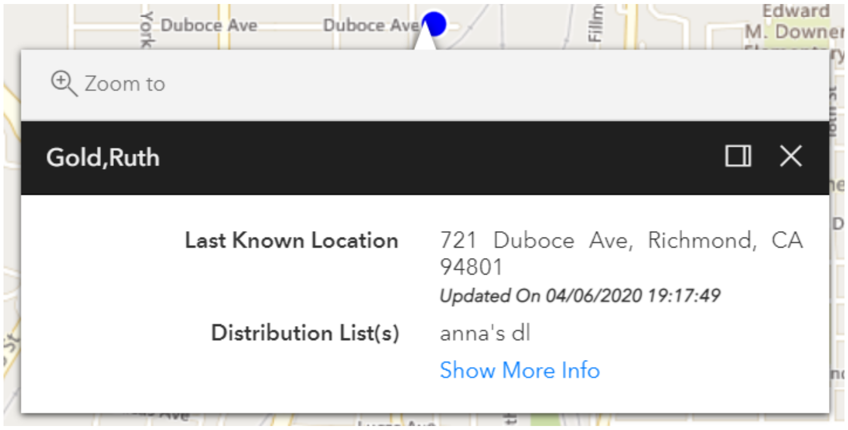
- □ Distribution Lists
  - □ ● Users with office address
  - ☑ ● Team A (22)
  - ☑ ● Team B (25)

Updated
12/02/2020 15:05:14

4. When users from different selected distribution lists are in the same location, they are displayed in a grey circle. Only unique users are displayed in the count. If the same user is a member of multiple distribution lists, they are counted as one user in the grey circle. Click a grey circle to display separate circles that have users from the selected distribution lists:



5. Optionally, click a circle to open the user details pop-up. The user details pop-up displays the last known location and distribution list membership for a user. The last known location includes a timestamp of when the user's location was last updated.



Zoom to

Gold,Ruth

Last Known Location 721 Duboce Ave, Richmond, CA 94801
Updated On 04/06/2020 19:17:49

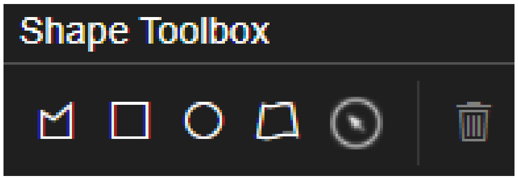
Distribution List(s) anna's dl
Show More Info

6. Optionally, click **Show More Info** to display the attributes, groups, and devices for the user. The details of the user pop-up can be configured in **Settings** > **General Settings** > **Layouts** > **User Details - Popup View**.
7. Optionally, click ◫ to dock the user details pop-up to the right side of the map.
8. Optionally, click **Zoom to** to move the map view to the user.
9. Optionally, click ▶ to display the details for the next user.

   The ▶ icon appears only when more than one user is displayed in the selected location.
10. Optionally, select the **Dynamic Map Zoom** option to keep the map focus on selected groups or individual users.

View users in drawn shapes

Operators with alert publishing permissions can use the Shape Toolbox on the live map to draw shapes, view the number of users in the shape, and target them in alerts. Click a shape button on the Shape Toolbox panel and click and drag on the screen to draw a shape on the live map.



As you create shapes on the live map, the number of unique users in that area are displayed in the center of the shape. If you move the shape to another location on the map, the number of users is recalculated. If you are accessing the live map from an enterprise organization, the number of users displayed in the shape includes users in the enterprise and its suborganizations.

You can draw multiple shapes on the live map.

Click and drag a shape to move it. To edit a shape, click the shape and then click and drag on any of the circles that appear around the edge of the shape. To delete a shape, select it and click 🗑 or press **Delete** on your keyboard.

When you draw a shape on the map, the User Action panel opens. The Users tab of the User Actions panel displays the number of unique users found in the shapes drawn on the map. The number of available users (◉) and blocked users (⊘) that are available for alert targeting are displayed. Organizations with users in the drawn shapes are displayed in the Organization Filters section. If there is an enterprise organization and suborganizations, the enterprise organization is listed first.

Select filters in the Organization Filters, Attribute Filters, and Shape Selection by Layer sections to filter the targeted users in the drawn shapes by organization or geolocation attribute. All geolocation attributes for an organization are available as filters. You can filter users by a timeframe of when their Last Known Location attribute was last updated. Select the number of minutes, hours, or days.

As you select filters, the number of targetable users updates automatically. Click the x **Users** link to view the list of targeted and blocked users. On the **User Selections** dialog you can:

- Use the **Search** field to find specific users.
- Select **Blocked users** or **Targeted users** from the **All users** pull-down list to filter the targeted users.
- Block or unblock individual users.

Click **Apply** to save and view the updated user selections.

After you have selected your targeted and blocked users, you can Export users from the User Action panel or Publish a quick alert from the live map.

Publish a quick alert from the live map

Operators with alert publishing permissions can target users and send them alerts from the live map by drawing a shape or selecting an imported shape layer.

1. In the **Shape Toolbox**, do any of the following:

    - Click a shape and then draw a shape on the map.
    - Click in the top navigation bar to open the Imported Shape Layers panel and then select the check box beside an imported shape layer to display it on the map. Click and then click the imported shape layer on the map.

    Note: You can select multiple custom shapes and imported shape layers on the map.

    When you create a custom shape or select an imported shape layer, the **User Action Panel** opens.
2. On the **User Action Panel**, on the **Users** tab, select or deselect organization, attribute, and shape selection by layer filters. For more information, see View users in drawn shapes and View imported shape layers on the live map.
3. Optionally, click the x **Users** link to open the **User Selections** dialog and view and select blocked and unblocked users. Click **Apply**.
4. Click the **Quick Alert** tab.
5. From the **Select Alert Template** list, select a template. Alert templates must have location enabled in alert template settings and must have the "Available for quick publish" option enabled to be available for publishing.
6. Optionally, update the **Title** and **Body** fields.

    Tip: Click to open the Alert Content dialog where you can edit the Title and Body fields. Click **Apply** to save your changes.
7. In the **Personal Devices** section, select all or select individual devices to use to send the alert to the targeted users.
8. Optionally, click the x **Users** link to view and update the list of targeted and blocked users. For more information, see View users in drawn shapes.
9. Optionally, click the x **Reachable Users** link to open the **Reachable Users** dialog and view the reachable users.
10. Click **Refresh** to update the list of targeted users.
11. Click **Publish**.
12. Optionally, click **View Report** to view the details of the sent alert.

The sent alert includes a map that displays the targeted location. For alerts delivered to email and the desktop app, the map is an image. For alerts delivered to the BlackBerry AtHoc mobile app, an interactive map is included. If the alert template used to send the alert includes a map, it is overwritten with the map of the targeted location.

The published alert appears in Live Sent Alerts in the BlackBerry AtHoc Layers panel on the live map. Details about the quick alert can be viewed in the Sent Alerts page in the BlackBerry AtHoc management system.

Export users from the User Action panel

1. Click a shape in the **Shape Toolbox** dialog and draw a shape on the map.
2. On the **User Action** panel, click the **Users** tab.
3. Optionally, click the *x* **Users** link to open the **User Selections** panel and do any of the following:
   - Use the **Search** field to find specific users.
   - Select **Blocked users** or **Targeted users** from the **All users** pull-down list to filter the targeted users.
   - Block or unblock specific users.

   Click **Apply**.
4. Optionally, in the **Organization Filters** section, click ☒ to remove users from a specific organization from the export .csv file.
5. Optionally, in the **Attribute Filters** section, deselect users from any of the attribute filters to exclude them from the export .csv file.
6. Optionally, in the **Attribute Filters** section, filter users based on when their Last Known Location attribute was last updated. Select **Minutes**, **Hours**, or **Days** from the pull-down menu, and enter a number.
7. Click **Export CSV**.

A .csv file with the selected targeted users downloads to your local system. The columns included in the .csv are defined in the user details pop-up view layout. To view or modify the user details pop-up view layout click ⚙ > **General Settings** > **Layouts** > **User Details - Popup View**.

Publisher map

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

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

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

Map controls

The following control options are available on the publisher map:

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

Change the map type

To change the map style in an alert or alert template, click 🗺 in the bottom left corner of the screen and then click to select the map you want to use. Available map types include the following:

- **Bing Road**: Microsoft's standard drawing map with streets and major landmarks labeled.
- **Bing Aerial**: Microsoft's standard aerial photograph of the map area.
- **Imagery**: Aerial photograph of the map area.
- **Imagery with Labels**: Aerial photograph of the map area with major landmarks labeled.
- **Streets**: Traditional drawing map with streets and major landmarks labeled.
- **Topographic**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Dark Gray Canvas**: Dark drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.
- **Light Gray Canvas**: Light drawing map with bodies of water and cities labeled. Roads are shown but are not labeled.

- **National Geographic**: Traditional drawing map with topographical features displayed and streets and major landmarks labeled.
- **Oceans**: Traditional drawing map with topographical land features displayed and underwater topography labeled.
- **Terrain with Labels**: Traditional drawing map with topographical features displayed and cities and major roads labeled.
- **OpenStreetMap**: Traditional drawing map with streets and major landmarks labeled.

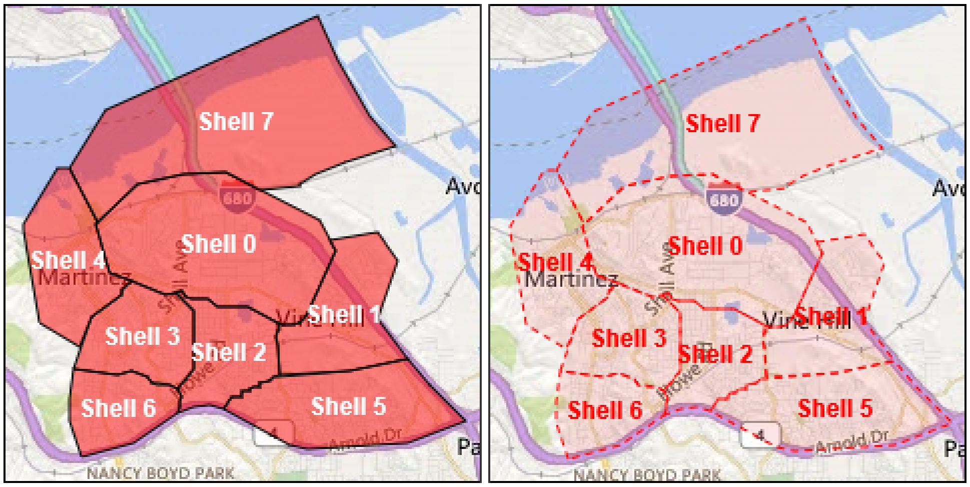
Note: OpenStreetMap is provided by OpenStreetMap (www.openstreetmap.org.) All other map types, except for Bing maps, are provided by ESRI (www.esri.com.)

View layers on the publisher map

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

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

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



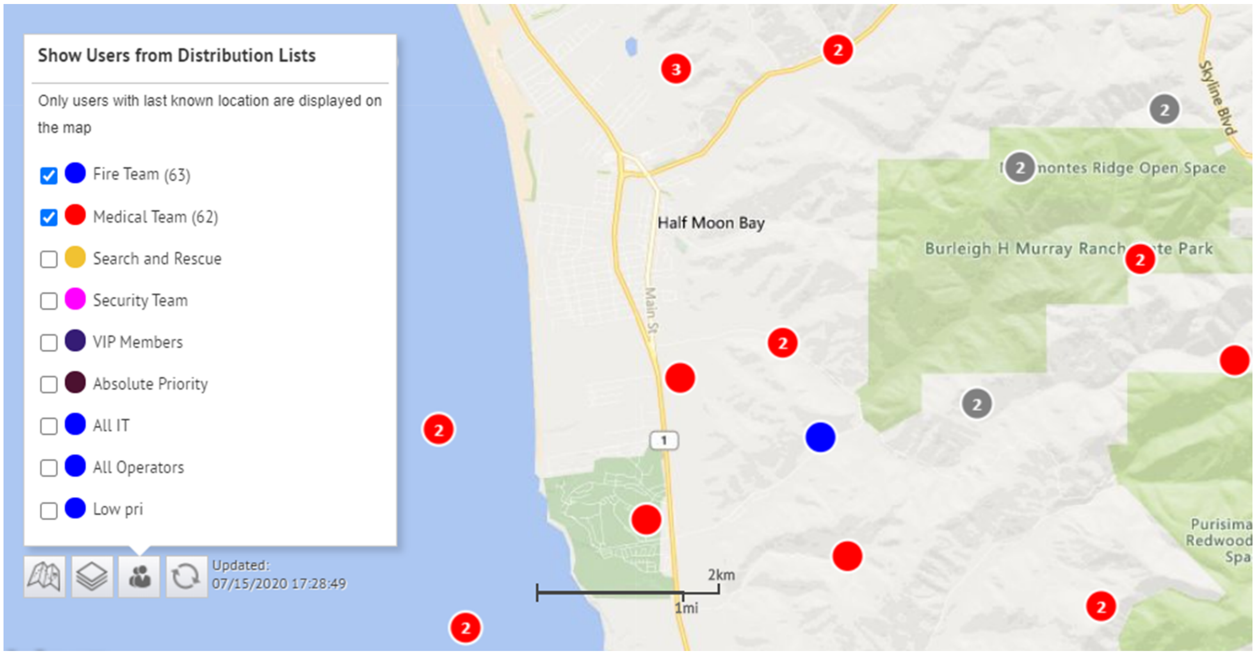
To select a location from a predefined layer for alert targeting, use the **Select Predefined Locations** panel.

View users on the publisher map

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

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

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



Show Users from Distribution Lists

Only users with last known location are displayed on the map

☑ ● Fire Team (63)

☑ ● Medical Team (62)

☐ ● Search and Rescue

☐ ● Security Team

☐ ● VIP Members

☐ ● Absolute Priority

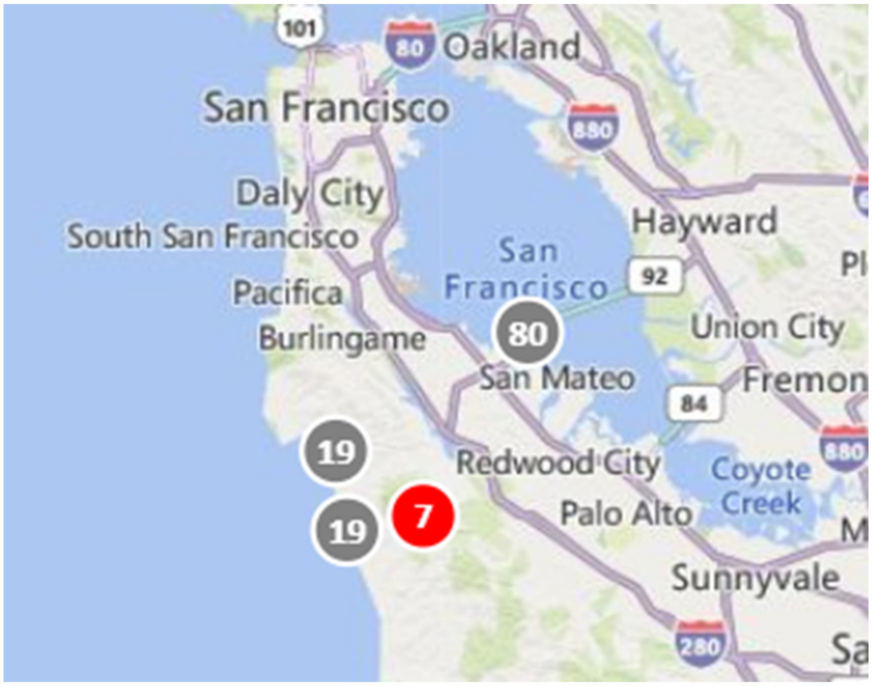
☐ ● All IT

☐ ● All Operators

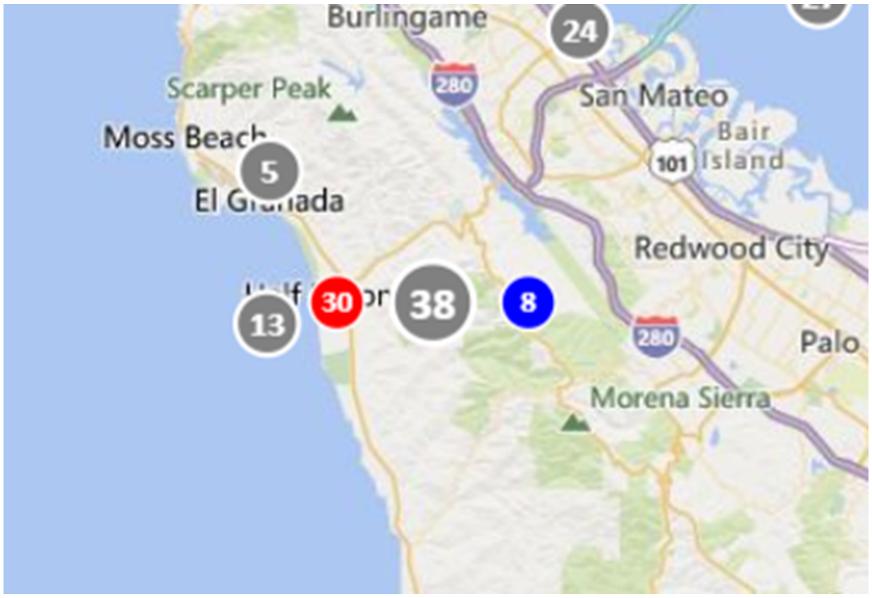
☐ ● Low pri

Updated: 07/15/2020 17:28:49

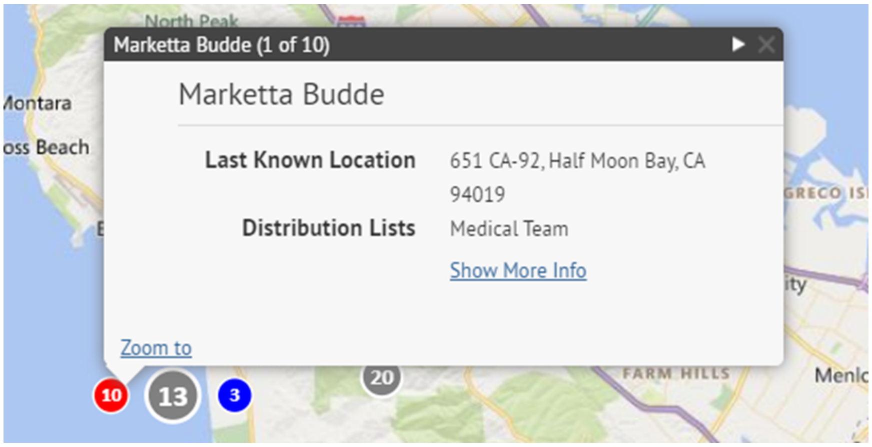
2. Optionally, click ⛶ to zoom the map out to show all users in the selected distribution lists:



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



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



Marketta Budde (1 of 10)

Marketta Budde

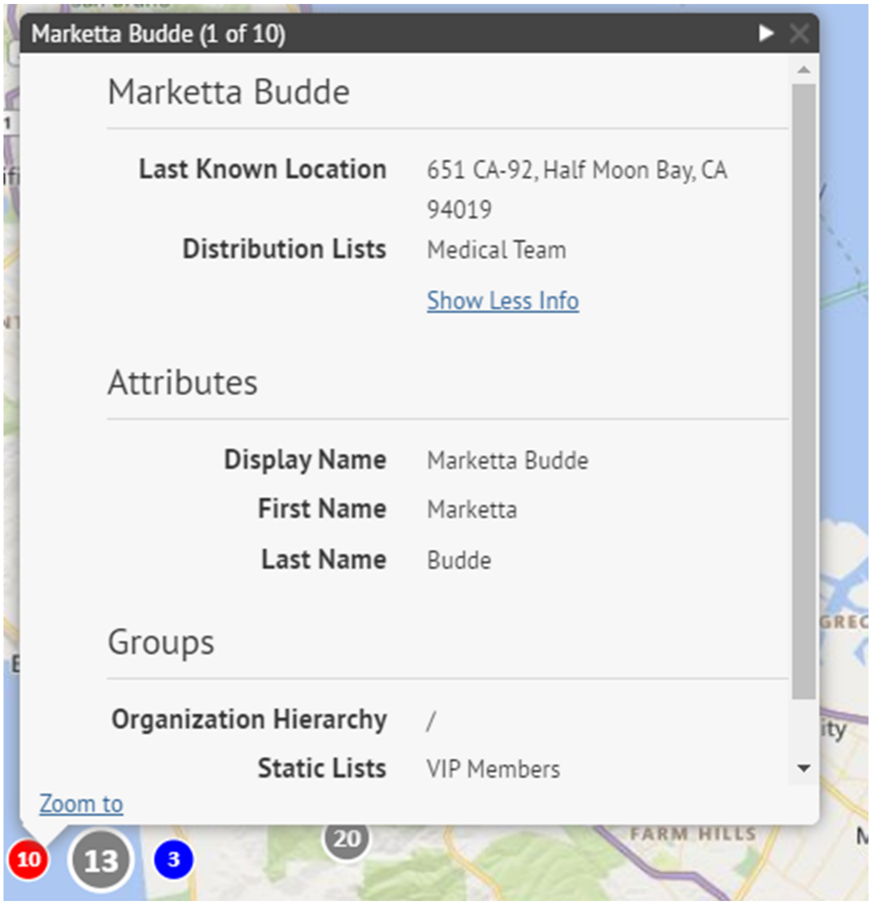
Last Known Location 651 CA-92, Half Moon Bay, CA 94019

Distribution Lists Medical Team

Show More Info

Zoom to

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



Marketta Budde (1 of 10)

Marketta Budde

Last Known Location 651 CA-92, Half Moon Bay, CA 94019

Distribution Lists Medical Team

Show Less Info

Attributes

Display Name Marketta Budde

First Name Marketta

Last Name Budde

Groups

Organization Hierarchy /

Static Lists VIP Members

Zoom to

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

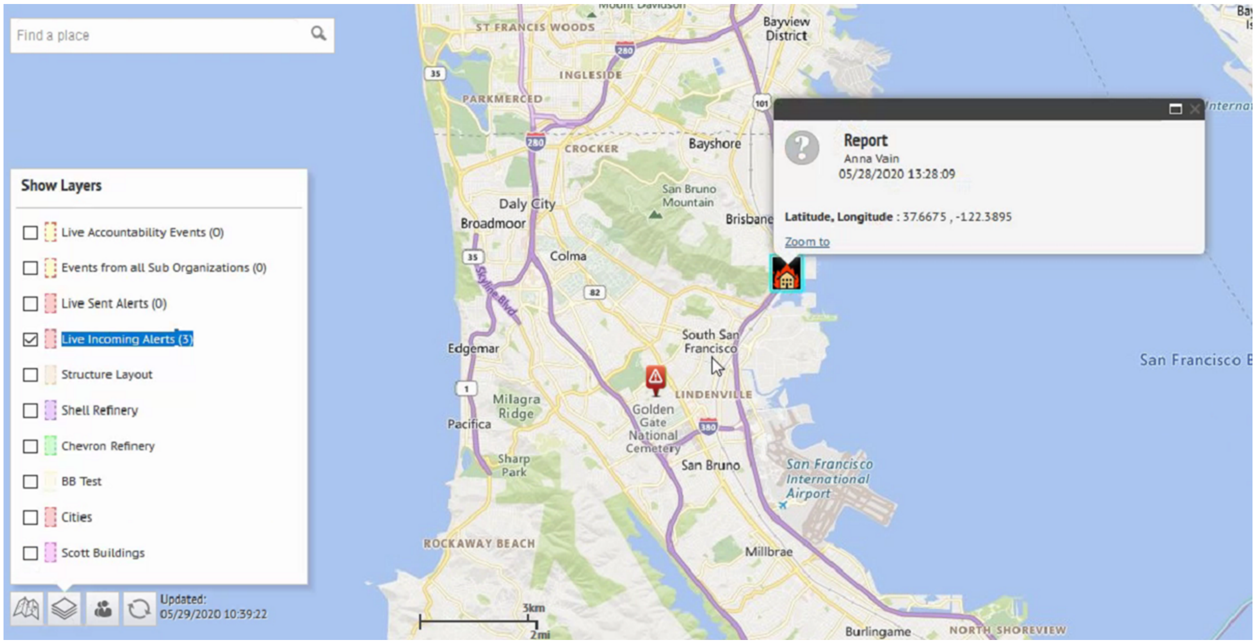
   The ▶ icon appears only when more than one user is displayed in the selected location.

View incoming alerts on the publisher map

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

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

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



Find a place

Show Layers

- ☐ Live Accountability Events (0)
- ☐ Events from all Sub Organizations (0)
- ☐ Live Sent Alerts (0)
- ☑ Live Incoming Alerts (3)
- ☐ Structure Layout
- ☐ Shell Refinery
- ☐ Chevron Refinery
- ☐ BB Test
- ☐ Cities
- ☐ Scott Buildings

Updated: 05/29/2020 10:39:22

Report
Anna Vain
05/28/2020 13:28:09

Latitude, Longitude : 37.6675 , -122.3895

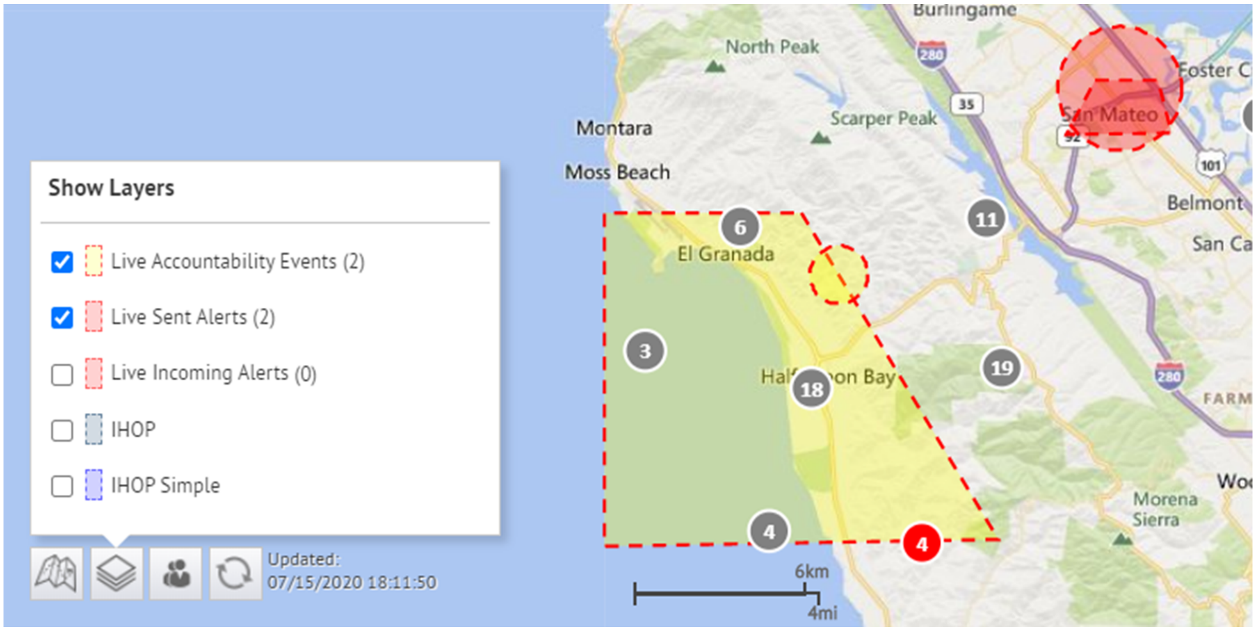
Zoom to

View live alerts and events on the publisher map

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

The publisher map displays all live accountability events and alerts for your organization. If you are logged in to an enterprise organization, it also displays live alerts from your suborganizations.

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



Show Layers

☑ Live Accountability Events (2)

☑ Live Sent Alerts (2)

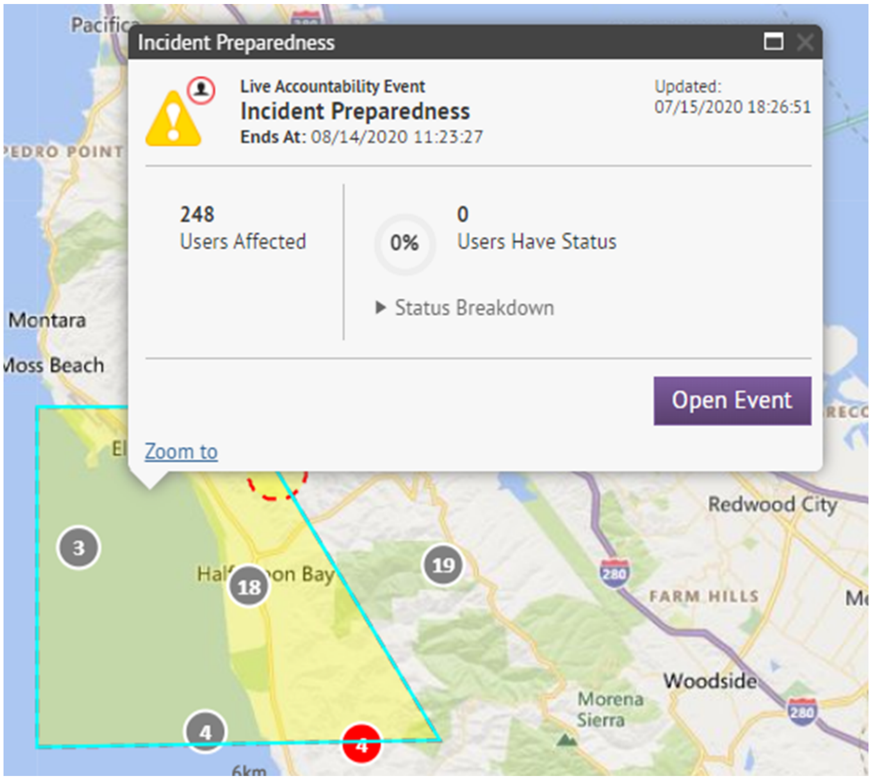
□ Live Incoming Alerts (0)

□ IHOP

□ IHOP Simple

Updated:
07/15/2020 18:11:50

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



Incident Preparedness

Live Accountability Event
Incident Preparedness
Ends At: 08/14/2020 11:23:27

Updated:
07/15/2020 18:26:51

248
Users Affected

0%

0
Users Have Status

▶ Status Breakdown

Open Event

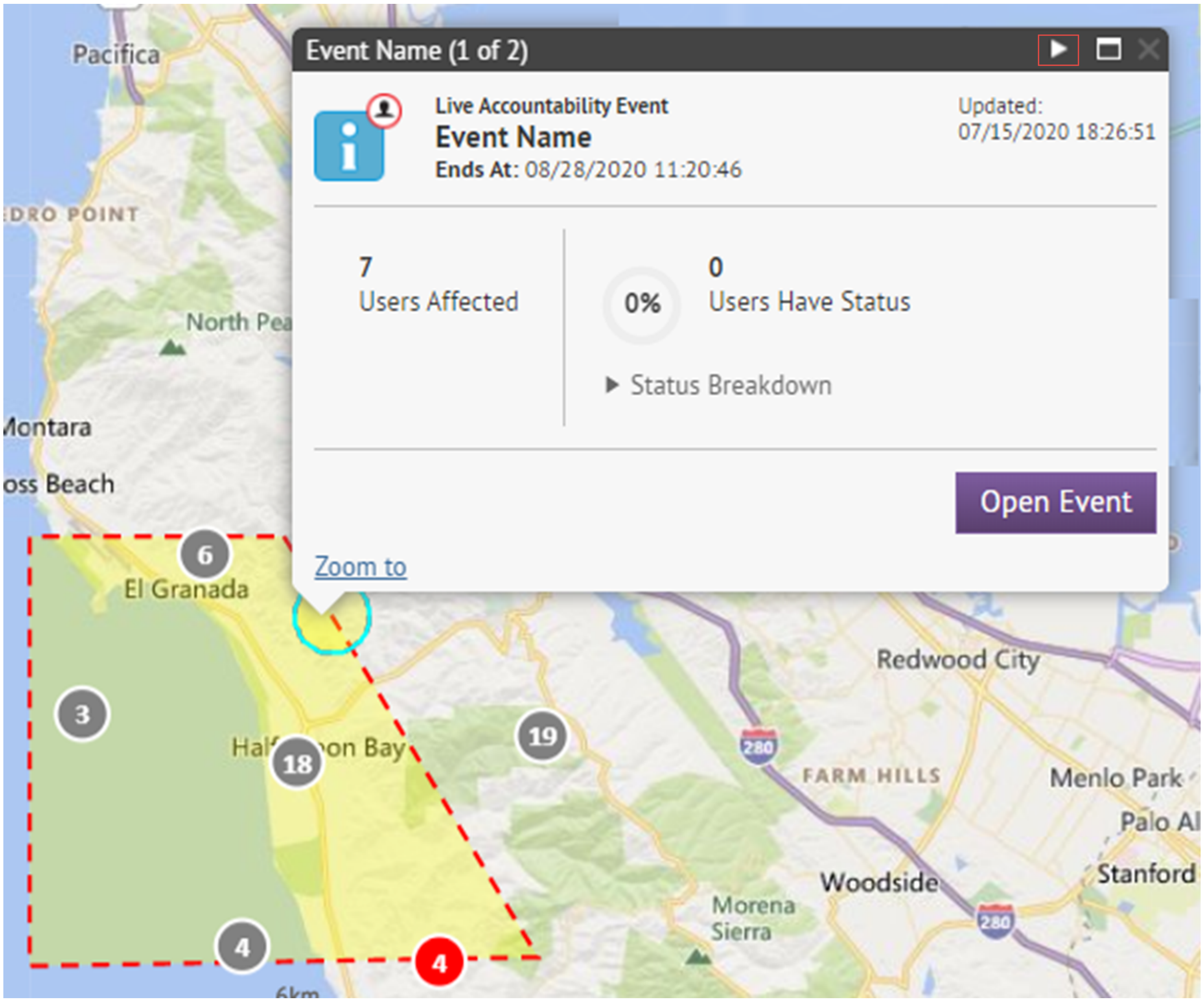
Zoom to

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

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

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

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



Event Name (1 of 2)

Live Accountability Event
Event Name
Ends At: 08/28/2020 11:20:46

Updated:
07/15/2020 18:26:51

7
Users Affected

0%
0
Users Have Status

▶ Status Breakdown

Open Event

Zoom to

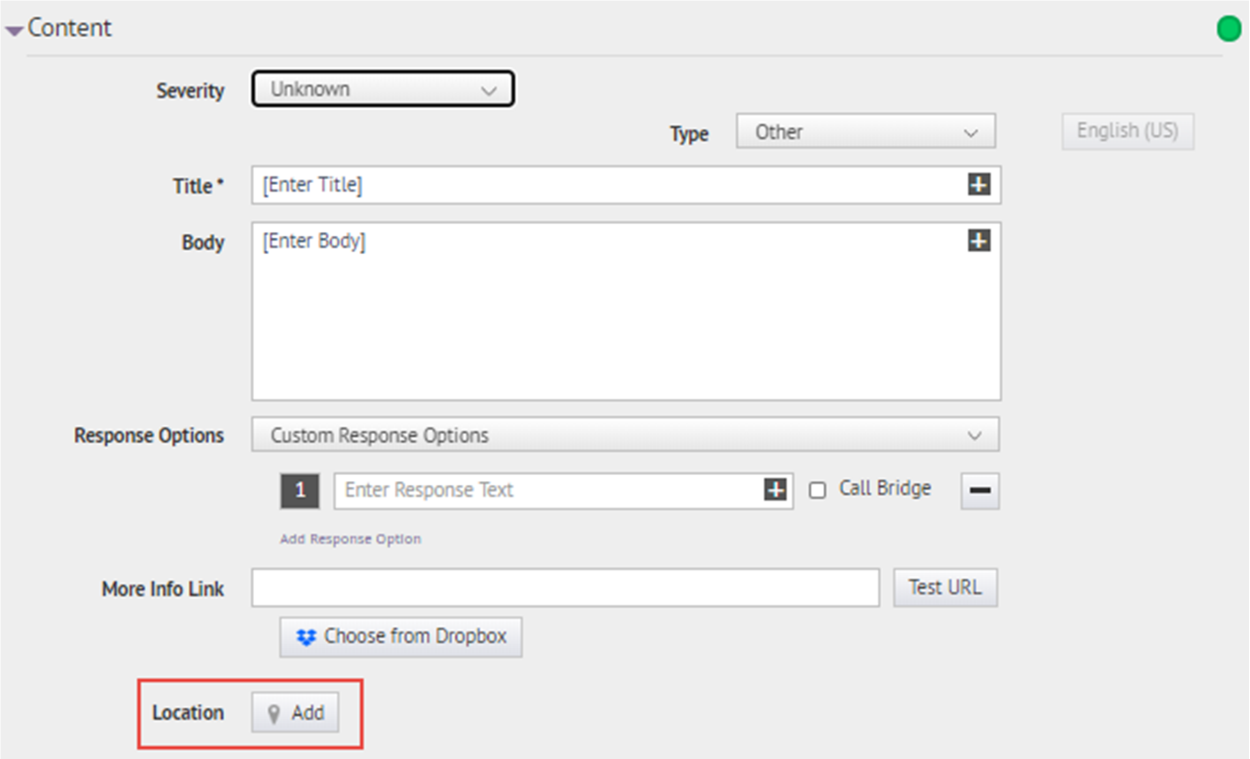
Select an alert or event location

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

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

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

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



Severity Unknown

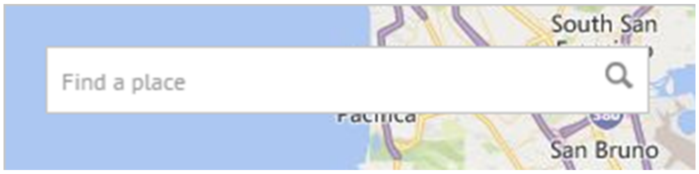
Type Other

English (US)

Response Options Custom Response Options

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

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

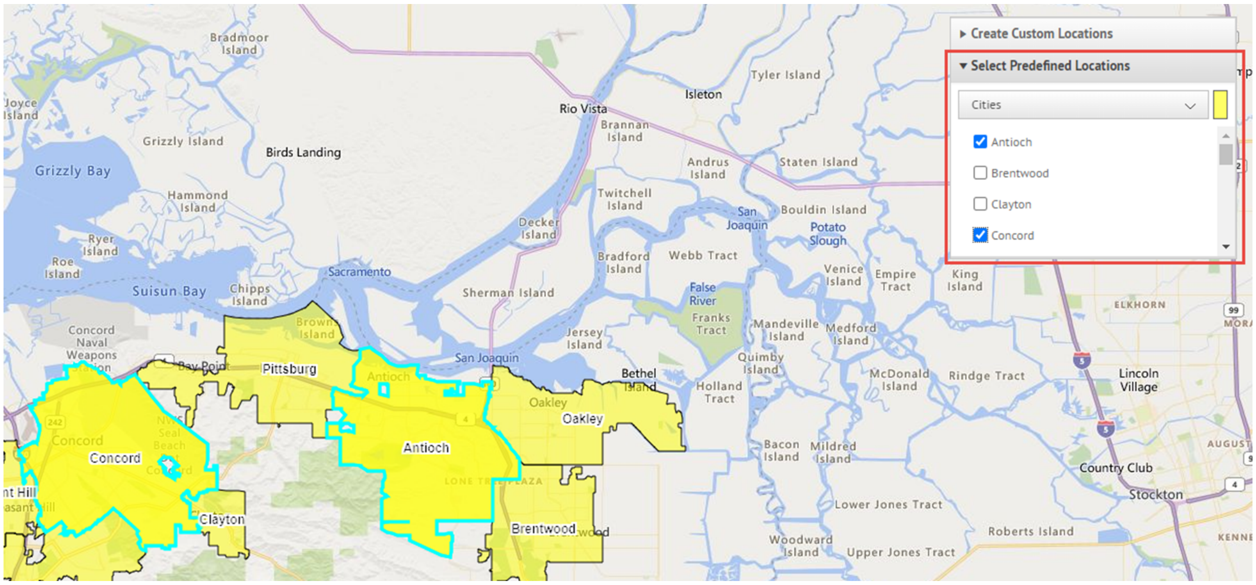


3. To use a predefined location on the map as a targeting criteria, click **Select Predefined Locations** to access a drop-down menu where you can select any predefined layers. When you select a layer, the map updates automatically to display the layer location on the map.

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

   Note: Uploading multiple layers with different sets of predefined locations is recommended to improve usability and system performance. Shape layers are configured on the Map Settings screen. Administrators can access them at **Settings** > **Basic** > **Map Settings**. For more information, see Shape layers.

4. Select one or more predefined locations within the layer by clicking them on the map or selecting them in the drop-down menu. As you make selections, the locations are highlighted on the map.



▸ Create Custom Locations

▾ Select Predefined Locations

Cities

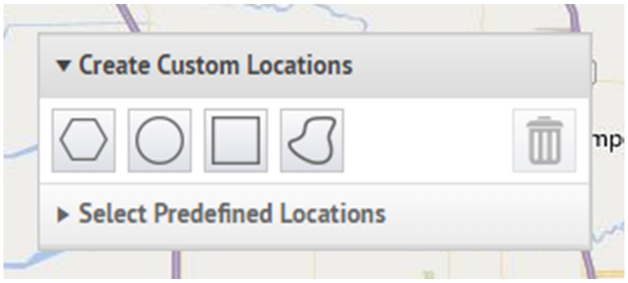
☑ Antioch

□ Brentwood

□ Clayton

☑ Concord

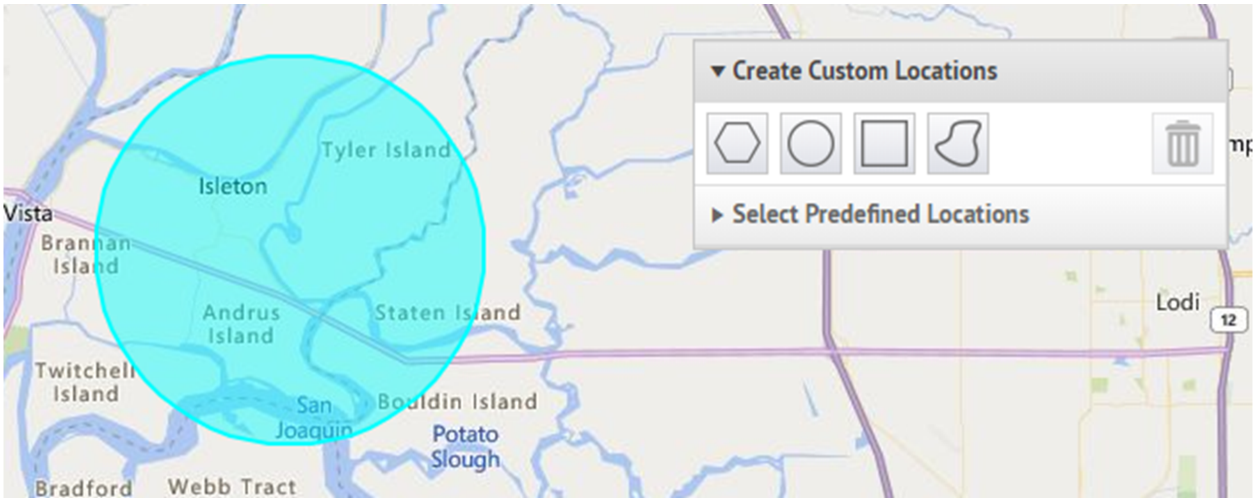
5. To create a custom location, click **Create Custom Locations** to display the drawing tools for creating shapes.



▾ Create Custom Locations

▸ Select Predefined Locations

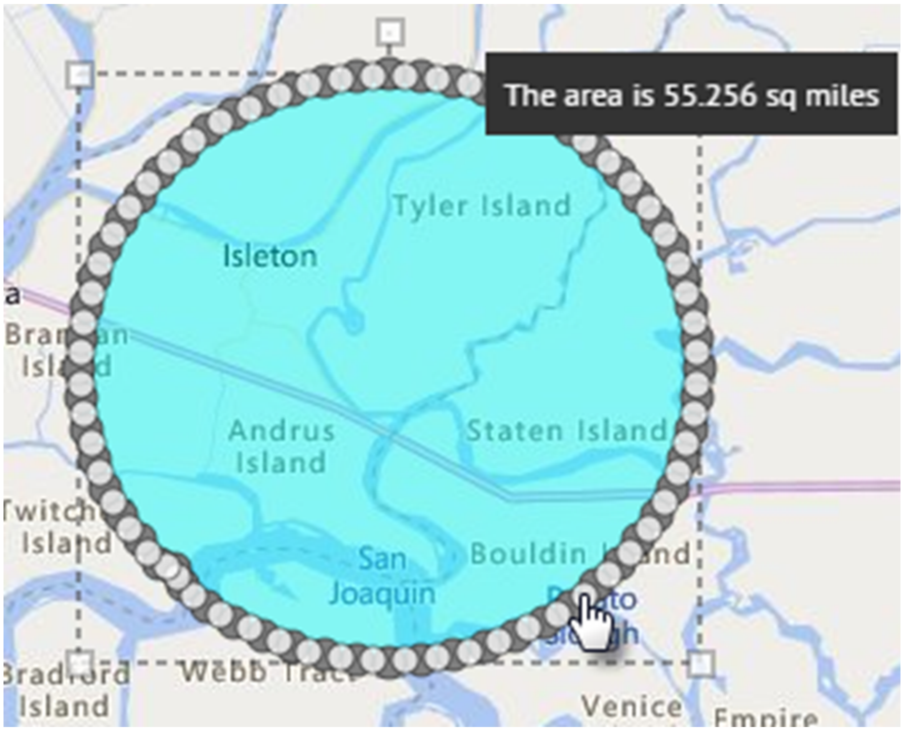
6. In the **Create Custom Locations** toolbar, select a shape and click and drag on the screen to select the location you want to use in the alert or event.



▾ Create Custom Locations

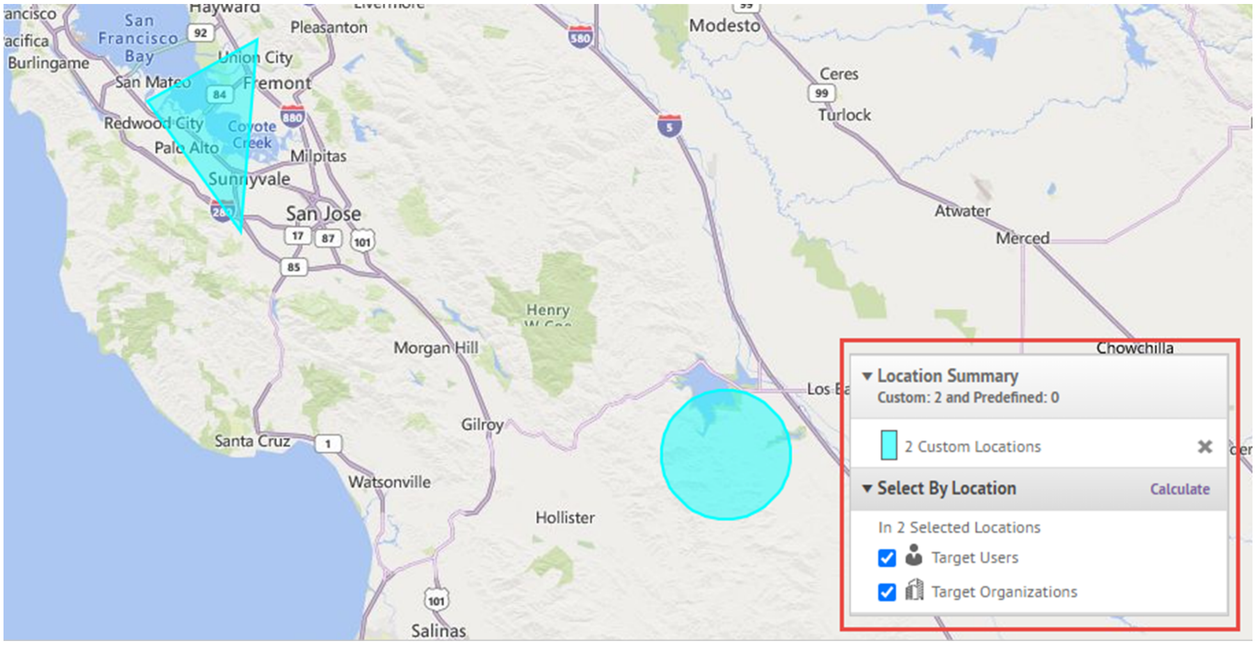
▸ Select Predefined Locations

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



8. To edit a custom location, click the shape and then click and drag on any of the circles that appear around the edge of the shape.
9. To scale new shapes up and down while preserving their dimensions, complete the following steps:
    a. Press and hold the SHIFT key on your keyboard.
    b. Click and release the shape to select it.
    c. Move your cursor over one of the white squares around the shape.
    d. Click and hold on the white box while dragging the mouse to increase or decrease the shape size.

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



Location Summary
Custom: 2 and Predefined: 0

2 Custom Locations ✖

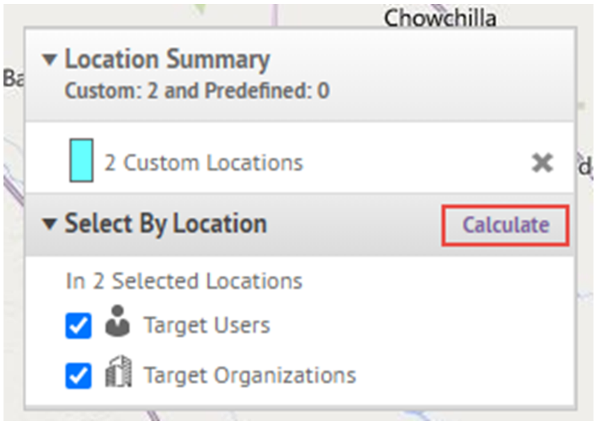
Select By Location Calculate

In 2 Selected Locations

☑ Target Users

☑ Target Organizations

10. To delete the custom locations you created, in the **Location Summary** section, click the **X** beside the custom locations. If you have created more than one custom location, they are combined in the list and cannot be deleted individually. To delete a single custom location, click the border of the location shape on the map to select it, then click 🗑 on the Create Custom Locations toolbar.
11. To view the total number of users and organizations that are located within the selected map locations, click **Calculate** next to the **Select By Location** field.



Location Summary
Custom: 2 and Predefined: 0

2 Custom Locations ✖

Select By Location Calculate

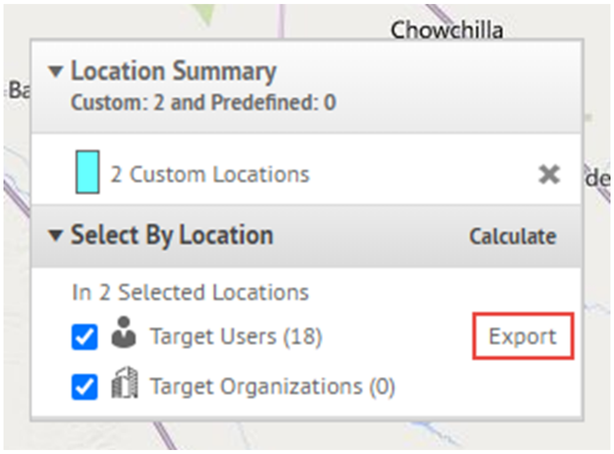
In 2 Selected Locations

☑ Target Users

☑ Target Organizations

Note: Users and organizations listed in the Select By Location field are automatically added to the alert or event target list. To remove them as targets, deselect **Target Users** and **Target Organizations**. For more information, see Target users by location in alerts and Target affected users by location in accountability events.

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



Location Summary
Custom: 2 and Predefined: 0

2 Custom Locations ✖

Select By Location Calculate

In 2 Selected Locations

☑ Target Users (18) Export

☑ Target Organizations (0)

a. On the **Export Options** screen, select the columns to export in the left column and click **Add**.
b. Optionally, use the control buttons on the right to order the selected columns.
c. Click **Export PDF** or **Export CSV**. The .pdf or .csv file downloads to your system.
d. Click **Cancel** to close the **Export Options** screen.

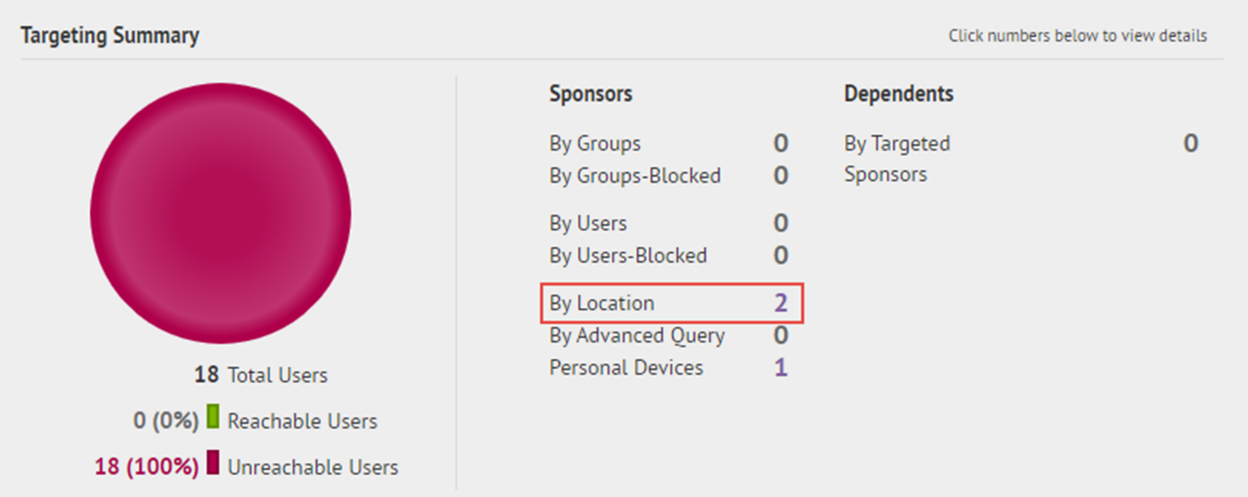
13. Click **Apply**.

Target users by location in alerts

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

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

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



Targeting Summary

Click numbers below to view details

18 Total Users

0 (0%) 🟩 Reachable Users

18 (100%) 🟥 Unreachable Users

Sponsors		Dependents	
By Groups	0	By Targeted Sponsors	0
By Groups-Blocked	0		
By Users	0		
By Users-Blocked	0		
By Location	2		
By Advanced Query	0		
Personal Devices	1		

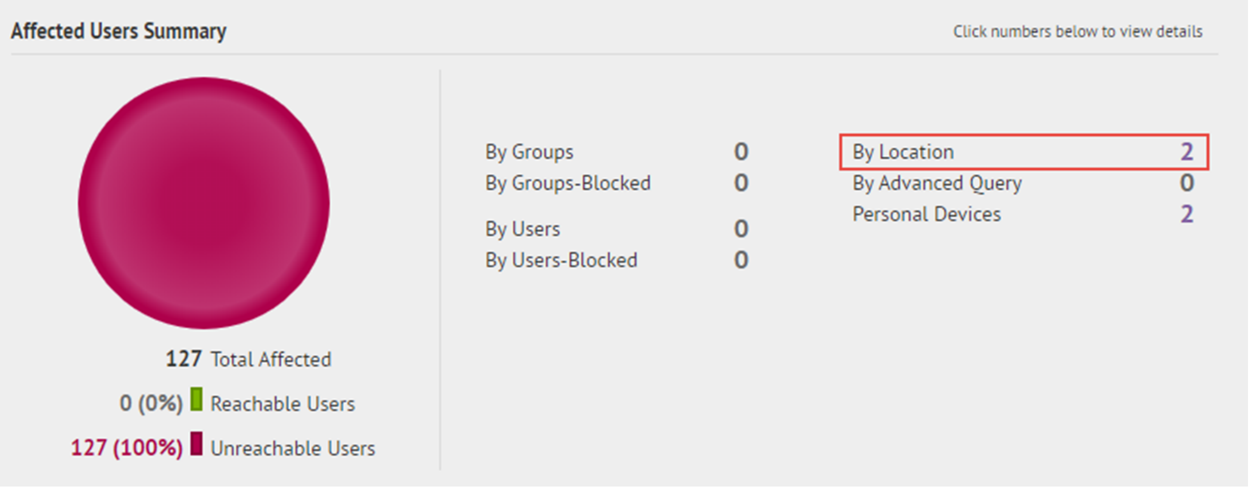
Target affected users by location in accountability events

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

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

   For more information, see Select an alert or event location.
3. Click **Apply**. The 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 who 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.



Affected Users Summary

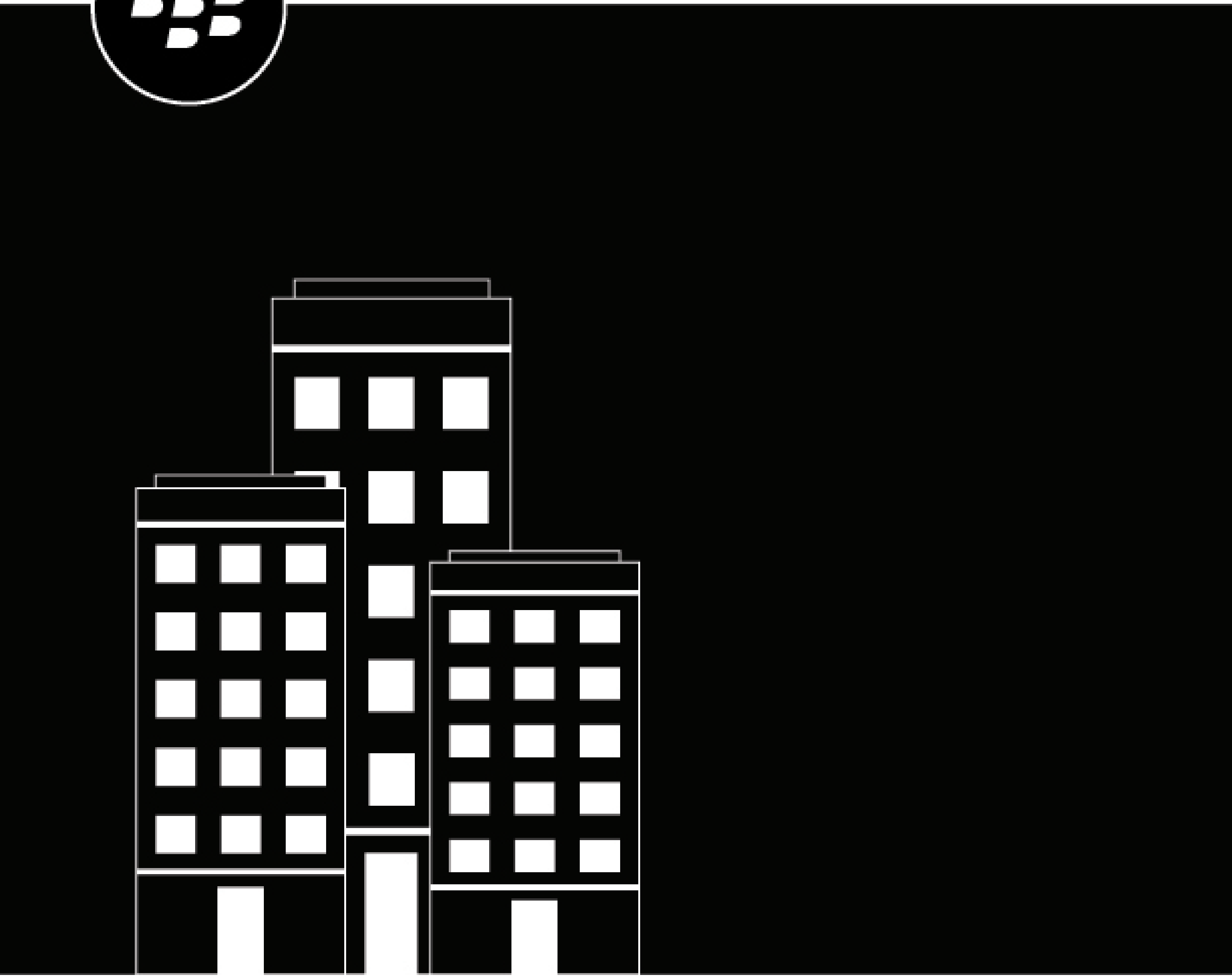
Click numbers below to view details

127 Total Affected

0 (0%) 🟩 Reachable Users

127 (100%) 🟥 Unreachable Users

By Groups	0
By Groups-Blocked	0
By Users	0
By Users-Blocked	0
By Location	2
By Advanced Query	0
Personal Devices	2



BlackBerry AtHoc

Manage Users

7.16

Contents

Manage users.. 28

Manage organization subscriptions..31

Manage user attributes.. 34

Manage user authentication...53

Manage users

This document describes how to manage users in the BlackBerry® AtHoc® system. Users can be the end users that receive alerts, dependents of users, operators with varying degrees of privileges, or administrators that configure BlackBerry AtHoc settings.

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

For information about operator roles and permissions, see the *BlackBerry AtHoc Operator Roles and Permissions* guide or the *BlackBerry AtHoc Roles and Permissions Matrix*.

Quick Action Guides

View all Quick Action Guides

- Manage operator roles and permissions
- Create a user
- Create a static distribution list
- Create a dynamic distribution list

Create a user

Note: You must be an End Users Manager to create users.

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

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

   Note: Fields marked with an asterisk (*) on the New User screen are required.
3. On the **New User** screen, in the **Basic Information** section, enter the following details about the user:
   - **Username**: The name the user is assigned by the system. Usernames are frequently imported from external systems and cannot be edited later.
   - **First Name** and **Last Name**
   - **Display Name**: The name used to refer to the user within the system, such as bsmith or Jack Jones. This field can be edited later by the end user.
   - **Organizational Hierarchy**: If the organizational hierarchy is available:
     - a. Click **Select**.
     - b. On the **Select the Organizational Position** window, navigate to the specific organization the user belongs to.
     - c. Click **Apply**.
   - Any custom fields added by administrators, including details such as CPR certification status, Emergency Community membership, or special skills.
   - Enter a work location and (if applicable) temporary work location.
4. In the **Numbers** section, enter the work, mobile, text messaging, pager, and any other numbers that can be used to contact the user.

Note: International numbers and numbers with extensions are supported.

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

Note: For pagers, only devices that are enabled for the organization appear in the list.

5. In the **Online Addresses** section, enter work and home email addresses.
6. In the **Physical Addresses** section, enter work and home addresses.
7. In the **Distribution List Membership** section, select the distribution lists the user is a member of.

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

10.Click **Save**.

The details of the new user appear in summary form on the screen. You can return to the Users screen or grant the user operator permissions. For details, see "Grant operator permissions to a user" in the *BlackBerry AtHoc Operator Roles and Permissions* guide. For quick steps, see *Manage operator roles and permissions*.

Enable users

You can enable a user if the following conditions are true:

- You are an End Users Manager in the organization.
- You are an End Users Manager for the user. In some cases, the user may be outside of your user base and appear as read-only.

1. In the navigation bar, click **Users** > **Users**.
2. If the **Status** column is not visible in the user list, click **Add** in the header row to add a column.
3. Click the ⌄ in the new column heading, and then select **Status**.
4. Select the check boxes beside the users whose status you want to change.
5. Click **More Actions** > **Enable**.

The users are enabled and the Status column updates for each of the affected users.

Note: If a sponsor has dependents, the dependents are also enabled.

Note: If you have selected users that you do not have permissions to enable, a warning message appears.

Disable users

Disabling a user temporarily removes them from alert target lists or groups but keeps them in the system so that they can be re-enabled again. Users are commonly disabled when they take a leave or temporarily join another organization.

You can disable a user if the following conditions are true:

- You must be an End Users Manager for the organization.
- The user is in your user base. Your user base may be restricted to exclude the user and the user is hidden from view.

It may be more efficient to identify the users that you want to disable based on a specific user attribute or set of attributes they have in common. For instructions, see Automatically disable users based on attributes.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, select the check boxes beside the users whose status you want to change from Enabled to Disabled.
3. Click **More Actions** > **Disable**.
4. On the confirmation window, click **Disable**.

The users are disabled.

Note: If any selected users have dependents, they are also disabled.

Note: If you have selected users that you do not have permission to disable, a warning message appears.

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

Delete users

You can delete a user if the following conditions are true:

- You are an End Users Manager for the organization.
- The user is in your user base. Your user base may be restricted to exclude the user and the user is hidden from view.

Note: You can identify the users you want to delete based on a specific user attribute or set of common attributes. For more information, see Automatically delete users based on attributes.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, select the check boxes beside the users you want to delete.
3. Click **More Actions** > **Delete**.
4. On the confirmation window, click **Delete** to permanently remove the users from the system.

   The screen refreshes and the Users list no longer displays the users.

Note: If the sponsor or sponsors have dependents, those dependents are also deleted.

Note: If you have selected users that you do not have permission to delete, a warning message appears.

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

Note: When a user is deleted, all personally identifiable information about the user is deleted from the BlackBerry AtHoc system. In historic user tracking reports, the deleted user's details are replaced with DEL_[GUID].

Purge deleted users

When users are deleted, they no longer appear in the BlackBerry AtHoc management system, but data for those users is still held in the database until purged. Deleted users are purged once a day by default. Purging deleted users ensures that the user base is kept current and database performance is maximized. Do not disable purging deleted users unless your organization has a data retention requirement. You can change the purge interval.

1. In the navigation bar, click ⚙.

2. In the **Users** section, click **Disable and Delete Users**.
3. On the **Disable and Delete Users** screen, scroll down to the **Purge Deleted Users** section.
4. Select the **Purge deleted users after** option.
5. From the **Purge deleted users after** list, select the purge interval.
6. Click **Save**.

Important: After a purge occurs, it cannot be undone.

Edit user details

You can edit the details of an individual user in the BlackBerry AtHoc system. To make a global change to all users, see Make mass changes to user details.

Note: You must be an End Users Manager to edit user details.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click ✎ beside the name of a user.
3. On the user details page, make changes to any of the user fields in the following sections:
    - Basic Information
    - Numbers
    - Online Addresses
    - Physical Addresses. Displays the time the user's location was last updated. To view the user's location on a map, click 🌐.
    - Last Known Location. Populates with location information from a check in, check out, alert response, report, emergency, or tracking from the BlackBerry AtHoc mobile app. Click 🌐 to view the user's last known location on a map. Click **Clear** to remove the last known location. The last known location cannot be edited from the BlackBerry AtHoc management system or Self Service.
    - Distribution List Membership
    - Login and Location
    - BlackBerry AtHoc Apps: See Delete unused mobile devices from a user profile.
    - Organization subscriptions (if enabled): This section appears when the organization subscription feature is enabled and organizations are configured for subscription. This section displays the user's subscribed organizations, the start and end dates, and the assigner for each subscription.
    - Any user attributes defined by administrators

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

Delete unused mobile devices from a user profile

To prevent reaching the user device limit, the operator can remove unused mobile devices from a users profile page in the BlackBerry AtHoc management system.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click ✎ beside the name of the user.
3. On the users profile page, in the **BlackBerry AtHoc Apps** section, beside **Mobile App**, click **Active** (*x*).
4. On the **User Mobile Devices** window, click ✖ beside the mobile device you want to delete.
5. On the confirmation window, click **Delete**.

The mobile device is removed from the user's profile and can no longer be targeted in alerts and events.

Enable users to receive alerts in their preferred language

Enable the Bilingual Support feature in the BlackBerry AtHoc management system to allow end users to select a preferred language to receive alerts in.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Click ⚙.
3. On the **Settings** page, in the **System Setup** section, click **Feature Enablement**.
4. On the **Feature Enablement** page, ensure that **IsBilingualAlertSupported** is set to True.
5. Click ⚙.
6. On the **Settings** page, click **General Settings**.
7. On the **General Settings** page, in the **Customization** section, select to enable delivery locales from the **Delivery Locales** pull-down menu.
8. Click **Save**.
9. On the **Settings** page, click **User Attributes** > **Preferred Language**.
10. On the **Preferred Language** page, in the **Page Layout** section, select the section in the User details pages to display the Preferred Language attribute in.
11. Click **Save**.
12. Optionally, to enable users to select their preferred language from the BlackBerry AtHoc mobile app:
    a) Click ⚙.
    b) On the **Settings** page, in the **Devices** section, click **Mobile App**.
    c) On the **Mobile App** page, in the **Features** section, select the **My Profile Page** option.
    d) Select the **Show Preferred language selection to support bilingual alerts** option.
    e) Click **Save**.

Prioritize personal devices

Operators can set the priority of alert delivery by device type for end users. When enabled, the device delivery preference feature prevents end uses from receiving the same alert on multiple devices. When device delivery preference is enabled, and user preferred is selected as the device delivery preference in an alert or event template, end users receive alerts on their enabled devices in the order specified in the user's profile.

Before you begin:

- Device delivery preference must be enabled for the organization.
- At least one personal device must be enabled in the organization.
- The user must have at least one enabled device with an address in their profile.
- You must be an Enterprise Administrator, Organization Administrator, End Users Manager, Alert Manager, or Advanced Alert Manager to prioritize personal devices for a user.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** page, select the user you want to update.
4. On the user details page, click **More Actions** > **Prioritize Personal Devices**.
5. On the **Prioritize Personal Devices** window, click ⬍ and drag to reorder the device. Personal devices are prioritized according to their position in the list, with the highest priority device appearing on top.
6. Click **Save**.

Import users from a .csv file

Important: When you import user details into BlackBerry AtHoc using a .csv file, the values that exist in the .csv file overwrite any existing values in the database. If the file contains blank fields, the current values in the database are replaced by empty values. Ensure that all required fields are populated before you upload the file.

To import users from a file, the file must be correctly formatted. If you do not know how to format the file, see Format a user import file.

To import operators from a file, see "Importing and exporting operators" in the *BlackBerry AtHoc Operator Roles and Permissions* guide.

If duplicate users (identified by username or mapping ID) are found in the .csv file, they are not imported and one of the following error messages is displayed:

```
[Username]: <username> already exists in the payload
```

```
[Mapping ID]:<mapping id> already exists in the payload
```

The remaining unique users in the .csv file are imported.

If a username contains a space or one of the following characters, the user is not imported and an error message is displayed:

[ ] : ; | = , + * ? < >

If the username contains leading or trailing spaces, the spaces are ignored and trimmed during the import process. After the spaces are trimmed, the user is imported.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click **More Actions** > **Import** > **Users**.
3. Optionally, click **Download a template CSV file** to download a blank .csv file to use as a template for your import user file. Save the file to your computer and fill in the appropriate user information.

   Note: Using the template ensures that all of the mandatory attribute columns are included in the import file.
4. Click **Browse**.
5. Navigate to the location of the import user file on your computer.
6. Open the file to enter or modify the user data.

   Note: Microsoft Excel hides some characters from view. If you edit the file in Microsoft Excel, it might format your entries with extra characters. The incorrect format might cause the import operation to fail. If you are using anything other than a text editor to modify the .csv file, open the file in a text editor such as Microsoft Notepad, review the syntax for problems, then save the modified file as a .txt file. Edit the file name to change the extension from .txt to .csv. This method preserves the formatting in the text file.
7. Ensure that columns with multiple values have the correct format to import correctly.
   - The entire entry must be enclosed within double-quotes. This rule is true even if a multi-select picklist has only a single entry.
   - Use a comma to separate each value. Do not include spaces before or after the comma.
     - Example: Two column names, separated by a comma (no space before or after the comma). `POSITIONS` is a multi-select picklist column: `USERNAME,POSITIONS`
     - Example: A multi-select picklist attribute column with multiple entries: `Cadiz,"ESH Team Tech Supv,FMT Coordinator,SITE 300,Exercise Call Out,Field Monitoring Team,Coordinator DOC"`
     - Example: A multi-select picklist attribute with a single entry: `East,"LEDO"`
   - An entry can have a space within it. For example: `Field Monitoring Team`
8. Verify that columns with multiple values have the correct format to import correctly.

- Use a comma to separate each value. Do not include spaces before or after the comma.
- If you are importing user base restrictions, you must enclose each value with double quotation marks ("").

9. Optionally, make sure that any geolocation attributes in the .csv file are in the correct string address, "Latitude,Longitude" or Point(long,lat) format. For example, 311 Fairchild Drive, Mountain View, CA, "37.538226,-122.32726", or POINT(-122.32726,"37.538226).
10. (Optional, for enterprise organizations with user uniqueness enabled.) If you want to prevent users from being moved between organizations after you have imported them, include the **Prevent User Move** column, and enter **Yes** for all users.
11. After you have entered your data, save and close the file.
12. Click the filename, and click **Open** to upload the file into the system.

    The filename appears in the User CSV File field on the Import User File screen. Each of the columns from the import file are listed in the **Select the columns to import** section.
13. Optionally, select **Partial User Import Enabled** to enable partial user data to be imported. When selected, if a user entry contains an invalid value, the rest of the user's data is still imported.

    Note: Even if you do not select this option, partial user import is still applied when importing geolocation attributes that use a physical address.
14. Select the columns of data you want to import or click **Select All**.
15. Review the **Columns that cannot be imported** list to make sure it does not contain important data that you must be able to view in BlackBerry AtHoc. If the list contains important columns of information, contact BlackBerry AtHoc customer support for help.
16. Click **Import**.

The Importing Users window opens. The import happens in batches of 5000 users.

While the import is in progress, a **Stop Import** button appears on the **Importing Users** window. Clicking this button stops the import process immediately and prevents the next batch of users from being imported from the file. However, records that have already been added are not removed and records that have been updated are not restored to previous values.

When the import completes, an import summary screen displays following information:

- Total number of users in the import file
- Total number of users who were processed
- Number of users who were successfully processed
- Number of users who were partially processed
- Number of users who failed to be processed
- Username of the person who imported the file
- Time the file import process started and ended

Note: To import and export operators, see "Importing and exporting operators" in the *BlackBerry AtHoc Operator Roles and Permissions* guide.

Tip: Click **Download Log** on the Import Details: Import Completed screen to download a .csv file that includes information about the sync status of the operator import.

Format a user import .csv file

The following table describes the required import .csv formatting standards.

Field Name	Description	Is Mandatory?
Username	The Username is a value that identifies a user in the BlackBerry AtHoc system and the user repository (for example, LDAP or Microsoft Active Directory) within your organization. The Common Name field must contain a unique value, such as an Employee ID or a Windows user name. After the Common Name is registered with the BlackBerry AtHoc system, the user is linked to the user profile within your organization. The username cannot contain spaces or any of the following characters: [ ] : ; | = + * ? < >. Leading or trailing spaces are trimmed during the import process. After the leading or trailing spaces are trimmed, the username is accepted and the user is imported.	Yes
Status	Use the Status column to enable, disable, or delete a user. The following attribute values can be used: • Enabled: Enable the user • Disabled: Disable the user • Deleted: Delete the user The import file must contain a Status column, but the column can be empty. If the Status column is empty but the database contains Status information, the current Status information is overwritten and replaced by the empty values in the import file on import.	Yes
HRCHY: Hierarchy Name	Use the "HRCHY:" prefix to specify the location in your User Base Hierarchy where the user is a member. Click **Users** > **Users** > 👥 to view your organizational hierarchy.	No
SDL: Static Distribution List Name	Use the "SDL:" prefix to specify the name of a static distribution list to add users to. Click **Users** > **Users** > 👥 to view your distribution list hierarchy. There can be multiple "SDL: list name" columns. If the user does not already exist, this option can only be used to add the user to a static distribution list. A valid value is "Yes" (the user will be added to this static list.) If the user already exists, use this option to add or remove the user from a static distribution list. Valid values are "Yes" (the user will be added to this static list) or "No" (the user will be removed from this list.)	No
User Attribute Name	Specify a user attribute name as column heading to update user attribute values.	No

Field Name	Description	Is Mandatory?
Device: Device Name	Use the "Device:" prefix to specify a device name in the import file. For pager addresses, specify the pager carrier ID followed by a colon (:) before the pager number. For example, to import pager number, "5551222" with pager carrier ID 3, use "3:5551222" as the pager address in the .csv file. To view the list of pager carrier IDs and names, see "Pager carrier IDs and names" in the *BlackBerry AtHoc Create and Publish Alerts* guide.	No
Password	Passwords must conform to the password rules set in **Settings** > **Security Policy** > **Password Update Rules**.	No
Organization	Only available for enterprise organizations with user uniqueness enabled. Specify the display name for each organization. New users are created in the specified organization and existing users are moved to the specified organization. **Note:** If the following error occurs while importing users in the Enterprise, "[Organization]: Column was not recognized as an attribute or device", it is because user uniqueness is not enabled. You can enable user uniqueness in **Settings** > **General settings**.	No
Subscribed Organizations	Only available when the organization subscription feature is enabled and organizations are available for subscription. Specify organizations to subscribe users to. You can subscribe a user to a maximum of ten organizations. Separate organization names with a comma. You can also specify start and end dates for the subscription. Use the date format of your organization. Separate the start and end dates with a pipe (|) character. For example: Sub-Org1: 4/5/2021|8/8/2021, Sub-Org3: 5/5/2021|, Sub-Org4: |7/7/2021.	No

Stop the import users process

Important: When you import user details into BlackBerry AtHoc using a .csv file, the values that exist in the .csv file overwrite any existing values in the database. If the .csv file contains blank fields, the current values in the database are replaced by empty values.

While the import user process is underway, the import happens in batches of 5000 users. Click the **Stop Import** button on the **Importing Users** window to stop the import process and prevent the next batch of users from being imported.

The Stop Import button stops the import, but does not undo it. Records that have already been added are not removed and updated records are not restored to previous values. To download a .csv file that contains information about the users that were imported before the import was stopped, click **Download Log** on the **Import Details: Stopped** window.

Bulk-update users' physical locations

You can use the BlackBerry AtHoc .csv file import process to bulk-update your organization's users physical addresses without converting the addresses to the latitude,longitude or POINT(longitude latitude) format. When the import process begins, a query is sent to the Bing geolocation API to calculate the longitude and latitude of the user's physical address provided in the input file. Only addresses that the Bing API returns with a match code of High Confidence or Good are processed and added to the database. The latitude,longitude and POINT(longitude latitude) formats are still supported.

After the .csv file user import updates users' physical locations, a preprocessor job performs the following functions:

- Checks for duplicate entries in the input .csv file and removes any duplicates before sending the request to the Bing API.
- Checks the database for existing addresses before sending the request to the Bing API. Existing addresses are not sent to the Bing API for processing.
- Sends the job to the Bing API for processing.

The preprocessor job runs automatically every 8 hours. The BlackBerry AtHoc management system makes three attempts to submit failed requests to the Bing API at 8 hour intervals.

The post processor job pings the Bing API every 4 hours to check the status of submitted jobs. If a job is complete, the postprocessor job performs the following functions:

- Gets the translated geolocations in latitude,longitude from the Bing API.
- Records the results in the database.
- Updates the Geocoding Summary and Logs settings page in the BlackBerry AtHoc management system.
- Sends an email to the operator who initiated the bulk update that provides the status of the update including the total number of records processed, successfully processed, and not processed. The email contains a link to the Geocoding Summary and Logs settings page in the BlackBerry AtHoc management system.
- Adds a record of the update to the operator audit trail in the BlackBerry AtHoc management system.

The postpocessor job runs automatically every 4 hours. The BlackBerry AtHoc management system makes three attempts to download the postprocessor job at 4 hour intervals.

Note: For more information about the Geocoding Summary and Logs settings page, see "View geolocation transactions and logs" in the *BlackBerry AtHoc System Administrator Configuration Guide* guide.

Undo the import users process

The import users process cannot be undone after it runs. The only way to undo the import is to re-import the original data that was overwritten.

Troubleshooting tips for user import

This topic describes some of the issues that may cause a user import to fail, and how to resolve those issues.

Include mandatory fields: Make sure your .csv file contains a column for the mandatory Username field. The Username field must contain a unique value, such as an Employee ID or a Windows user name.

Populate required fields: Before uploading a .csv file to import users, make sure that the file includes columns that match the mandatory user fields in the organization's Users list. If the import file contains a Status column, it must contain a status value.

Use the correct column formatting: Ensure that columns with multiple values have the correct format to import correctly.

- The entire entry must be enclosed within double-quotes. This rule is true even if the multi-select picklist has only one entry.
- A comma must be used to separate each of the values. There can be no spaces before or after the comma.

  Examples:

  - This example shows two column names, separated by a comma (*no* space before or after the comma). `POSITIONS` is a multi-select picklist column:

    ```
    USERNAME,POSITIONS
    ```
  - This example shows a multi-select picklist attribute column with multiple entries:

    ```
    Cadiz,"ESH Team Tech Supv,FMT Coordinator,SITE 300,Exercise Call Out,Field
    Monitoring Team,Coordinator DOC"
    ```
    - The entire entry starts and ends with regular double-quote characters, not the "smart quotes" used by some word-processors.
    - Each picklist entry is separated by a comma with no spaces before or after the comma.
    - An entry can have a space within it. For example: `Field Monitoring Team`
  - This example shows a multi-select picklist attribute with a single entry:

    ```
    East, "LEDO"
    ```
- Make sure that any geolocation attributes in the .csv file are in the correct string address or "Latitude,Longitude" format. For example, 311 Fairchild Drive, Mountain View, CA or "37.538226,-122.32726".

Enable user uniqueness for enterprise organizations: If you are importing users in an enterprise organization, user uniqueness must be enabled. Otherwise, the import fails with the following error: "[Organization]: Column was not recognized as an attribute or device".

For instructions on how to enable user uniqueness, see "Enable enterprise features" in the *BlackBerry AtHoc Enterprise Features* guide.

User import errors: The following table describes possible error messages that may be encountered when importing users from a file:

Error message	Notes/Workaround
Errors were found when parsing the CSV file, such as duplicate column names.	Generic message for unexpected errors. If your .csv file contains a column for organization hierarchy, make sure that it includes the prefix "HRCHY:" to specify the location in your User Base Hierarchy where the user is a member.
[Status]: Attribute is mandatory but no value has been provided.	Make sure that the Status column contains a value. Valid values are Enabled and Disabled.
Unable to locate upload directory.	This error occurs when the import file upload path does not exist on the application. The correct path is: %AtHocENS_home%\ServerObjects\uploadStage
The uploaded CSV file does not have a username column. The username column is required.	Update the .csv file to include a username column.

Error message	Notes/Workaround
The uploaded CSV file has no user rows.	Update the file to include user rows. Update the .csv file to include columns.
There was some error in processing the request.	Check the .csv file for duplicate columns.
[Username]: The following characters are not allowed in Username [ ] : ; | = , + * ? < > space.	The username contains one or more invalid characters.
Organization subscription end date provided for org [\{0}] can not be earlier than start date	If a Subscribed Organizations column with start and end dates is included, the end date cannot be earlier than the start date.
Invalid organization subscription end date provided for org [\{0}] , it should be in the format: {1}	If a Subscribed Organizations column includes an end date, the end date must be in the same format as the current organization.
Invalid organization subscription start date provided for org [\{0}] , it should be in the format: {1}	If a Subscribed Organizations column includes a start date, the start date must be in the same format as the current organization.
Unrecognized organization subscription value provided for org [\{0}]	If a Subscribed Organization column is included, the correct name of an organization that is enabled for subscription must be used. When assigning subscription dates, use a single colon (:) and a single pipe (|). Do not use double colons (::) or double pipes (|).
Organization subscription start date provided for org [\{0}] cannot be earlier than current date	If a Subscribed Organizations column includes a start date, the start date must be later than the current date.

Export users to a file

1. In the navigation bar, click **Users** > **Users**.
2. Select the check boxes beside the users you want to export.

   Note: To include dependent users in the export, choose **Sponsors and Non-Sponsors** or **Sponsors** from the pull-down menu and then select **Include Dependents**.
3. On the **Users** screen, click **More Actions** > **Export** > **Users**.
4. On the **Export Users** screen, click **Add >** to select the columns you want to include in the export file.

   Note: The export process allows you to export up to 79 columns of user data into a .pdf file.

   Note: You cannot include the password column in the export file.
5. Optionally, use the **Move Up** and **Move Down** buttons next to the **Selected Columns** field to change the order the information appears in the export file.

   Note: Click the **Reset to columns displayed in User List** to reset the Selected Columns field to its default values.
6. Click **Export PDF** or **Export CSV**.

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

Note: If you include a geolocation attribute in the export, if the user profile contains a physical address in the geolocation attribute, it is exported to two columns. The first column displays the geolocation attribute in the POINT(longitude latitude) format. The second column displays the attribute as the text string the user entered in their profile. For example, if you have a geolocation attribute called Office Location, a column with a heading Office Location is exported that contains the address in the POINT (longitude latitude) format. A second column with a heading Office Location (Physical Address) is exported that contains the text string the user entered in their profile.

Make mass changes to user details

Note: The following instructions explain how to make global changes to details about users in the BlackBerry AtHoc system. To make a change to an individual user, see Edit user details.

The quickest and easiest way to make mass changes to users in the system is to export the user details as a .csv file, open and modify that file, and then import the file back into the system.

Export the user details

1. In the navigation bar, click **Users** > **Users**.
2. If the users already appear in the results table, select the check boxes beside their names. Otherwise, use the **Search** field to locate them, and then select the corresponding check boxes.
3. Click **More Actions** > **Export** > **Users**.
4. In the **All Columns** field, select the columns you want to modify and then click **Add >** to move them to the **Selected Columns** field. To include all columns, click **Add All** at the top of the **All Columns** field.
5. Click **Export CSV**.
6. Save the file to your desktop or to a location you can access easily.

Modify the export file

1. Open the export file.

   Note: In most cases you will be viewing the file through Microsoft Excel.
2. Locate the column of information that you want to update.
3. If you are replacing the current values in the column with different values for each user, type or paste the values in each cell individually.

   If you are replacing the current values in the column with the same value for every user (for example, replacing an old office address with a new one) do the following:

   a. Type or paste the new value in the cell immediately below the header cell.
   b. Position your cursor over the bottom right corner of the cell and click and hold as you drag the cell downward to the end of the column.
   c. When you release the cursor, all of the values will be replaced by the entry you typed in the first cell.
4. Save the file.

Import the modified user details

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click **More Actions** > **Import** > **Users**.
3. Click **Browse**.
4. Navigate to the location of the file you modified on your computer.
5. Click **Open**.

Search for users

By default, the search engine uses an AND operator between the search criteria in the search field. All search results will contain both criteria. For example, entering `john smith` returns all users containing both `john` and `smith`. For a basic search, the system looks for matches in the user's display name, last name, first name, and username.

To use an OR operator, separate the search criteria by a comma in the search field. For example, entering `john,smith` returns all users containing `john`, or `smith`, or both.

To search for an exact string, enclose the search criteria in quotes. For example, entering `"smith,john"` returns only users containing the exact string `smith,john`.

Each criteria pill under the Search field has an AND relationship to other criteria. For example, if you have two existing pills, `John` and `jSmith` and then enter the search string `Smith` in the Search field and click the Search icon, all search results will contain `John`, `jsmith`, and `Smith` in at least one of the following fields: display name, first name, last name, or username.

In advanced searches, when multiple attributes are included in a search, you can select the AND/OR operator. AND is selected by default. The AND/OR operator applies within a search condition and between multiple search conditions. For example, if AND is selected, and the search conditions `Last Name starts with smi` and `First name contains joh` are entered, both conditions must be met for a username to appear in the search results. When OR is selected, users with any of the conditions appear in the search results.

The search engine matches any set of letters or numbers anywhere in a word or ID. For example, a search for `man` returns values such as Manager, Germany, and John Hilman, and a search for `134` returns 134506, 721349, and 863134.

The search is not case-sensitive. For example, searching for `Man` or `man`, produces the same results.

Wildcards are not supported in searches.

Run a basic search for a user

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, in the **Search** field, type or paste all or part of any of the following user-related search criteria: display name, first name, last name, or username. You can also enter group-related search criteria for hierarchy nodes or distribution lists.
3. Optionally, select the **Include Dependents** option to include dependent users in the search results.
4. Click 🔍 to view the results. The search terms you enter appear in a pill under the Search field.
5. Optionally, add additional search terms and click 🔍. Additional pills appear under the Search field for each entered criteria. When a new pill is added, the total count of matching results is updated below the Search field.
6. Optionally, click the ☒ icon in a search pill to remove the pill. The search results update to display the users that match the remaining search criteria
7. Optionally, filter search results by user type.
8. Optionally, click **Clear All** to remove all search pills.

Include groups as search criteria

Use the 👥 (groups) button to open the **Select Groups** window and include distribution lists, organization hierarchy nodes, or targetable groups as additional search criteria.

1. On the **Users** screen, click 👥.
2. On the **Select Groups** window, select the groups to include in the search.
3. Click **Apply**. The selected groups, lists, and nodes appear as separate pills beneath the search field.
4. Click 🔍 to view the results.

Run an advanced search for a user

Note: Before running an advanced search, see Search engine overview for important information on how the search engine works and Advanced search attribute types for a complete list of user attributes you can use to create advanced searches.

You can run an advanced search for a user that includes organizational hierarchies and user attributes as search criteria.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click **Advanced**.
3. On the **Create Conditions** window, select the **AND** or **OR** operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
4. Click **Select Attribute** and select the attribute you want to add to the search.

   Note: The list that appears contains all organizational hierarchies and attributes you have access to in the system.
5. After you make an attribute selection in Step 4, a **Select Operation** field appears. Select an operation.
6. After you make an operation selection in Step 5, a third field appears. Depending on the attribute type selected in Step 4, the third field can be a text-entry field, a drop-down list, a date field, or any other field types listed in Advanced search attribute types. Enter or select a value in the field.

   Tip: For Multi-select Picklist, Single-select Picklist, and Status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.
7. Optionally, click **Add Condition** to add another attribute condition to the search, then repeat steps 4 through 6.
8. Click **Apply**.

The search results display all users who match the attribute conditions you created.

Advanced search attribute types

The following table lists the different attribute types, operators, and values you can use in an advanced search. It also provides examples to illustrate how each attribute criteria would appear in the advanced search field.

Attribute Type	Operator	Value	Examples
Checkbox	• IsYes • IsNotOrEmpty	• Yes	• Currently Online is Yes • CPR Certified is No

Attribute Type	Operator	Value	Examples
Date	• Equals • NotEquals • Before • After • IsEmpty • IsNotEmpty	• Date Panel (showing date value + Past & Next x days value) • Hide	• Joining Date equals 5/4/2022 • CPR Expiration Date older than Sysdate - 30 days • Expiration Date is empty
Date Time	• Before • After • IsEmpty • IsNotEmpty	• Date Time Panel (showing date value + Past & Next x days value)	• Age is empty • Age is not empty
Geo-aware Single-select Picklist	• Equals • NotEquals • IsEmpty • IsNotEmpty	• Single-value selection option of a geolocation	• Home Office equals Mountain View
Geolocation	• IsInside • IsOutside	• Map screen to show selections • Hide	• Home Location is inside shape on the map
Memo	—	—	—
Multi-select Picklist	• Equals • NotEquals • IsEmpty • IsNotEmpty	• Multi-value selection options	• Emergency Community not equals Fire • Rank equals Commander, Captain
Number	• Equals • NotEquals • LessThan • GreaterThan • GreaterThanOrEqualTo • LessThanOrEqualTo • IsEmpty • IsNotEmpty	• Whole number without decimals • Hide	• Age equals 30 • Age greater than 18 • Age less than 65 • Age is empty • Age is not empty
Single-select Picklist	• Equals • NotEquals • IsEmpty • IsNotEmpty	• Single-value selection option	• Building is not empty
Status	• Equals • NotEquals • IsEmpty • IsNotEmpty	• Alphanumeric text	• Status is Safe

Attribute Type	Operator	Value	Examples
Text(String)	• Equals • NotEquals • StartsWith • EndsWith • Contains • DoesNotContain • IsEmpty • IsNotEmpty	• Alphanumeric text • Hide	• First Name equals John • First Name starts with A • First Name contains andy • First name is empty
Org Hierarchy	• At • AtOrBelow • NotAt • NotAtOrBelow	• Multiselection of node in hierarchy	• <Node name or names>

Search for users by User Last Updated Source

Operators can search for users by the source that last updated the users' profiles. This can be useful for operators who want to set up rules to automatically disable user accounts based on when a user profile was last updated and by the source that updated the profile. Searching for users by source can also be used to track who is modifying user accounts. The following table lists the possible sources and the search terms required to search by source.

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

1. In the navigation bar, click **Users** > **Users**.

2. On the **Users** screen, click **Advanced** beside the search field.
3. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
4. From the **Select Attribute** list, select **User Last Updated Source**.
5. Select an operation from the **Select Operation** list.
6. In the blank field that appears, enter the source you want to search 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.
7. Click **Apply**.

Filter search results by user type

You can limit the types of users to include in search results before running the search or after generating results.

Click the links below the search field and then select from the following filter options:

- **Enabled Users**: Search results include enabled users only, excluding disabled users. This option is selected by default.
- **All Users**: Search results include everyone.
- **Enabled Users with Operator Permissions**: Search results include all enabled users who have been granted operator permissions. Results exclude disabled users with operator permissions and all users without operator permissions.
- **All Users with Operator Permissions**: Search results include all users who have been granted operator permissions regardless of whether the user is enabled or disabled. Results exclude all users without operator permissions.
- **Sponsors and Non-Sponsors**: Search results include all users regardless of whether they have dependents. This option is selected by default.
- **Sponsors**: Search results include only users who have dependents.
- **Non-Sponsors**: Search results include only users who do not have dependents.
- **Include Dependents**: Search results include dependents.

Customize search results columns

1. Click **Add** in the header row of the **Users** list. A blank column appears in the table.
2. Click ⌄ in the **Select a column to add** field to view the available user attributes and devices you can add to the results list.
3. Click to select one of the options. The table refreshes to display the new column.

Note: To remove any of the search result columns that you added, click the X icon beside the column header. The Display Name/Username column appears by default and cannot be removed.

Select search results

After you run a search, you can select individual users or all users from the search results list.

- To select individual users, select their corresponding check box in the first column.
- To select all search results, select the check box in the column header of the first column.

When users are selected, click **More Actions** and select any of the following actions:

- Enable the selected users
- Disable the selected users
- Delete the selected users
- Export the user information to .csv
- Export the user information to .pdf
- Move the user to another organization

Note: Subscribed users from other organizations that appear in the search results can be viewed but not edited, disabled, deleted, or exported.

Note: The Users list also contains a link that allows you to import users from a spreadsheet or other file, which does not require the selection of users from the search results.

Sort search results

To sort search results, click a of the column header to sort the results based on the data in the selected column.

After you click the column header, a small ▲ (**Up**) or ▼ (**Down**) icon appears beside the name, indicating which column the data is being sorted by and the direction of the sort.

Click the same column header again to sort the data in the other direction: for example, ascending or descending, alphabetical or reverse alphabetical, or largest or smallest value.

If dependents are enabled in your organization, the **Sponsor** column appears. Sorting on this column displays dependent users under their sponsors.

Reset the search field

To reset the search field, which removes all search criteria and returns the search table to its default state, click **Clear all** next to the user link after you have run a search with at least one search criteria.

Note: Clicking the **Clear all** button does not remove any filtering on the search screen. For example, if users are filtered by a specific kind of user such as enabled users or sponsors, clicking **Clear all** does not affect those settings.

View user details

Note: You must be an End Users Manager to view detailed information about users in the BlackBerry AtHoc system, including contact address, memberships, login information, and location information.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click a user name.

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

   - Basic information including:
     - Username
     - Display name
     - First and last name
     - Date the user was created
     - Sponsor (if dependents are enabled.) If the user is a dependent, their sponsor's Display Name is displayed. If the user is a sponsor, the Sponsor field displays their Display Name with (Self).
   - Numbers
   - Online addresses
   - Physical addresses. Displays the time the user's location was last updated. To view the user's location on a map, click 🌐.
   - Last Known Location. Populates with location information from a check-in, check-out, alert response, report, emergency, or tracking from the BlackBerry AtHoc mobile app. Click 🌐 to view the user's last known location on a map. Click **Clear** to remove the last known location. The last known location cannot be edited from the BlackBerry AtHoc management system or Self Service.
   - Distribution list membership
   - Password
   - Organization subscriptions
   - Permissions
   - Login and location
   - BlackBerry AtHoc Apps: Shows whether the user is active on the BlackBerry AtHoc desktop app or mobile app. If the user is logged in, the number of instances they are logged in to on each app is displayed. If the user is not logged in, the field displays the phrase *Not Available*.
   - User activity, including:
     - Self Service last sign-on, profile updated, and device information updated dates
     - Do not auto delete or disable settings
     - User move information including date the user was moved, who moved the user, and what organization the user was moved from
   - Any user attributes defined by administrators

View operator roles in multiple organizations

If an operator has roles and permissions in multiple organizations, you can view the operator's roles in the organization you are currently logged in to from the Permissions section of the operator's profile page. You can also view the operator's roles in other organizations from the user manager page and from the operator's profile page.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** page, do one of the following:

  - In the **Roles** column, click **Roles in {x} other organizations**.
  - Click the row for the operator you want to view. In the user profile page, in the **Permissions** section, click **This user has roles in {x} other organizations**.

The **Roles in other organizations** window opens and displays the roles the operator has in each organization.

View user activity

The Activity List screen enables authorized users to view all activities for individual users in the BlackBerry AtHoc system. Click a specific user activity to open an activity details screen that provides information about the activity and any response the user made.

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

   The user details screen opens, displaying information for the user in the system.
3. Click **More Actions** > **View Activities**.
4. Click a specific activity to view more details.

The details of the activity appear to the right of the activities list.

For each activity, the following details are displayed:

- Title
- Content
- Date and time the activity was initiated or created
- Publisher
- The timeline for the activity, listing all devices the activity was sent to and the time the alert was sent and received. The timeline also lists details about instances where the alert was responded to, but ignored by the system.
- If the alert was responded to, a Responded section appears above the Activity Timeline, displaying the date and time and responding device of the first response received.

Export user activity details

You can export the user activity details to a .pdf file. You can export one or all activities for a user.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the user name.
3. On the user details page, click **More Actions** > **View Activities**.
4. Choose which activities to export:

   - To export all activities, click **Export PDF**.
   - To export a specific activity:

     a. Click a specific activity. The details of that activity appear beside the activities list.
     b. Click the PDF in the corner of the activity details field.

Manage users

This document describes how to manage users in the BlackBerry® AtHoc® system. Users can be the end users that receive alerts, dependents of users, operators with varying degrees of privileges, or administrators that configure BlackBerry AtHoc settings.

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

For information about operator roles and permissions, see the *BlackBerry AtHoc Operator Roles and Permissions* guide or the *BlackBerry AtHoc Roles and Permissions Matrix*.

Quick Action Guides

View all Quick Action Guides

- Manage operator roles and permissions
- Create a user
- Create a static distribution list
- Create a dynamic distribution list

Create dependents for a user

You can add dependent accounts for users with family members or others that should receive alerts when they do. Users with dependents are referred to as sponsors. Sponsors and administrators can add a dependent account for anyone who should receive alerts but does not have an account in the BlackBerry AtHoc system.

A dependent is a sub account of a sponsor user. The sponsor user has full control to create, edit, and delete their dependents from Self Service.

The operator has the option to include dependents when sending out an alert or requesting accountability status.

Dependents can respond to alerts and update their status for events from the Self Service Inbox if a password is added to their user profile and manual user authentication is enabled for Self Service in the organization.

If a dependent does not respond to an accountability event, the sponsor user may be requested to provide the status of the dependent through the Self Service Inbox.

The layout of the user page for dependent users is different than the layout for sponsors. If there are attributes that should be included for dependents, the administrator must modify the page layout for dependents from **Settings** > **General Settings**.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Users** > **Users**.
3. On the **Users** screen, search or scroll down the users list to find the sponsor user you want to add a dependent for.
4. Click the row with the sponsor user's name.
5. On the user details screen, click **More Actions** > **View Dependents**.
6. On the **Dependents** screen, click **New**.
7. On the **New Dependent** screen, in the **Basic Information** section, enter a Username, First Name, Last Name, and Display Name. Only a Username is required.
8. Optionally, in the **Online Addresses** section, add contact information for the dependent.

9. Optionally, in the **Password** section, enter and confirm a password for the dependent. You must enter and confirm a password if you want the dependent to be able to log in to Self Service to view and respond to alerts and events.
10. Click **Save**.
11. Click **Back** to return to the Dependents screen.
12. Optionally, repeat Steps 6 to 11 to add additional dependents for the sponsor user.

Import dependent users

To import dependent users, include the username of the sponsor in a Sponsor column in the import .csv file.

The following conditions apply to importing dependent users with a .csv file:

- The dependents feature must be enabled for your organization.
- The username of the sponsor must already exist in the BlackBerry AtHoc system before attempting the import.
- You cannot import a user as a dependent if they are already in the system as a sponsor.
- Dependents can only be imported into the organization of their sponsor.
- Dependents must have unique usernames in the BlackBerry AtHoc system.
- If partial user import is enabled and there is an error in the sponsor user row, the dependent user is imported as a standalone user, not as a dependent of the sponsor.
- You can change the sponsor of a dependent to another sponsor in the BlackBerry AtHoc system.
- You can change a sponsor user into a dependent user by setting their sponsor attribute to the username of another sponsor user.
- You cannot import both the organization attribute and the sponsor attribute in the same file. This prevents a dependent from being created in a different organization than their sponsor.

View or edit a dependent

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Users** > **Users**.
3. Optionally, to view or edit the details for a dependent from the Users page:
    a) On the **Users** screen, select **Sponsors** from the pull-down menu under the search field.
    b) Select the **Include Dependents** option.
    c) Click the column header of the **Sponsor** column to sort the list of sponsors and their dependent users. Dependents are displayed under their sponsors.
    d) Click the row with the dependent's name.
4. Optionally, to view or edit the details for a dependent from a sponsor's profile page:
    a) Search or scroll down to find the sponsor.
    b) Click the row with the sponsor user's name.
    c) On the user profile page, click **More Actions** > **View Dependents**. The Dependents screen opens.
    d) Optionally, on the **Dependents** screen, enter a name in the **Search by name** field to find a specific dependent.
    e) On the **Dependents** screen, click the row for a dependent.
5. On the dependent profile page, edit the basic user information, contact information, or password as needed.
6. Optionally, in the **BlackBerry AtHoc Apps** section, click **Active** (*x*) beside **Mobile App** to delete the dependent's unused mobile device. On the **User Mobile Devices** window, click ✖ beside the mobile device to delete.
7. Click **Save**.

Delete a dependent

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Users** > **Users**.
3. Optionally, to delete a dependent from the Users page:
   a) On the **Users** screen, select **Sponsors** from the pull-down menu under the search field.
   b) Select the **Include Dependents** option.
   c) Click the column header of the **Sponsor** column to sort the list of sponsors and their dependent users. Dependents are displayed under their sponsors.
   d) Select the check box in the row with the dependent's name.
   e) Click **More Actions** > **Delete**.
   f) On the confirmation dialog, click **Delete**.
4. Optionally, to delete a dependent from a sponsor's profile page:
   a) Search or scroll down to find the sponsor.
   b) Click the row with the sponsor user's name.
   c) On the sponsor profile page, click **More Actions** > **View Dependents**. The Dependents screen opens.
   d) Optionally, on the **Dependents** screen, enter a name in the **Search by name** field to find a specific dependent.
   e) On the **Dependents** screen, click the row for a dependent.
5. On the dependent profile page, click **Delete**.
6. On the confirmation dialog, click **Delete**.

Deleting a dependent cannot be undone.

Prioritize personal devices for dependents

Before you begin:

- Device delivery preference must be enabled for the organization.
- At least one personal device must be enabled in the organization.
- The dependent must have at least one enabled device with an address in their profile.
- You be an Enterprise Administrator, Organization Administrator, End Users Manager, or Advanced Alert Manager to prioritize personal devices for a dependent.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select the user whose dependents you want to update.
4. On the user details page, click **More Actions** > **View Dependents**.
5. On the **Dependents** screen, click **Prioritize Personal Devices**.
6. On the **Prioritize Personal Devices** window, click ⇕ and drag to reorder the device. Personal devices are prioritized according to their position in the list, with the highest priority device appearing on top.
7. Click **Save**.

Manage organization subscriptions

This section describes how to manage organization subscriptions for users in enterprise organizations.

Use organization subscriptions to enable users in an enterprise organization to receive alerts and accountability events from other suborganizations in their enterprise organization. This feature enables users to subscribe on a temporary basis to up to 10 suborganizations. The subscribed user can then receive any alerts or events that are targeted to them in their home organization as well as in their subscribed organizations. The user's home organization is the organization where their profile is stored. A user's subscribed organization is an organization that a user can be targeted in, but their profile does not get moved to.

Subscribed users can be targeted from their subscribed organization using email, SMS, phone, and mobile app devices and can be targeted using any targeting criteria such as location, groups, or attributes. Targeted devices must be enabled on both the home and subscribed organizations. When targeting subscribed users by attributes, those attributes must be enterprise-level attributes.

The organization subscription feature is disabled by default and must be enabled by a System Administrator. Enterprise Administrators select the suborganizations within their enterprise organization that are available for subscription.

Users can be subscribed to a maximum of 10 available organizations.

Once organization subscriptions are enabled, operators can subscribe users from the BlackBerry AtHoc management system or by using the .csv user import process. Users in suborganizations can subscribe themselves to enabled suborganizations from Self Service or the mobile app. The Organization Subscription for End Users option in the Customization > Self Service section in General Settings must be selected in a suborganization for it to appear for subscription in Self Service. This option is enabled by default.

If the organization subscription feature is disabled, any existing subscriptions are cancelled. Administrators and users can set a start date, set an end date, or cancel their subscriptions.

The profiles of users who are subscribed to organizations remain on the home organization.

On the subscribed organization, subscribed users are visible in search results, can be added to distribution lists, and can be targeted in alerts or events. Their profiles can be viewed, but not edited or deleted, from the subscribed organization. Two new standard user attributes "Temporary work location" and "Subscribed Organizations" have been added to enable searching and targeting subscribed users.

Standalone users and sponsor users can subscribe to organizations. Dependents cannot be subscribed to other organizations.

User uniqueness must be enabled on the enterprise organization before organization subscriptions can be enabled. For more information, see the *BlackBerry AtHoc Enterprise Features* guide.

Subscribe users to organizations

This section describes how to subscribe users to suborganizations other than their home organization using the BlackBerry AtHoc management system or the .csv user import process. For instructions on subscribing to organizations from Self Service, see the *BlackBerry AtHoc Self Service User Guide*.

Before you begin: Before users can be subscribed to organizations, the following conditions must be met:

- The Organization Subscriptions feature must be enabled on the enterprise organization.
- The Enterprise Administrator must select the organizations that are available for subscription.

The Organization Subscription for End Users option must be selected in the Customization > Self Service section in General Settings in a suborganization for end users to be able to subscribe to that organization from Self Service.

Subscribe a single user

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select a user from the list.
4. On the user profile screen, click **Edit User**.
5. On the user profile screen, in the **Organization Subscriptions** section, click **Add Subscription**.
6. On the **Subscribe Organization** screen, select an organization from the list.
7. Click **Apply**.
8. In the **Organization Subscriptions** section, enter a date or click 📅 to select a start date for the subscription.
9. Optionally, click 📅 to set an end date for the subscription.
10. Optionally, repeat Steps 5 to 9 to subscribe the user to additional organizations. You can subscribe the user to a maximum of 10 available organizations.
11. Click **Save**.

The user can now be targeted in alerts and events from their subscribed organizations.

Subscribe multiple users

You can use the .csv user import process to delete or modify organization subscriptions for multiple users.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select the users you want to subscribe to organizations.
4. Click **More Actions** > **Export** > **Users**.
5. On the **Export Users** screen, in the **All Columns** list, select **Subscribed Organizations** > **Add >**.
6. Click **Export CSV**.
7. Save the .csv file to your local system.
8. Open the .csv file.
9. Update the **Subscribed Organizations** column to add, remove, or modify the organizations for each user. You can subscribe each user to a maximum of 10 available organizations.
10. Optionally, in the **Subscribed Organizations** column, add start and end dates for the subscription. Separate the start and end dates with a pipe (|) character. Use the date format of your current organization. For example: `Sub-Org1: 4/5/2021|8/8/2021, Sub-Org3: 5/5/2021|, Sub-Org4: |7/7/2021`.
11. Save the .csv file.
12. In the BlackBerry AtHoc management system, click **Back** to return to the Users screen.
13. lick **More Actions** > **Import** > **Users**.
14. On the **Import User File** screen, click **Browse** and select the .csv file on your local system.
15. Click **Open**.
16. In the **Select the columns to import** section, select **Subscribed Organizations**.
17. Click **Import**.
18. Optionally, on the **Import Details** window, click **Download Log** to view the results.

The updated users can now be targeted in alerts and events from their subscribed organizations.

View subscribed users

Subscribed users can be viewed in their subscribed organization from the user manager and from search results. Subscribed users cannot be edited or deleted from the subscribed organization.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** page, click **Add**.
3. In the **Select a column to add** list, select **Subscribed Organizations**.

A sortable Subscribed Organizations column is added.

Manage user attributes

User attributes provide powerful ways to organize, filter, and manage users. For example, you can create user attributes to describe characteristics of end users, and then use the attributes to target users for alerts through dynamic distributions lists.

The following sections describe how to view, create, edit, and translate user attributes.

User attributes can also be configured as preset response options in alerts and events. For more information about creating user attributes as response options, see "Configure a response option as a user attribute" in the *BlackBerry AtHoc Create and Publish Alerts* guide.

View a list of user attributes

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, the following information is displayed for each attribute:
    - **Name**: The name that is displayed when the attribute appears in lists or on fields in the BlackBerry AtHoc system.
    - **Type**: The kind of data that corresponds to the attribute: text, number, memo, date, dates and time, single-select picklist, multi-select picklist, geolocation, or check box.
    - **Organization**: Specifies the organization the attribute was created in.
    - **Updated On**: Specifies the date the attribute was last modified.

    Tip: You can sort the list by any column.
4. Click the name of an attribute to view the details.

Out-of-the-box user attributes

The following table describes the user attributes that are included automatically in your system.

Note: The following out-of-the-box attributes include additional subattributes such as Updated By or Updated On:

- Last Known Location
- My Info Updated On
- User Last Updated On

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Accountability Exercise Participation	ACCOUNTABILITY-EXERCISE-PARTICIPATION	Captures response options for accountability events.	Y	Y	Picklist

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Alert Last Responded On	ALERT-LAST-RESPONDED-ON	Captures when a user last responded to an alert.	N	N	Datetime
Created On	CREATEDON	Displays a user's created date.	N	N	Datetime
Display Name	DISPLAYNAME	Displays a user's display name.	Y	N	String
Distribution List Folder	Distribution Lists	Defines the distribution list hierarchy. This attribute is available at every level of an enterprise hierarchy.	Y (Read-only for end users.)	N	Path
Do not Auto Delete User	DO-NOT-AUTO-DELETE-USER	Prevents a user from being automatically deleted.	Y (Operators only.)	Y	Checkbox
Do not Auto Disable User	DO-NOT-AUTO-DISABLE-USER	Prevents a user from being automatically disabled.	Y (Operators only.)	Y	Checkbox
Client Certificates	DSW-CLIENT-CERT	Holds the client certificate subject string when the desktop app performs registration using CAC authentication.	N	N	String
OS Domain Name	DSW-DOMAINNAME	Captures a user's desktop client computer domain name.	N	N	String

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Currently Online	DSW-IS-ONLINE	Captures the desktop client online status. At registration the value is captured as ON. After captured, there is no way to set this value to OFF.	N	Y	Checkbox
Desktop Last Redirected To	DSW-LAST-REDIRECTED	Captures the organization the desktop client was last redirected to.	N	N	String
OS Logon Name	DSW-LOGONNAME	Captures a user's desktop client computer log on name.	N	N	String
Machine IP	DSW-MACHINEIP	Captures a user's desktop client computer IP.	N	N	String
Machine Name	DSW-MACHINENAME	Captures a user's desktop client computer name.	N	N	String
Desktop Client Redirect URL	DSW-REDIRECT-BASEURL	Captures the desktop client redirection organization base URL.	Y (Operators only.)	N	String
Desktop Received Redirect	DSW-REDIRECT-COMPLETE	Indicates whether the desktop client has received redirect settings.	N	Y	Checkbox

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Desktop Client Redirect Organization	DSW-REDIRECT-VPS-ID	Captures the desktop client redirection organization ID.	Y (Operators only.)	N	Number
Desktop Last Sign-On	DSW-SIGNON-TIME	Holds the desktop client first sign on date and time.	N	N	Datetime
OS User Name	DSW-USERNAME	Captures a user's desktop client computer log on name.	N	N	String
Desktop Software Version	DSW-VERSION	Captures a user's desktop client version.	N	N	String
Escalation Group	ESCALATION-GROUP	Group attribute that groups users in an escalation category.	Y	N	Special Attribute
First Name	FIRSTNAME	Captures a user's first name.	Y	N	String
Incident Preparedness Status	INCIDENT-PREPAREDENESS-STATUS	Captures the status of accountability event response options.	Y	Y	Picklist
Incident Prevention Status	INCIDENT-PREVENTION-STATUS	Captures incident prevention status for accountability event response options.	Y	Y	Picklist
Last Known Location	LAST-KNOWN-LOCATION	Captures a user's last known location from the mobile app.	Y (Operators only.)	N	Geolocation

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Last Login Date	LAST-LOGIN-DATE	Captures the date and time an operator last logged in.	N	N	Datetime
Last Name	LASTNAME	Captures a user's last name.	Y	N	String
Username	LOGIN_ID	Captures a user's Username.	Y	N	String
Mapping ID	MAPPING_ID	Captures a user's Mapping ID.	Y	N	String
Organizational Hierarchy	Organizational Hierarchy	Publishes an alert to specific users in a hierarchy. This attribute is used only for standalone and suborganizations and is not applicable at the enterprise level.	Y (Read-only for end users.)	N	Path
Work Availability	PA-AVAILABILITY	Enterprise level attribute that captures a user's work availability status in accountability events.	Y	Y	Picklist
CPR Certified	PA-CPR-CERTIFIED	Enterprise level attribute that captures a user's CPR certification status in accountability events.	Y	Y	Picklist

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Current Location	PA-CUR-LOCATION	Enterprise level attribute that captures a user's current location in accountability events.	Y	Y	Picklist
Office Building	PA-OFFICE-BUILDING	Enterprise level attribute that captures a user's office building in accountability events.	Y	Y	Picklist
Transport Needs	PA-TRANSPORT	Enterprise level attribute that capture's a user's transport needs in accountability events.	Y	Y	Picklist
Pin	PIN	Configures a PIN that a user is prompted to enter during a telephone message. This attribute is not searchable.	Y	N	String
Prevent User Move	PREVENT-USER-MOVE	Enterprise level attribute that prevents users from moving to other organizations.	Y	Y	Picklist
Safety Status	SAFETY-STATUS	Captures a user's Safety Status in accountability event response options.	Y	Y	Picklist

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Self Service First Sign-On	SS-FIRST-SIGNON	Captures the date and time a user first signed in to Self Service.	N	N	Datetime
Self Service Last Sign-On	SS-LAST-SIGNON	Captures the date and time a user last signed in to Self Service.	N	N	Datetime
Self Service My Device Info Updated On	SS-MY-DEVICE-INFO-UPDATED-ON	Captures the date and time a user updated the device information in their profile using Self Service or the mobile app.	N	N	Datetime
My Info Updated On	SS-MY-INFO-UPDATED-ON	Captures the date and time a user updated their profile using Self Service or the mobile app.	N	N	Datetime
Status	STATUS	Captures a user's status.	Y (Operators only.)	Y	Picklist
Temporary Work location	SUB-ORG-TEMP-LOCATION	Captures a user's temporary work location. This attribute is used for organization subscription.	Y	N	Geolocation
Subscribed Organizations	SUBSCRIBED-ORGANIZATIONS	Enterprise attribute that holds a user's organization subscriptions.	Y	N	Picklist

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
System Groups	SYSTEM-GROUPS	Target group attribute that contains the All Users, All Registered Users, and All Sign Out Users attribute values. By default, users are assigned to the All Users group. The All Users group is used in publishing to target all users.	Y (Operators only.)	Y	Multi-select Picklist
Designation	USER-DESIGNATION	Enterprise level attribute used in Situation Response.	Y	Y	Picklist
User Last Updated On	USER-LAST-UPDATED-ON	Captures the date and time when a user record was last updated.	N	N	Datetime
Organization	USER-ORGANIZATION	Enterprise level attribute that filters organization-specific entities used for user moves. This attribute is editable by user sync, user import, and the User API.	Y	Y	Picklist
Preferred Language	USER-PREFERRED-LANGUAGE	Enterprise level attribute that holds a user's preferred language settings.	Y	Y	Picklist

Attribute name	Common name	Description	Editable (Y = Editable, N= Read-Only)	Available as response option	Attribute type
Sponsor	USER-SPONSOR	Maps sponsors to their dependents.	Y	N	String
Password	USR_PSWD	Captures a user's self registration password. This attribute is not searchable.	Y	N	String
Work Availability Status	WORK-AVAILABILITY-STATUS	Status attribute that captures a user's work availability status in accountability event response options.	Y	N	Picklist
ATHOC-GV-KEYS	ATHOC-GV-KEYS	Giant Voice integration attribute.	Y	N	Memo
ATHOC-GV-TYPE	ATHOC-GV-TYPE	Giant Voice integration attribute.	Y	Y	Picklist

Create a user attribute

Note: User attributes can be managed at the system, enterprise, or organization level. Inheritance rules can have an impact on who can use them, so verify that you are creating them at the correct organization level. For more information, see "Manage common content with inheritance" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

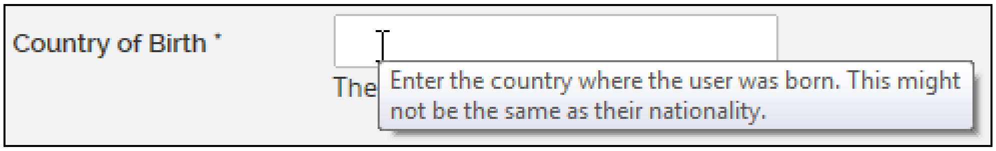
1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, click **New** and select one of the following attribute types:

    - Checkbox
    - Date
    - Date Time
    - Geo-aware Single-select Picklist
    - Geolocation
    - Memo
    - Multi-select Picklist
    - Number
    - Single-select Picklist
    - Status
    - Text

    The New Attribute screen displays the fields required to create a user attribute.

4. In the **Name** field, enter the name that will be displayed when the attribute appears in lists or fields in the BlackBerry AtHoc system. The attribute name has a 128 character limit.

   Note: If the user attribute will be used for preset response options, enter "RO" before the name. Operators can identify it as a response option when publishing an alert.
5. Optionally, in the **Tooltip** field, enter a hint that displays when users hover their cursor over the attribute field.

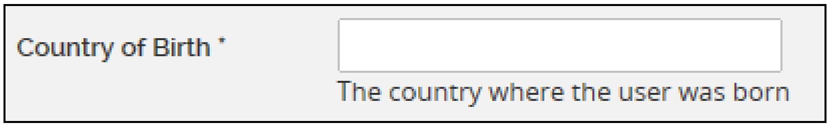


Country of Birth *

The

Enter the country where the user was born. This might not be the same as their nationality.

6. Optionally, in the **Help Text** field, enter text that will appear under the field.



Country of Birth *

The country where the user was born

7. Optionally, modify the **Common Name** value.

   Note: The value of the Common Name field is the same as the attribute Name value by default. You can modify the Common Name, but it is not typically changed. The common name has a 128 character limit.
8. Select **Users Can Update** if users need to modify the value.
9. Select **Mandatory** if the attribute is a required field in user profiles.
10. Optionally, select **Use as a Response Option**.

    Note: Only Checkbox, Geo-aware Single-select Picklist, Single-select Picklist, and Status attribute types can be used as a response option. Attributes used as response options can have up to 9 values.
11. In the **Values** section, click **Add value**. Depending on the attribute type selected, the following fields appears:

Attribute type	**Values fields**
• Checkbox	Select the **Selected by Default** option for the attribute to be selected by default when it appears.
• Date • Date Time	Select the **Earliest Allowed Date Time** and **Latest Allowed Date Time** from the calendar pickers. Set the date-range and time-range for the fields by entering the first and last dates and times it covers.
• Geo-aware Single-select Picklist	**a.** In the **Value** field, enter a value that a user can select from a pull-down list. **b.** In the **Geo location** field, specify a real physical address or location coordinates in the POINT(longitude/latitude) or latitude,longitude format. **Note:** Due to validation of individual geolocation entries in the .csv import file, importing many values will take time. **c.** Optionally, click **Import Values** to import the attribute values from a .csv file. **d.** Specify the order the values appear in the list. The sort order is the same anywhere the attribute is displayed.

Attribute type	Values fields
	e. Click **Save**.
• Geolocation	**a.** Click **Change** beside **Map Icon** to select the icon to display on maps to represent the attribute. **b.** Optionally, select the **Save Location History** option to track where the icon is located on the map over time.
• Memo	—
• Multi-select Picklist • Single-select Picklist	**a.** In the **Value** field, enter a value that a user can select in the attribute field. **b.** Optionally, select a default value. **c.** Optionally, click **Import Values** to import the attribute values from a .csv file. **d.** Specify the order the values appear in the list. The sort order is the same anywhere the attribute is displayed. This is also the order users will be sorted in when sending an alert that contains escalation rules. **e.** Click **Save**.
• Number • Text	In the **Minimum Value** and **Maximum Value** fields, enter the minimum and maximum number of characters that end users must enter in the attribute field.
• Status	**a.** In the **Value** field, enter a value that a user can select in the attribute field. **b.** Specify the order the values appear in the list. The sort order is the same anywhere the attribute is displayed. **c.** Optionally, click **Import Values** to import the attribute values from a .csv file. **d.** Click **Save**.

12. Optionally, in the **Page Layout** section, select the pages and sections where the user attribute appears. For each page listed in the section, click the drop-down list and select the location where you want the user attribute to appear or select **Do not show** to avoid having it appear anywhere on the corresponding page.
13. Optionally, for multi-select, single-select, and geo-aware single-select picklist attributes, complete the **Personnel Reports** section to create a personnel report based on the attribute and its values:

    a. Select the **Enabled** option.
    b. Enter a report name and description.

    You can view this report from **Reports** > **Personnel**.
14. Click **Save**.

Edit a user attribute

Note: User attributes that are created prior to the deployment of the organization cannot be edited within the organization. If editing user attributes on System Setup, do not modify the common name.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.

   The **User Attributes** screen opens, displaying all of the attributes available to users in the organization.
3. Click the user attribute you want to edit.

   Note: You can search by attribute name to filter the list of attributes. You can also display only the attributes that are defined within the organization to filter out inherited enterprise and system attributes.
4. Update the **Basic**, **Values**, **Page Layout**, **Bulk Update Values** and **Personnel Reports** sections.

   Note: The **Info** section cannot be edited. It lists the name of the user who created the attribute, the date it was created, the last user to update the attribute, and the last date the attribute was updated.
5. Click **Save**.

Prevent users from editing System Setup attributes

To preserve the integrity of user data and improve security, administrators can prevent end users from editing the following System Setup attributes from their Self Service profile:

- Username
- First Name
- Last Name
- Mapping ID
- Display name

By default, users can edit these System Setup attributes in Self Service.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. Optionally, click the **Organization** column to sort the list of attributes or use the **Search** field to find the attribute.
4. On the **User Attributes** screen, click the System Setup attribute you want to update.
5. On the attribute details page, in the **Basic** section, deselect the **Users Can Update** option.
6. Click **Save**.

Delete a user attribute

Note: User attributes use inheritance. To delete an attribute, it must be in the organization where you are performing the delete action. If you do not see the Delete button, verify that you are deleting the attribute from the correct organization level in the enterprise. For more information, see "Manage common content with inheritance" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

If a user attribute becomes obsolete, you can delete it and all records of the attribute that are associated with end users.

When you try to delete a user attribute that is currently being used in alert targeting, alert template targeting, preset response options, dynamic distribution lists, or disable and delete users conditions, a pop-up box appears, listing all locations where the attribute appears. Removing an attribute in a user query can have unintended consequences, such as changing the target audience of an alert. To avoid these effects, you must remove the attribute from each of the dependencies manually before you can delete the attribute itself.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, in the **Attribute Name** column, click the name of an attribute that is defined in the organization.
4. On the attribute details screen, click **Delete**.
5. On the **Delete User Attribute** window, click **Delete**.

   Note: If the attribute is being used for alert targeting, preset response options, or any other purpose, you must manually remove the attribute from each dependency before you can access the delete confirmation screen.

The attribute is removed from the system and no longer appears in the User Attributes list.

Clear attribute values for all users

System Administrators can clear the values of some user attributes for all users.

Important: Clearing the values for an attribute cannot be undone.

Before you begin: You must be logged in to the organization where the attribute was created.

1. Click **Users** > **User Attributes**.
2. On the **User Attributes** screen, click the attribute whose values you want to clear.
3. On the attribute details page, in the **Bulk Update Values** section, click **Clear for All Users**.
4. On the **Clear for All Users** dialog, click **OK**.

Translate custom attributes

Enterprise Administrators, Organization Administrators, Alert Managers, and System administrators can add translation strings for custom attribute names, values, and tooltips in any of the following supported locales:

- Deutsch (Deutschland)
- English (UK)
- English (US)
- Español (España)
- Español (México)
- Français (Canada)
- Français (France)
- Italiano (Italia)
- Nederlands (Nederland)

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Translate Custom Attributes**.
3. On the **Custom Attributes Translation** screen, from the **Select Attribute** list, select an attribute.
4. Enter a custom translation for the attribute.
5. If the custom attribute has values, select the value from the **Attribute Value** list.

6. Optionally, enter a translation for the attribute tooltip.
7. Click **Save**.

Automatically disable users based on attributes

In organizations where changes to the user base occur frequently, it is often more efficient to automatically disable users based on one or more user attributes. This helps ensure the user base is kept current and database performance is maximized by reducing the number of active users.

For instructions on how to disable users directly from the Users list, see Disable users.

Note: Automatically disabling sponsors also disables their associated dependents users.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Disable and Delete Users**.
3. On the **Disable and Delete Users** screen, in the **Disable Users** section, select the AND/OR operator. When AND is selected, users must meet all conditions to be added. When OR is selected, users that match any of the conditions are added. The default is AND.
4. Click the **Select Attribute** drop-down list and select the first attribute to use to identify users to be disabled.
5. When you make a selection in the **Select Attribute** drop-down list, the **Select Operation** drop-down list appears. Select an option from the list.
6. In the field that appears to the right of the **Select Operation** field, enter or select a value.

   Tip: For Multi-select Picklist, Single-select Picklist, and Status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.
7. Optionally, to add another condition to the list of criteria that must be met for a user to be disabled, click **Add Condition** and then repeat steps 3 through 6.

   Note: When the AND operator is selected, if more than one condition appears in the Disable Users section, all conditions must be met for a user to be disabled.

   Tip: You can use the User Last Updated by Source attribute to search for and disable users. For more information, see Automatically disable users based on the User Last Updated Source attribute.
8. Select **Disable users automatically every 7 day(s)** to enable a database job that disables users every week.

   Note: If you do not select this option, you must navigate to this screen and click **Disable Now** each time you want to disable users.
9. Optionally, click **Calculate** to see the number of users that will be impacted by the criteria you set.
10. Optionally, consult the **Last Run** field to see the date and time the most recent disable action was performed.
11. Optionally, click **Download Log** in the **Last Run Result** field to download a list of users who were disabled during the last disable action.
12. Click **Save**.
13. Optionally, click **Disable Now** if you want to disable the list of users immediately.

Automatically disable users based on the User Last Updated Source attribute

Operators can set up rules to automatically disable user accounts based on when a user profile was last updated and by the source that updated the profile. The following table lists the possible sources and the search terms required to search by source.

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

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Disable and Delete Users**.
3. On the **Disable and Delete Users** screen, in the **Disable Users** section, select the AND/OR operator. When AND is selected, users must meet all conditions to be added. When OR is selected, users that match any of the conditions are added. The default is AND.
4. Click the **Select Attribute** drop-down list and then select **User Last Updated Source**.
5. Select an operation from the **Select Operation** list.
6. In the blank field that appears, enter the source that you want to disable 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.
7. Click **Save**.

Automatically delete users based on attributes

In organizations where changes to the user base occur frequently, it is often more efficient to automatically delete users based on one or more user attributes. For instructions on how to delete users directly from the Users list, see Delete users.

Note: Automatically deleting sponsors also deletes their associated dependent users.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Disable and Delete Users**.

3. On the **Disable and Delete Users** screen, in the **Delete Users** section, select the AND/OR operator. When AND is selected, users must meet all conditions to be added. When OR is selected, users that match any of the conditions are added. The default is AND.
4. Click the **Select Attribute** drop-down list and select the first attribute to use to identify users to be disabled.
5. When you make a selection in the **Select Attribute** drop-down list, the **Select Operation** drop-down list appears. Select an option from the list.
6. In the field that appears to the right of the **Select Operation** field, enter or select a value.

   Tip: For Multi-select Picklist, Single-select Picklist, and Status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.
7. Optionally, click **Add Condition** to include another condition that must be met for a user to be deleted.

   Note: When the AND operator is selected, if more than one condition appears in the Deleted Users section, all conditions must be met for a user to be deleted.

   Tip: You can use the User Last Updated by Source attribute to search for and delete users. For more information, see Automatically delete users based on the User Last Updated Source attribute.
8. Select **Delete users automatically every 7 day(s)** to enable a database job that will delete users every week.

   Note: If you do not select this option, you must navigate to this screen and click **Delete Now** each time you want to delete users.
9. Optionally, click **Calculate** to see the number of users that will be impacted by the criteria you set.
10. Optionally, consult the **Last Run** field to see the date and time the most recent delete action was performed.
11. Optionally, click **Download Log** in the **Last Run Result** field to download a list of the users who were deleted during the last delete action.
12. Optionally, in the **Purge Deleted Users** section, select the **Purge deleted users after** option and select an interval from the pull-down menu to purge deleted users from the system. For more information, see Purge deleted users.
13. Click **Save**.
14. Optionally, click **Delete Now** if you want to delete the list of users immediately.

Automatically delete users based on the User Last Updated Source attribute

Operators can set up rules to automatically delete user accounts based on when a user profile was last updated and by the source that updated the profile. The following table lists the possible sources and the search terms required to search by source.

Source	Search term
Mobile app	• Check-in • Check-out • Report • Emergency • User Tracking - Mobile App • Mobile
Self Service	SelfService
BlackBerry AtHoc Management System	ManagementSystem
User Sync Client	UserSyncClient
API	API

Source	Search term
CSV Import	UserImport
Targeted Device	• Alert Tracking - Desktop Popup • Alert Tracking - Email • Alert Tracking - Mobile App • Alert Tracking - Phone • Alert Tracking - Text Messaging

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Disable and Delete Users**.
3. On the **Disable and Delete Users** screen, in the **Delete Users** section, select the AND/OR operator. When AND is selected, users must meet all conditions to be added. When OR is selected, users that match any of the conditions are added. The default is AND.
4. Click the **Select Attribute** drop-down list and then select **User Last Updated Source**.
5. Select an operation from the **Select Operation** list.
6. In the blank field that appears, enter the source to use to delete users. 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.
7. Click **Save**.

Configure an Organizational Hierarchy attribute

Organizational Hierarchy attributes define organizational hierarchies that can be selected as alert or event targets. Organizational hierarchies are commonly created by integrating an external user directory, such as LDAP or Microsoft Active Directory.

You can also create an organizational hierarchy by importing it from a .csv file. For more information, see Import an organizational hierarchy.

Note: The BlackBerry AtHoc AD Module for synchronizing users creates the organizational hierarchy from Active Directory. If you are using the AD Module and you make changes to the organizational hierarchy manually, those changes may be lost when the next user synchronization occurs.

Note: The organizational hierarchy attribute is not available in enterprise organizations. Organizational hierarchy attributes are available only in suborganizations or stand alone organizations.

Note: If you update an existing organizational hierarchy and a mapped node is not included in the new hierarchy, any user that is mapped to the excluded node is automatically mapped to the root node. Users can be mapped to the correct node by using a new organizational hierarchy during a user import or user sync.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, click **Organizational Hierarchy**. The Organizational Hierarchy details page opens.
4. Optionally, select **Users Can Update** if users need to modify the value.
5. Optionally, select **Mandatory** if the attribute is a required field in the user profile. If this check box is selected, users must select a node in the organizational hierarchy, and cannot select the root directory.

6. In the **Values** section, click **Add Node** to add a new node to the organizational hierarchy. If no nodes are selected, the new node is added to the bottom of the organizational hierarchy. Select an existing node and click **Add Node** to add a new node under it.
7. Type the node name in the new field and press **Enter**. The node name has a 128 character limit.
8. Optionally, to move a node, drag the node to the new location.
9. Optionally, to edit a node name, double-click on the node name and type your changes.
10. Optionally, to delete a node, select the name and click **Delete Node**.
11. Optionally, to revert your changes, click **Remove Changes**.
12. Click **Save**.

All new and modified nodes are displayed in italics until saved.

Note: When you make changes to the organizational hierarchy, you must click **Save** to save your changes. If you navigate to another page, your changes are not saved. If you attempt to export the organizational hierarchy before saving, your changes are not exported.

Import an organizational hierarchy

You can create a new organizational hierarchy or update an existing one using an import .csv file. Include the hierarchical node in the Node Name column and the path in the Node Path column of the import file.

Tip: To modify an existing organizational hierarchy, follow the steps in Export an organizational hierarchy, save and update the downloaded .csv file, then import the updated organizational hierarchy.

- The import .csv file must have the two required columns Node Name and Node Path.
- Both required columns must contain a value. Empty cells in the .csv file will result in an error.
- The import process replaces the existing organizational hierarchy.
- Do not include double slashes (//) in the node path or node name.
- Do not include duplicate records in the import .csv file.
- The first level of each path should be the root node and represented as a forward slash (/).
- Up to 30 levels are allowed in one node path.
- Up to 500 nodes can be imported in a single import.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Users** > **User Attributes**.
3. On the **User Attributes** screen, find and click the **Organizational Hierarchy** attribute.
4. On the **Organizational Hierarchy** screen, in the **Values** section, click **Import**.
5. Optionally, on the **Import Organizational Hierarchy** screen, click **Download Template CSV file** or **View Instructions**.
6. On the **Import Organizational Hierarchy** screen, click **Browse**, then browse to and select the .csv import file.
7. Click **Import**.
8. When the import is complete, the **Import Organizational Hierarchy results** window opens.
   Click **Close** or **Download Log**.
9. Click **Save**.

   When you make changes to the organizational hierarchy, you must click **Save** to save your changes. If you navigate to another page, your changes are not saved. If you attempt to export the organizational hierarchy before saving, your changes are not exported.

Export an organizational hierarchy

To update an existing organizational hierarchy, you can export it to a .csv file, make updates, and then import the file.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click **Users** > **User Attributes**.
3. On the **User Attributes** screen, find and click the **Organizational Hierarchy** attribute.
4. On the **Organizational Hierarchy** screen, in the **Values** section, click **Export to CSV**.

   Any changes you make to the organizational hierarchy must be saved before you export the organizational hierarchy.

A .csv file containing the organizational hierarchy is downloaded to your local computer.

Create a Geo-aware Single-select Picklist attribute

Create a geo-aware single-select picklist attribute to enable geo-targeting of users on the live and publisher maps without the need to import and define shape layers. Administrators create geo-aware single-select picklist attributes and define a specific geolocation by entering a physical address or location coordinates in the POINT(longitude/latitude) or latitude,longitude format. Operators can draw a custom shape on the map (or select a predefined shape) and target users that have selected that location in their user profile in the BlackBerry AtHoc management system or Self Service.

Geo-aware single-select picklist attributes can be edited by end users or operators, found in advanced searches, and used as response options.

Bulk-clear for all users is available for geo-aware single-select picklist attributes.

1. In the BlackBerry AtHoc click **Users** > **User Attributes**.
2. On the **User Attributes** screen, click **New** > **Geo-aware Single-select Picklist**.
3. On the **New Attribute** screen, in the **Name** field, enter the name that will be displayed when the attribute appears in lists or fields in the BlackBerry AtHoc management system. The attribute name has a 128 character limit.
4. Optionally, enter text in the **Tooltip**, **Help Text**, and **Common Name** fields. For details, see Create a user attribute.
5. Optionally, select **Users Can Update**, **Mandatory**, and **Use as a Response Option** as needed. For details, see Create a user attribute.
6. In the **Values** section, click **Add value**.
7. In the **Value** field, enter a value that a user can select from a pull-down list.
8. In the **Geo location** field, enter a real physical address or location coordinates in the POINT(longitude/latitude) or latitude,longitude format.
9. Click **Save**.
10. Repeat steps 6-9 to add additional values.
11. Optionally, click **Import Values** to import the attribute values from a .csv file. The import .csv file must include columns for the value names and geo location values. You can elect to replace current values for the attribute with the values in the import .csv file. Due to validation of individual geolocation entries in the .csv import file, importing many values will take time.
12. Optionally, in the **Page Layout** section, select the pages and sections where the user attribute appears. For each page listed in the section, click the drop-down list and select the location the user attribute appears or select **Do not show** to avoid having it appear anywhere on the corresponding page.
13. Optionally, in the **Personnel Reports** section, select the **Enabled** option and then enter a name and description. The report is available to view in **Reports** > **Personnel**.
14. Click **Save**.

Manage user authentication

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

The user authentication settings establish the login protocol and user authentication rules used for BlackBerry AtHoc.

Enable authentication methods

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select the check boxes beside the authentication methods you want to use in the BlackBerry AtHoc management system.

   The following authentication methods are available:

   - **LDAP Attribute**: Applicable for the desktop app only.
   - **Smart Card**: When this option is selected, the operator must select a valid certificate on their device.
   - **Username and Password**: When this option is selected, you can also enable two-factor authentication for operators and Self Service. For more information, see Enable two-factor authentication.
   - **Windows Authentication**: Select an option to authenticate with a username only, or with a domain and username.
   - **Single Sign-On (SSO)**: Enable single sign-on. This option is not available for the desktop app.
4. Click **Save**.

Note: The options selected in this section determine the options available for selection in the Assign Authentication Methods to Applications section.

Assign authentication methods to applications

You can specify the authentication method to use for the mobile app, desktop app, Self Service, and the BlackBerry AtHoc management system.

Mobile app

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods for mobile app from the **Authentication Method** list:

   - **Smart Card**: This option enables smart card authentication. When smart card authentication is enabled, when an operator starts the alert publishing, report summary, or accountability officer respond-on-behalf-of-others (ROBO) flows, a window appears for the operator to select a valid certificate. The certificate must already be present on the operator's device. When a valid certificate is selected, the operator can then complete the flow. If the selected certificate is not valid, the operator is redirected to the username and password login screen. When the operator selects a valid certificate, they are redirected to the mobile app to complete the flow. If the selected certificate is not valid, or the smart card authentication fails, the operator is redirected to authenticate using their username and password.
   - **Username and Password**: This option requires operators to authenticate using their BlackBerry AtHoc username and password. This option is selected by default and cannot be deselected.

Note: This section appears only when the mobile app gateway is enabled and configured.

4. Optionally, select the **Create New User if an Account is not Found** option.

   Note: When this option is enabled, user profiles are created automatically using the mobile app. In this case, the provided email is used as the username. If users are then created by other means such as .csv import, API, or the User Sync Client, and email is not used for the username, duplicate users may be created.
5. Click **Save**.

Desktop app

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods for the desktop app from the **Authentication Method** list:

   - **LDAP Attribute**: This option enables the desktop app to authenticate with a Microsoft Active Directory attribute that you provide in the **Attribute** field. The desktop app queries this attribute directly from the signed-in user's directory profile and sends it to the server. This option allows the desktop app to operate while sending less user information to the server. When this option is selected, the desktop app does not send Windows user names or domain names in sign on or check update query strings.

     Note: This option requires desktop app version 6.2.x.271 or later.
   - **Smart Card**: This option enables smart card authentication.

     - From the **Number of Certificates** list, select the number of client certificates to collect. The recommended value is 3.
     - Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=(?<edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.
     - Optionally, in the **Client Regular Expression** field, enter a client regular expression in the following format: `.*?(^)(?:(?!\s-[A||E||S]).)*`. This format extracts information from the client certificate subject name to find the identical certificates for authentication. The regular expression provided in the UI is a sample expression that may not be suitable for your environment. You can build you own regular expression or contact BlackBerry AtHoc customer support to configure this field.
     - Optionally, select **Create new user if an account is not found** to configure the desktop app to create a user at sign on if the user does not already exist.
   - **Defer to Self Service**: This option requires users to sign in using a registration window determined by the authentication type configured for Self Service.

     - If the Self Service authentication method is set to Username and Password, the users sees a registration window and must provide their first name, last name, username, password, confirm their password, and fill in a captcha. The user has the option to register as a new user or to sign in with their existing user credentials.
     - If the Self Service authentication method is set to Smart Card, the user sees a CAC Certificate selection screen and must pick a certificate.
     - If the Self Service authentication method is set to Windows Authentication, the user sees a Windows credentials screen and must provide their username and password.
     - If the Self Service authentication method is set to Single Sign-On, the user is sent to a configured external URL for single sign-on.
   - **Windows Authentication**: This option configures the desktop app to use only the Windows username or to use both the Windows username and the domain.
4. If LDAP Attribute, Smart Card, or Windows Authentication is selected, you can select **Create new user if an account is not found** to configure the desktop app to create a user at sign on if the user does not already exist.
5. Click **Save**.

Self Service

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods for Self Service from the **Authentication Method** list:

    - **Smart Card**: This option enables smart card authentication. Select the number of client certificates to collect. The recommended value is 3.
    - **Username and Password**: This option requires users to sign in to Self Service using their BlackBerry AtHoc username and password.
    - **Windows Authentication**: This option configures Self Service to use only the Windows username or to use both the Windows username and the domain.
    - **SSO Single Sign-On (SSO)**: This option enables the use of an external URL for single sign-on. For more information, see Enable single sign-on as an authentication method.
4. Optionally, if you selected **Single Sign-On** as the authentication method, select **Username and Password** from the **Alternative Authentication Method** list. This option enables both SSO and Username/Password to be used for user authentication.
5. Optionally, if you selected **Username and Password** as the authentication method, select any of the following options:

    - **Option to Save Username on User's Computer**.
    - **Self Registration for New Users**: Select this option to enable new users to self register for Self Service. Click **Modify Fields** to select the attributes and personal devices that are used as fields on the Registration screen. On the **Self Registration fields** dialog, add or remove fields. The Username and Password fields are included by default and cannot be removed. You can add up to 8 additional fields. If you include an email field, the Use Email as Username option appears.
    - **Use Email as Username**: Select this option to require that users enter an email address when registering for Self Service. This email address is used as their username. Select an email from the **Select Email Device** pull-down menu. Only Email fields selected in the Self Registration fields dialog are available for selection.
6. Click **Save**.

BlackBerry AtHoc management system

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods for Management System from the **Authentication Method** list:

    - **Username and Password**: This option requires users to sign in to the BlackBerry AtHoc management system using their BlackBerry AtHoc username and password. This option is selected by default and cannot be deselected.
    - **Single Sign-On**: This option enables the use of an external URL for single sign-on. When this option is selected, the Sign In URL is auto populated. If an organization code is available, the URL format is: <*server*>/client/*organization-code*. If an organization code is not available, the URL format is: <*server*>/client/*provider-ID*. For more information, see Enable single sign-on as an authentication method.
4. Click **Save**.

Configure SDK access security

The SDK Access Security setting allows you to specify a list of IP addresses that are authorized to call the SDK. If no IP addresses are specified, any computer can send API requests (subject to username and password restrictions.) Each API request must include a username and password to provide secure access to the API and to define the rights of specific API requests.

You must have the required operator role to submit an API request. For more information, see the BlackBerry AtHoc Roles and Permissions Matrix.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** screen, scroll down to the **SDK Access Security** section.
4. In the **Allowed IP Addresses** field, enter a list of IP addresses, separated by commas, that are authorized to access the SDK.
5. Click **Save**.

Enable two-factor authentication

You can require all end user or operators in your organization to use two-factor authentication when logging in with a username and password to Self Service or to the BlackBerry AtHoc management system.

When two-factor authentication is enabled for your organization, when a user or operator logs in, they first enter their username and password. They are then presented with a screen to select a verification code delivery method (email, text, or phone.) The user or operator then receives a verification code on their selected device which they enter to continue the login process.

The verification code expires if not used after five minutes. If the verification code expires, or the user or operator does not enter the verification code correctly, they can request a new verification code. If the user or operator attempts to log in with a second verification code, they will need to fill in a captcha field. They can request up to three verification codes. If a user or operator requests more than three verification codes, they are returned to the login page, and an unsuccessful login attempt is logged. This may result in the user or operator account becoming locked if they exceed the number of login attempts defined in the organization's security policy settings.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** screen, in the **Enabled Authentication Methods** section, select the Username and Password **Enable** option.
5. In the **Two-Factor Authentication** section, select the **Require for Operators** and **Require for Self Service** options as needed.
6. Select one or more methods from the **Verification Code Delivery Methods** list.
7. Beside **Users Unable to Log In**, click **Calculate** to see the number of users who do not have any selected delivery methods. If you enable two-factor authentication, users who do not have one of the selected delivery methods will not be able to log in to Self Service.
8. Optionally, click **User(s)** to open the **Users Unable to Log In** window, where you can see which users will not be able to log in. You can export this list to a .csv file, add any missing delivery method information, and import the updated information into the BlackBerry AtHoc system.
9. Click **Save**.

Enable single sign-on as an authentication method

The Single Sign-On feature is not enabled by default. A system administrator must enable SSO in the Feature Enablement settings in the BlackBerry® AtHoc® management system. For more information, see "Enable and disable features" in the *BlackBerry AtHoc System Settings and Configuration* guide.

When SSO is enabled for your organization, if your users are already authenticated and signed in using your identity provider (IDP), they do not need to sign in again to access the BlackBerry AtHoc management system or Self Service.

Note: SSO is supported on the desktop app when the authentication method is set to "Defer to Self Service" and Self Service is enabled for SSO.

If a user is not signed in, they are redirected to their organization's customer IDP login when they attempt to sign in. This IDP is managed by your organization or by a third party vendor that provides IDP services. The IDP authenticates the user. The user is then redirected to BlackBerry AtHoc. If the user is already signed in to the IDP they are automatically redirected to the BlackBerry AtHoc management system or Self Service with an active session.

You must have organization administrator, enterprise administrator, or system administrator permissions to enable single sign-on as a user authentication method.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select the Single Sign-On (SSO) **Enable** check box.
5. Click **Save**.

Enable single sign-on for Self Service

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Self Service** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/selfservice/*organization-code*. This URL is used when users attempt to access Self Service using SSO authentication.
5. Optionally, if you selected **Single Sign-On** as the authentication method, select **Username and Password** from the **Alternative Authentication Method** list to enable both SSO and Username/Password user authentication.

   Note: When an alternative authentication method is added, the Self Service sign-in URL is appended with /sso for single sign-on authentication. For example, <*server*>/selfservice/*organization-code*/sso.
6. Click **Configuration**.

   Note: If the **Configuration** button is not available, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
7. On the **Self Service SSO configuration** window, export SP and IDP settings and then import IDP settings.

   Note: You can also configure the IDP and SP settings manually. For more information, see Configure identity provider settings and Configure service provider settings.
8. Click **Apply**.
9. Click **Save**.

Enable single sign-on for the BlackBerry AtHoc management system

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Management System** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/client/*organization-code*. This URL is used when a user attempts to access the BlackBerry AtHoc management system using SSO authentication.

   Note: If the **Authentication Method** list is disabled, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
5. Click **Configuration**.
6. On the **Management system SSO configuration** window, export SP and IDP settings and then import IDP settings.

   Note: You can also configure the IDP and SP settings manually. For more information, see Configure identity provider settings and Configure service provider settings.
7. Click **Apply**.
8. Click **Save**.

Import a service provider certificate

Import a BlackBerry AtHoc signed service provider certificate for use in Single Sign-On (SSO.) This enables administrators to select a BlackBerry AtHoc certificate instead of uploading and maintaining a custom SP certificate.

You must be a System Administrator to import a service provider certificate.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Security Policy**.
5. On the **Security Policy** page, in the **Service Provider Certificate** section, click **Import Certificate**.
6. On the **Import Certificate** window, enter a valid password for the service provider certificate.
7. Click **Browse** and navigate to and select a valid BlackBerry AtHoc certificate. Only .pfx and .p12 files can be imported.
8. Click **Import**.
9. On the **Security Policy** page, click **Save**.

Configure identity provider settings

The identity provider (IDP) provides authentication for users. The service provider (SP), in this case BlackBerry AtHoc or Self Service, requests authentication from the IDP.

When SSO is enabled for access to the BlackBerry AtHoc management system or Self Service, when a user logs in, they are redirected to their organization's IDP for authentication. If the user is already logged in to the identity provider, the authentication request is processed and sent to the service provider, and the user is granted access without the need to log in again.

1. Log in to the BlackBerry AtHoc management system as an organization administrator or enterprise administrator.
2. Click ⚙.
3. In the **Users** section, click **User Authentication**.

4. On the **User Authentication** page, in the **Assign Authentication Methods to Applications** section in the **Self Service** or **Management System** section, click **Configuration**.

   Note: If the **Configuration** button is not available, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
5. Do one of the following:

   - Import IDP settings.
   - On the **Management system SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, configure the following **General Settings**.

     a. **Identity Provider Name**: Each SAML configuration is identified by a unique identity provider name. This name is internal to the configuration and is not exposed to partner providers. This field is required only when there are multiple SAML configurations. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
     b. **Sign On Service URL**: Enter the URL of the location of the identity provider's SSO service where SAML authentication requests are sent as part of a SP-initiated single sign-on.
     c. **Sign On Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
     d. **Logout Service URL**: The URL of the local service provider's single log out service where SAML logout messages are received. If single logout is not required, leave this field blank. For more information, see SSO logout service.
     e. **Logout Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
     f. **Artifact Resolution Service URL**: Optionally, enter an artifact resolution service URL. The service provider uses the Artifact Resolution Protocol to exchange an artifact for the actual SAML message referenced by the artifact.
     g. **Artifact Resolution Service Binding**: Optionally, select **SOAP**, **POST**, **REDIRECT** or **ARTIFACT** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default is **SOAP**.
     h. **Name ID Format**: Optionally, select **Email Address**, **Persistent**, or **Transient** as the format to be used by the SP and IDP to identify a subject name identifier.
     i. **User Mapping Attribute**: Optionally, select the attribute that identifies the user. This attribute is retrieved from the SAML assertion metadata. The default is **Subject Name**.
     j. **Attribute Name**: Enter the name of the attribute used to identify the user.
6. Configure the following **Security Settings**:

   a. **SAML Response Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML responses sent to the partner service provider must be signed. Sending signed authentication requests is highly recommended, but optional.
   b. **Assertion Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML assertions sent to the partner service provider must be signed.

      Note: You must select **Signed** for either **SAML Response Signature** or **Assertion Signature** or both.

      Note: You must have a valid certificate installed for your organization.
   c. **Signature Algorithm**: Select an algorithm. The default is **RSA-SHA256**.
   d. **Assertion Encryption**: Select **Encrypted** or **Unencrypted**. When **Encrypted** is selected, SAML assertions sent to the partner service provider must be encrypted.
   e. If **Assertion Encryption** is set to **Encrypted**, select an **Assertion Algorithm**. The default setting is **AES128**.
   f. In the **Certificate*** field, click **Browse** to navigate to and select a certificate file. Only .cer and .crt files are supported.

7. Optionally, add the following **Additional information**:

    a. **Company Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
    b. **Company Display Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
    c. **Company URL**
    d. **Contact Person Name**
    e. **Role or Department**
    f. **Email Address**
    g. **Telephone Number**
8. Do one of the following:

    - If you are modifying an existing SSO configuration, click **Apply**, and then click **Save** on the **User Authentication** page.
    - For a new SSO configuration, configure Service Provider settings.

Configure service provider settings

1. Log in to the BlackBerry AtHoc management system as an organization administrator or enterprise administrator.
2. Click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** page, in the **Assign Authentication Methods to Applications** section in the **Self Service** or **Management System** section, click **Configuration**.
5. In the **Management system SSO configuration** or **Self Service SSO configuration** window, scroll down to the **Service Provider** section.
6. Configure the following **General Settings**:

    a. **Service Provider Name**: Enter the name of the service provider that sends the SAML authentication request. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
    b. **Assertion Consumer Service URL**: This field is pre-populated with the service provider's endpoint URL that receives the SAML from the identity provider. The assertion consumer service URL is appended with the organization code. For example:

        - Self Service URL: `https://domain/SelfService/Account/NewSSO/`*`organization-code`*
        - BlackBerry AtHoc management system: `https://domain/Client/`*`organization-code`*
    c. **Logout Service URL**: This field is pre-populated with the URL of the service provider's endpoint that receives SAML log out messages. For more information, see SSO logout service.
    d. **Custom Logout URL**: Optionally, enter a custom URL to redirect users to at logout.
    e. **Custom Logout Service Binding**: Optionally, select **POST** or **Redirect** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner IDP. The default setting is **POST**.
7. Configure the following **Security Settings**:

    a. **SAML Request Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML authentication requests received from the partner service provider must be signed. Receiving signed authentication requests is optional, but highly recommended.
    b. If **SAML Request Signature** is set to **Signed**, select a **Signature Algorithm**. The default setting is **RSA-SHA256**.
    c. In the **Certificate*** section, do one of the following:

        - Select **Use BlackBerry Certificate** to use the signed BlackBerry certificate.

Note: A system administrator must upload a valid BlackBerry signed certificate for this option to appear.

- Select **Use Custom Certificate** and click **Import Certificate**. On the **Import Certificate** window, enter a password and click **Browse**. Navigate to and select a valid certificate file. Click **Import**. Only .pfx and .p12 file types are supported.

8. Click **Apply**.
9. On the **User Authentication** page, click **Save**.

SSO logout service

If the logout URL is configured in the identity provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider forwards the logout request to an identity provider.
3. The identity provider validates the logout request.
4. The identity provider sends a logout request for the user to all other service providers that the identity provider is aware of that the user has an active security session with.
5. The identity provider terminates the user's sessions and sends a response to the original service provider.
6. The original service provider informs the user that they have been logged out.

If the logout URL is displayed in the Service Provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider terminates any of the user's active sessions that are handled by a third-party service.
3. The service provider forwards the logout request to the logout URL.

If the logout URL is not configured for either for identity provider or the service provider, when a user requests a logout, the service provider terminates the user's active session and displays the login page (for the BlackBerry AtHoc management system) or the sign out page (for Self Service.)

The following table describes the log out flows for the BlackBerry AtHoc management system:

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom logout URL.
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the organization's SSO login URL.
Session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Sign out or session timeout	IDP	No	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the custom logout URL.
Session timeout	IDP	No	No	The end user is signed off locally and redirected to the manual login page with a Session Timeout message.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.
Sign out	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.
Sign out	IDP	No	No	The end user is signed off locally and redirected to the manual login page.

The following table describes the log out flows for Self Service:

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the sign out page.

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	IDP	No	No	The end user is signed off locally and redirected to the sign out page.

Export SP and IDP settings

When you configure single sign-on, you can export settings data from the IDP and SP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Export**. The IDP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
2. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Service Provider** section, in the **General Settings** section, click **Export**.

   Note: Password and private key information is excluded from service provider metadata exports.

   The SP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
3. Click **Save**.

Import IDP settings

When configuring SSO, you can export and then import settings data from the IDP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Import**.
2. On the **Import Identity Provider Configuration** window, click **Browse** to select the .xml file that contains your IDP configuration.
3. Click **Open**.
4. Click **Import**. The fields in the Identity Provider section are populated with the data from the imported .xml file. If any fields were filled in before the import, they are over-written. If the .xml file contains any invalid fields, an error is displayed and no settings are imported.
5. Click **Apply**.

Import an existing IDP configuration

If you have an existing database-driven implementation of SSO and want to migrate to the improved user-interface based SSO solution, you can migrate the settings configuration from your IDP and import it into the BlackBerry AtHoc management system.

Contact your account representative or BlackBerry AtHoc customer support to obtain a copy of the `Utilities.zip` file needed to perform an SSO migration.

Note: Only IDP configurations can be imported. The SP configuration must be entered manually in the BlackBerry AtHoc management system. See Configure service provider settings.

1. Open a Windows command prompt and navigate to the following folder:

   ```
   <installed-directory>\AtHocENS\ServerObjects\Tools\SSO\EasyConnect
   ```
2. Run the following command to create and export a SAML metadata XML file:

   ```
   ExportMetadata.exe –partner <name> [-config <directoryName] [-baseurl <url>] [-
   file <filename>]
   ```

   where:

   - partner <*name* >: The name of the partner IDP configured in the `idp-partner.config` file or the partner SP configured in the `sp-partner.config` file.
     - If you specify a partner IDP, the corresponding local SP metadata is generated for the partner IDP.
     - If you specify a partner SP, the corresponding local IDP metadata is generated for the partner SP.
   - [-baseurl <*url*>]: Specify the directory that contains the EasyConnect configuration files. If you do not specify this directory, the export defaults to C:\EasyConnect\EasyConnectServer.
   - [-file <*filename* >]: Optionally, specify the name of the generated SAML metadata file. By default, the export uses the file name metadata.xml.

     Examples:

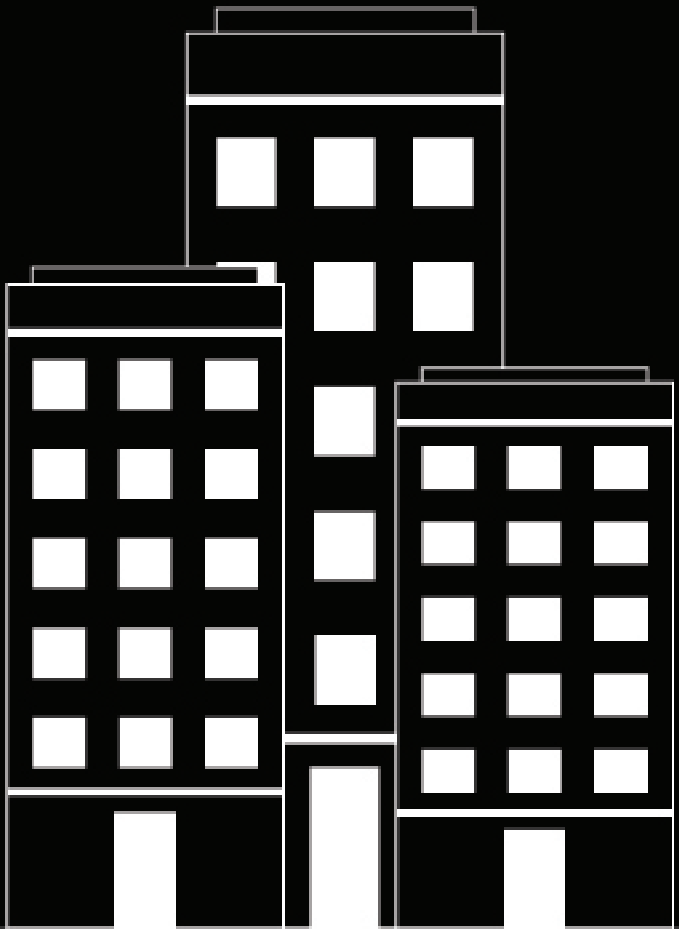
     - ExportMetadata.exe –partner ExampleIdentityProvider
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory"**
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com"*
     - ExportMetadata.exe –partner ExampleIdentityProvider config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com" -file "<File path>"**
3. Log in to the BlackBerry AtHoc management system and use the SSO IDP import feature to import the IDP metadata. See Export SP and IDP settings and Import IDP settings.

Enable SSO certificate revocation list checking

When single sign-on is enabled for your organization, a CRL is maintained. A CRL is a list of digital certificates that have been revoked and should not be trusted. If CRL checking is enabled, BlackBerry AtHoc checks the CRL before initiating a SAML authentication request to an identity provider or after receiving an SAML response from the IDP.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **SSO CRL (Certificate Revocation List) Settings** section, select the **Enable CRL Checking** option.

   Note: If the **SSO CRL (Certificate Revocation List) Settings** section is not visible, single sign-on is not enabled. See Enable single sign-on for Self Service and Enable single sign-on for the BlackBerry AtHoc management system.
4. In the **CRL Timeout Interval** field, enter the number of seconds to allow for certificate validation information to be retrieved from the CA. The minimum is 1 and the maximum is 60 seconds. The default is 20 seconds.
5. Optionally, select the **Ignore Verification Errors** option. If this option is selected, a certificate that fails verification will continue to be used and an error is logged. If this option is not selected, any certificate that fails verification is not used.
6. Click **Save**.



BlackBerry AtHoc

Distribution Lists

7.16

Contents

Manage distribution lists

This guide describes how to manage distribution lists within the BlackBerry® AtHoc® system.

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

- View all **Quick Action Guides**
- Create a static distribution list
- Create a dynamic distribution list

Create a static distribution list

You must have End Users Manager permissions to create a static distribution list.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click **New** > **Static**.
3. On the **New Distribution List** screen, enter values in the following fields in the **Basic Info** section:
    - **Name**: Enter a unique and easily identifiable name for the distribution list. The distribution list name has a 128 character limit.
    - **Common Name**: This field automatically populates based on the text entered into the Name field, but you can override it with a different name. The distribution list common name has a 128 character limit.
    - **Type**: This field cannot be edited.
    - **Description**: Optionally, enter details about the distribution list that will enable other operators to decide if the distribution list should be included in their alert.
    - **Folder**: Optionally, click **Select** and then drill down into the folder hierarchy to select the location to store the distribution list in. If you do not click the link, the distribution list will appear at the top level of the folder hierarchy.
4. Add users to your distribution list in the **Distribution List Members** section.
    - To add individual users, in the **Members** section, click **Modify**. Enabled users who can be added are displayed on the **Users** screen. Select the check boxes beside the names of the users to add, and then click **Add Selected**.

      Tip: You can add users to the distribution list based on the User Last Updated Source attribute. For more information, see Create a static distribution list based on the User Last Updated Source attribute.
    - To import users, in the **Members** section, click **Import File**. On the **Import Users** window, click **Browse** to select a .csv file and then click **Import**.
    - To add an existing distribution list, in the **Nested Static Lists** section, click **Modify**. On the **Nested Static Lists** screen, select the lists you want to add and then click **Add Selected**.
5. Click **Save**.

Create a static distribution list based on the User Last Updated Source attribute

Operators can create a static distribution based on the source that last updated the users' profiles. The following table lists the possible sources and the search terms required create a static distribution list using the User Last Updated Source attribute.

Source	Search term
Mobile app	• Check-in • Check-out • Report • Emergency • User Tracking - Mobile App • Mobile
Self Service	SelfService

Source	Search term
BlackBerry AtHoc Management System	ManagementSystem
User Sync Client	UserSyncClient
API	API
CSV Import	UserImport
Targeted Device	• Alert Tracking - Desktop Popup • Alert Tracking - Email • Alert Tracking - Mobile App • Alert Tracking - Phone • Alert Tracking - Text Messaging

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click **New** > **Static**.
3. On the **New Distribution List** screen, enter values in the fields in the **Basic Info** section. For details, see Create a static distribution list.
4. In the **Distribution List Members** section, beside **Members**, click **Modify**.
5. On the **Users** screen, beside the search field, click **Advanced**.
6. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
7. From the **Select Attribute** list, select **User Last Updated Source**.
8. Select an operation from the **Select Operation** list.
9. In the blank field that appears, enter the source to use to add members to the static distribution list. 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.
10. Click **Apply**.
11. On the **Users** screen, select the users to add.
12. Click **Add Selected**.
13. Click **Save**.

Create a dynamic distribution list

You must be an End Users Manager to create a dynamic distribution list.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click **New** > **Dynamic**.
3. On the **New Distribution List** screen, enter values in the following fields in the **Basic Info** section:
    - **Name**: Enter a unique and easily identifiable name for the distribution list. The distribution list name has a 128 character limit.
    - **Common Name**: (Optional) This field automatically populates based on the text entered into the Name field, but you can override it with a different name. The distribution list common name has a 128 character limit.
    - **Type**: This field cannot be edited.
    - **Description**: Optionally, enter details about the distribution list that will allow other users to decide if the distribution list should be included in their alert.
    - **Folder**: Optionally, click **Select** and drill down into the folder hierarchy to find the location to store the distribution list. If you do not click the link, the distribution list appears by default at the top level of the folder hierarchy.
4. In the **Distribution List Members** section, click **View**.
5. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all conditions to be added to the distribution list. When OR is selected, users that match any of the conditions are included. The default is AND.
6. In the **Select Attribute** drop-down list, select the first attribute you want to use as targeting criteria for the distribution list.
7. In the **Select Operation** drop-down list, select the operation to assign to the attribute.

    Note: The list of operations varies depending on the type of attribute selected.
8. In the third field, enter or select a value for the attribute.

    Tip: For Multi-select Picklist, Single-select Picklist, and Status type attributes, enter characters in the search box to filter the list of attribute values. You can enter characters that appear anywhere in the attribute value.
9. Optionally, click **Add Condition** and then repeat steps 6 through 8 to add additional attribute conditions as targeting criteria.

    Tip: You can add users to the distribution list based on the User Last Updated Source attribute. For more information, see Create a dynamic distribution list based on the User Last Updated Source attribute.
10. Optionally, if your organization is set up to display organizations, in the **Organization Hierarchy** section of the **Attribute** list, select one or more organizations or organizational nodes to use as targeting criteria for the distribution list.

    Note: Users must belong to the selected organizational nodes and meet the other specified attribute conditions to be included in the distribution list.
11. Click **Add**.
12. Click **Save**.

Create a dynamic distribution list based on user role

You must be an End Users Manager to create a dynamic distribution list.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click the **New** > **Dynamic**.
3. On the **New Distribution List** screen, enter values in the following fields in the **Basic Info** section of the screen:

- **Name**: Enter a unique and easily identifiable name for the distribution list.
- **Common Name**: (Optional) This field auto-populates based on the text entered into the Name field, but you can override it with a different name if you want.
- **Type**: This field cannot be edited.
- **Description**: Optionally, enter details about the distribution list that will allow other users to decide if the distribution list should be included in their alert.
- **Folder**: Optionally, click **Select** and drill down into the folder hierarchy to find the location to store the distribution list in. If you do not click the link, the distribution list will appear by default at the top level of the folder hierarchy.

4. In the **Distribution List Members** section, click **View**.
5. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all conditions to be added to the distribution list. When OR is selected, users that match any of the conditions are included. The default is AND.
6. Click the **Select Attribute** list, and then scroll down and click the **Roles** attribute in the **Operator Attribute** section.
7. In the **Select Operation** field that appears, select the **equals** operator.
8. A third field appears on the screen listing the roles available in the system. Click the role or roles you want to include in the distribution list.

   Tip: You can enter characters in the search box to filter the list of roles. You can enter characters that appear anywhere in the name of the role.

   Note: Operator roles that are associated with disabled features do not appear in the list. For more information, see "BlackBerry AtHoc roles" in the *BlackBerry AtHoc Operator Roles and Permissions* guide.
9. Click **Apply**. The Distribution List Members section displays the user roles that are included in the distribution list.
10. Optionally, click **View** to view the list of members. Click **Back** to return to the Distribution List details screen.
11. Optionally, click 🗋 to copy the selected conditions to use when creating another distribution list.
12. Click **Save**.

Create a dynamic distribution list based on organization subscriptions

You must be an End Users Manager to create a dynamic distribution list.

You can create a dynamic distribution list based on organization subscriptions to view users who are subscribed to each suborganization in an enterprise organization and to target them in alerts and accountability events.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click **New** > **Dynamic**.
3. Enter values in the following fields in the **Basic Info** section of the screen:

   - **Name**: Enter a unique and easily identifiable name for the distribution list.
   - **Common Name**: (Optional) This field automatically populates based on the text entered into the Name field, but you can override it with a different name.
   - **Type**: This field cannot be edited.
   - **Description**: Optionally, enter details about the distribution list that will allow other users to decide if the distribution list should be included in their alert.
   - **Folder**: Optionally, click **Select** and drill down into the folder hierarchy to find the location where you want to store the distribution list. If you do not click the link, the distribution list will appear by default at the top level of the folder hierarchy.

4. In the **Distribution List Members** section, click **View**.
5. On the **Create Conditions** window, click the **Select Attribute** list, and then scroll down and click **Subscribed Organizations** in the **Attribute** section.
6. In the **Select Operation** field that appears, select the **equals** operator.
7. In the field that appears, select your organization.

   Tip: You can enter characters in the search box to filter the list of organizations. You can enter characters that appear anywhere in the name of the organization.
8. Click **Apply**.
9. Optionally, in the **Distribution List Members** section, click **View** to view the users and their subscribed organizations.
10. Click **Save**.

Create a dynamic distribution list based on the User Last Updated Source attribute

Operators can create a dynamic distribution list based on the source that last updated users' profiles. The following table lists the possible sources and the search terms required to create a dynamic distribution list based on the User Last Updated Source attribute.

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

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, click **New** > **Dynamic**.
3. On the **New Distribution List** screen, enter values in the fields in the **Basic Info** section. For details, see Create a dynamic distribution list.

4. In the **Distribution List Members** section, beside **Membership Criteria***, click **View**.
5. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
6. From the **Select Attribute** list, select **User Last Updated Source**.
7. Select an operation from the **Select Operation** list.
8. In the blank field that appears, enter the source to use to add members to the static distribution list. 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.
9. Click **Apply**.
10. Optionally, click **View** to view the list of members. Click **Back** to return to the Distribution List details screen.
11. Click **Save**.

View all distribution lists

If you are an End Users Manager, you can access the Distribution Lists screen by navigating to **Users** > **Distribution Lists**.

The Distribution Lists screen opens, displaying all distribution lists you have permission to view in the BlackBerry AtHoc system. The following details are provided for each distribution list:

- The name of the list in the system
- The type of list: Static or Dynamic
- The system folder where the list is located

Search for distribution lists

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. Enter all or part of a distribution list name in the **Search list by name** field.
3. Optionally, to limit the search to a particular type of distribution list, select and deselect the relevant check boxes in the **Show lists of type** field.
4. Click 🔍 to view the results.

View distribution list details

You must be an End Users Manager to view information about distribution lists.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. Select a distribution list.

   The distribution list details screen opens, displaying all of the information in the BlackBerry AtHoc system for the corresponding list.

   Note: The content of the details screen varies depending on whether the list is static or dynamic.

Edit distribution list details

If you want to edit a static or dynamic distribution list that is from a remote organization, the only two fields that you can update are Name and Folder.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. Click ✎ beside the distribution list you want to edit.

   Note: The content of the distribution list edit screen varies depending on whether the list is static or dynamic.
3. Make changes to any of the editable fields on the screen.
4. Click **Save**.

Delete a distribution list

If you have administrator privileges, you can delete distribution lists in the system as long as all of the following are true:

- The list is not currently part of an alert template
- The list is not part of a draft alert
- The list is not nested within another distribution list

1. In the navigation bar, click **Users** > **Distribution Lists**. The Distribution Lists screen opens.
2. If the distribution list you want to delete already appears in the results table, select the check box beside its name. Otherwise, use the **Search list by name** field to locate the list, then click its name in the results field.
3. Click **Delete**.
4. If the lists you selected can be deleted, click **Delete** on the screen that appears. If a list cannot be deleted, the pop-up screen displays details about where the list is currently in use in the BlackBerry AtHoc system. To delete the list, you must first delete it from the alert or remove it from the distribution list it is nested in.

Export a distribution list

You must be an End Users Manager to export all members of a distribution list. To export only selected members of a distribution list, see Export the members of a dynamic distribution list and Export the members of a static distribution list.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click 👥.
3. Select a distribution list and then click **Apply**.
4. In the user list, select the check box next to each member name that you want to export.
5. Click **More Actions** > **Export** > **Users**.
6. On the **Export Users** screen, choose a set of columns to export.
7. Click **Export PDF** or **Export CSV**.
8. When the export is complete, save or open the .pdf or .csv file.

Export the members of a dynamic distribution list

You must be an End Users Manager to export the members of a distribution list.

1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, select a dynamic distribution list.
3. In the **Distribution List Members** section, beside **Users** , click **View**.
4. Optionally, on the **Member Users** screen, click **All Users** and select to filter the list by **Enabled Users with Operator Permissions** or **All Users with Operator Permissions**.
5. Optionally, click **Add** to add additional columns to the export. Only displayed columns are included in the export file.
6. Click **Export CSV**.

Export the members of a static distribution list

You must be an End Users Manager to export the members of a distribution list.

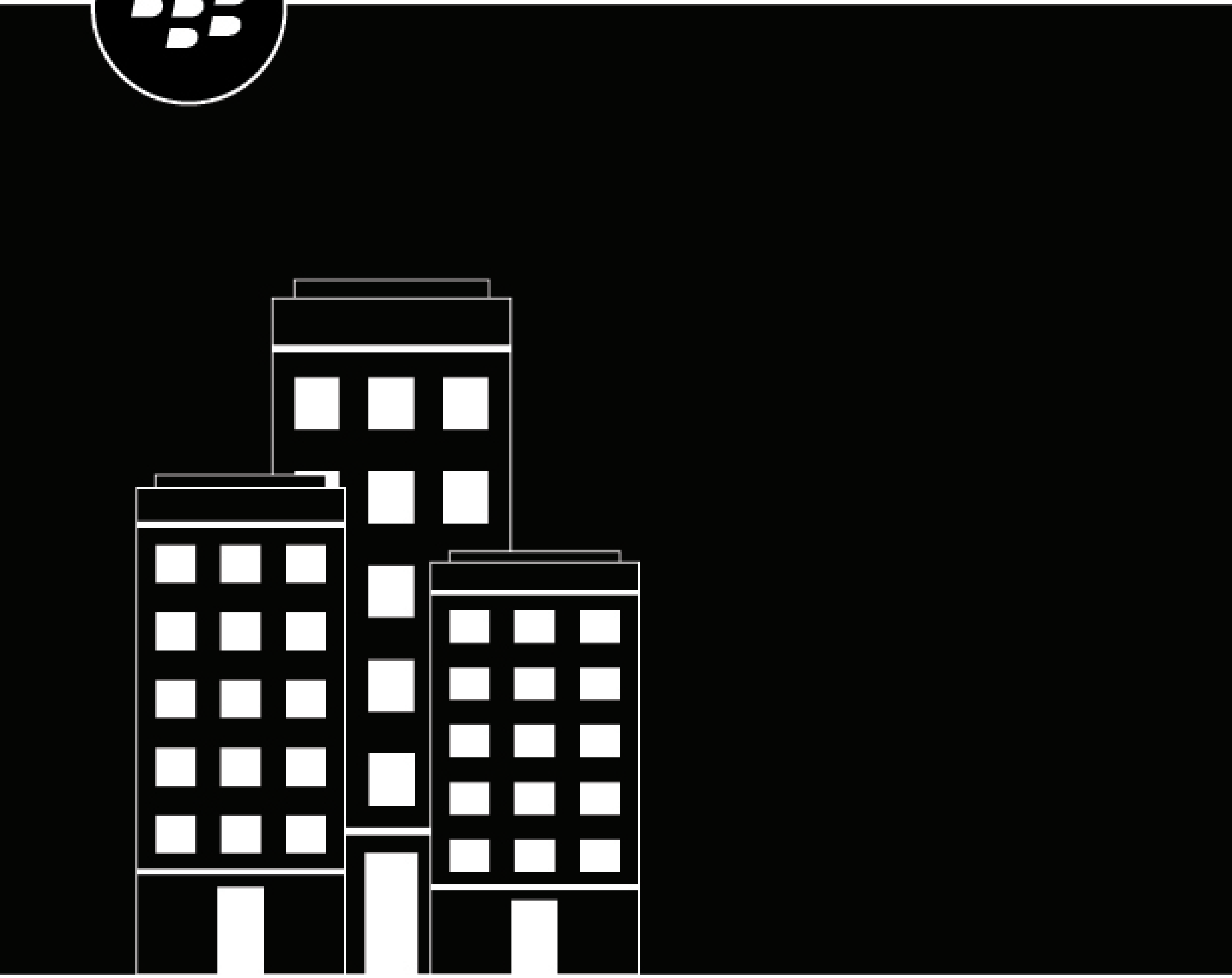
1. In the navigation bar, click **Users** > **Distribution Lists**.
2. On the **Distribution Lists** screen, select a static distribution list.
3. In the **Distribution List Members** section, beside **Members**, click **View**.
4. Optionally, click **More Actions** > **Modify** to remove specific distribution list members from the export.
5. Optionally, click **Add** to add additional columns to the export. Only displayed columns are included in the export file.
6. Click **More Actions** > **Export CSV**.

Configure distribution list folders

Distribution list folders define the structure of static and dynamic lists that can be selected as alert or event targets. You can create distribution lists using the Distribution Lists screen or by integrating with an external user directory.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **Distribution List Folders**.
3. On the **Distribution List Folders** screen, click **Add Node** to add a new node. If no nodes are selected, the new node is added to the bottom of the distribution list hierarchy. Select an existing node and click **Add Node** to add a new node under it.
4. Type the node name in the new field and hit **Enter**. The node name has a 128 character limit.
5. Optionally, to move a node, drag the node to the new location.
6. Optionally, to edit a node name, double-click on the node name and type your changes.
7. Optionally, to delete a node, select the name, and click **Delete Node**.
8. Optionally, to revert your changes, click **Remove Changes**.
9. Click **Save**.

All new and modified nodes are displayed in italics until saved.



BlackBerry AtHoc

Alert Templates

7.16

Contents

Manage alert templates

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

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

Note: When operators access the Alert Templates screen, they can see only alert templates associated with folders they have access to. For release BlackBerry AtHoc release 7.10 and later releases, if operators are members of multiple organizations, they only see the alert templates associated with the organization they are currently logged in to.

Access the Alert Templates screen

Note: Only Advanced Alert Managers and administrators can access the Alert Templates screen.

1. In the navigation bar, click **Alerts** > **Alert Templates**.

The following columns are displayed in the list:

- **Checkbox**: Displays a check box beside the alert templates that can be duplicated or deleted. System templates, such as the [New Alert Template] and the Incoming Connect Alert, cannot be duplicated or deleted, so no check boxes appear beside their names.
- **Alert Template Name**: Displays the alert template names, sorted alphabetically.
- **Folder**: Displays the name of the alert folder that contains the alert template.
- **Updated On**: Displays the date and time the alert template was last updated on.
- **Next Occurrence**: Displays the next scheduled date/time for an alert related to a recurring alert template.

You can click the column headers to sort the list.

On the **Alert Templates** screen, click **New** to create a new template. If a template has a check box beside its name, you can select it and use the **More Actions** list to duplicate, delete, or export it as needed.

Create an alert template

Note: Advanced Alert Managers and administrators can create new alert templates.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** screen, click **New**.
3. On the **New Template** screen, select or enter values in the following sections. For more information on completing each section, click the links to the *BlackBerry AtHoc Create and Publish Alerts* guide:
   - **Alert Template**: Define alert template details
   - **Content**: Define content for an alert or alert template
   - **Target Users**: Target users
     - **Select Personal Devices**: Select personal devices for an alert or alert template
   - **Target Organizations**: Target AtHoc Connect organizations (If this has been enabled for your organization.)
   - **Mass Devices**: Select and configure mass devices for an alert or alert template (Only available in English-language alert templates.)
4. Configure the schedule for the alert template. See Configure the schedule for an alert or alert template.
5. Click **Preview and Save** or **Save**.
6. On the alert template preview screen, do any of the following:
   - In the **Original Content** section, review the title, body, response options, more info links, location, attachments, and targeted users, groups, and organizations in the original alert template content.
   - In the **Device Summary** section, review the selected devices. This section displays the percentage of targeted users that are reachable by each selected device. This section also displays any selected device delivery preferences and mass devices.
7. If Email is a targeted device, review and edit how the email alert will appear to end users in the **Email Preview** section. You can do any of the following:
   - Select the **Include Map** option to include the location selected in the template as a map in the alert. Users who receive the alert can click the image of the map in the alert to go to an interactive map. This option is only available when a location is selected in the Content section.
   - Select a custom delivery template from the **Custom Template** pull-down menu. BlackBerry AtHoc provides default templates for each alert severity: High, Moderate, Low, Informational, and Unknown. By default, the custom delivery template associated with the selected alert severity is used.

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

   Your formatting updates are displayed in the **Email Preview** section.
8. Click **Save**.

Note: If the **Add bilingual** option is selected in the template settings, the **Preview and Save** button is not available. Click **Save**.

Configure the schedule for an alert or alert template

The Schedule settings specify how long alerts remain active.

1. Scroll down to the **Schedule** section in the alert or alert template.
2. In the **Alert Duration** field, enter the amount of time the alert should be active. Use the drop-down list to specify whether the time is in minutes, hours, or days.
3. Select the **Start Time**. Choose **Set during alert publishing** or **Activate Recurrence**. Select **Activate Recurrence** if you want to create an alert that will be used more than once. If you select this option, additional fields appear. For details, see Activate recurrence.
4. Click **Preview and Save**.
5. On the preview screen, review the template content.
6. Click **Save**.

Activate recurrence

Activate recurrence if you want to create an alert that will be used more than once.

1. Scroll down to the **Schedule** section in the alert or alert template.
2. In the **Start Time** section, select **Activate Recurrence**.
3. Select the hour, minute, and AM/PM from the pull-down menus to set the start time for the alert.
4. In the **Recurrence Pattern** section, from the **Interval** drop-down list, select how often the alert recurs: Daily, Weekly, Monthly, or Yearly.
5. In the **Recurrence Pattern** section, select recurrence options: Everyday, Every weekday (Monday-Friday) or Every x days.
6. In the **Recurrence Period** section, in the **Start Date** field, do one of the following:
    - Manually enter the day, month, and year that you want the alert to begin, writing the date in **MM/DD/YYYY** format (for example, January 25, 2021 would be written as 01/25/2021.)
    - Click 📅 and navigate to and then click the day, month, and year that you want to use.
7. In the **Recurrence Period** section, in the **End Date** field, select one of the three options:
    - **No end date**: The alert continues to recur until you or someone else manually deletes it, adds an end date to it, or limits the number of occurrences.
    - **End after <X> occurrences**: The alert continues to be sent out at the time interval you selected until it has been sent out the number of times you specify in this field.
    - **End by <date>**: The alert continues to be sent out until the date you select in this field.
8. Click **Preview and Save**.
9. On the preview screen, review the template content.
10. Click **Save**.

Manage visibility settings for alert template fields

Note: Only operators with Advanced Alert Manager, Alert Publisher, or Administrator roles can manage alert template settings.

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

The contents and behavior of the different sections of the alert template creation and alert template editing screens are controlled from a central Alert Template Settings screen. The visibility settings you select affect all alerts that are published from the template.

For example, if you choose to hide the Mass Devices section from an alert template called "Alert Mobile Users," that section will be hidden for all alerts that are published from the alert template.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** screen, select a template or click **New**.
3. On the **New Template** or template details screen, click **Settings**.
4. On the **Alert Template Settings** screen, customize the visibility settings for the fields in each of the following alert template sections:

   - Content
   - Target Users
   - Target Organizations
   - Mass Devices
   - Schedule
5. Click **Apply**.

Manage visibility options for Content fields in an alert template

1. On the **Alert Template Settings** screen, click the **Content** tab.
2. In the **Enable** section, select the options beside each of the content options that you want to make visible to users who are creating alerts based on this alert template. You can show or hide any of the following options for content:

   - **Response Options**: Select this option if you want users creating alerts from this alert template to be able to include response options in the alert.
   - **Add Bilingual**: Select this option if you want to enable operators to send an alert in two languages.
   - **Location**: Select this option if you want users creating alerts from this alert template to be able to designate a specific location for the alert on a map. This option must be selected to enable geofence targeting.
   - **Is Location Mandatory**: Select this option if you want to make it mandatory for users creating alerts from this template to select a location for the alert.
   - **Attachments**: Select this option if you want users to be able to include attachments in an alert. Users can then include documents, videos, and image files in alerts.
   - **Dropbox**: Select this option if you want users to be able to add attachments to their alerts. These attachments would be available to alert recipients through a link in the alert that opens a file stored in Dropbox.
3. In the **Visibility in Alert** section, do one of the following:

   - Select **Show Content Section**, then select the check boxes beside each option that you want to make available to users who are creating alerts from the alert template.

    - Select **Show as initially collapsed** if you want the Content section to display in its collapsed state when the alert template is first opened by the alert creator.
    - Select **Show as read-only and prevent publisher from editing** if you want the alert creator to be able to see the Content section without being able to edit it.
  - Select **Hide Content Section** if you do not want users who are creating alerts from the alert template to be able to see the Content section.

  Note: If a section is not ready, you cannot make that section read-only or hide it.
4. Click **Apply**.

Manage visibility options for Target Users fields in an alert template

1. On the **Alert Template Settings** screen, click **Target Users**.
2. Optionally, in the **Enable** section, select the **Fill Count** option to enable specifying a certain number of responses before ending an alert. For more information, see "Define fill counts and escalation" in the *BlackBerry AtHoc Create and Publish Alerts* guide.
3. Optionally, in the **Enable** section, select the **Dependents** option to enable inclusion of dependents in alerts. For more information, see "Create dependents for a user" in the *BlackBerry AtHoc Manage Users* guide.

   Note: You cannot enable Fill Count and Dependents at the same time.
4. In the **Enable Targeting** section, select the check boxes beside each of the user targeting options you want to make visible to users who are creating alerts based on this alert 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
   - Personal Devices. For this option, there is a list of the personal devices you can make visible or hide from users who are creating alerts based on the alert template.
5. In the **Visibility in Alert** section, do one of the following:
   - Select **Show Target Users Section**, then select the check boxes beside each option you want to make available to users who are creating alerts from the alert template.
     - Select **Show as initially collapsed** if you want the Targeted Users section to display in its collapsed state when the alert template is first opened by the alert creator.
     - Select **Show as read-only and prevent publisher from editing** if you want the alert creator to be able to see the Targeted Users section without being able to edit it.
   - Select **Hide Target Users Section** if you do not want users who are creating alerts from the alert template to be able to see the Target Users section.

   Note: If a section is not ready, you cannot make that section read-only or hide it.
6. Click **Apply**.

Manage visibility options for Target Organizations fields in an alert template

1. On the **Alert Template Settings** screen, click **Target Organizations**.
2. In the **Enable** section, select the check boxes beside each of the organization targeting options you want to make visible to users who are creating alerts based on this alert template. You can show or hide the By Name and By Location options for targeting organizations.
3. In the **Visibility in Alert** section, do one of the following:

   - Select **Show Target Organizations Section**, then select the check boxes beside each option you want to make available to users who are creating alerts from the alert template.

     - Select **Show as initially collapsed** if you want the Target Organizations section to display in its collapsed state when the alert template is first opened by the alert creator.

     - Select **Show as read-only and prevent publisher from editing** if you want the alert creator to be able to see the Target Organizations section without being able to edit it.

   - Select **Hide Target Organizations Section** if you do not want users who are creating alerts from the alert template to be able to see the Target Organizations section.

     Note: If a section is not ready, you cannot make that section read-only or hide it.
4. Click **Apply**.

Manage visibility options for Mass Devices fields in an alert template

Note: This feature is not available for non-English alert templates.

1. On the **Alert Template Settings** screen, click **Mass Devices**.
2. In the **Enable** section, select the check boxes beside each mass device you want to make visible to users who are creating alerts based on this alert template. If you do not want a currently selected mass device to be available, deselect the device's check box.
3. In the **Visibility in Alert** section, do one of the following:

   - Select **Show Mass Devices Section**, then select the check boxes beside each option you want to make available to users who are creating alerts from the alert template.

     - Select **Show as initially collapsed** if you want the Mass Devices section to display in its collapsed state when the alert template is first opened by the alert creator.

     - Select **Show as read-only and prevent publisher from editing** if you want the alert creator to be able to see the Mass Devices section without being able to edit it.

   - Select **Hide Mass Devices Section** if you do not want users who are creating alerts from the alert template to be able to see the Mass Devices section.

     Note: If a section is not ready, you cannot make that section read-only or hide it.
4. Click **Apply**.

Manage visibility options for Schedule Fields in an alert template

1. On the **Alert Template Settings** screen, click **Schedule**.
2. In the **Visibility in Alert** section, do one of the following:

- Select **Show Schedule Section**, then select the check boxes beside each option you want to make available to users who are creating alerts from the alert template.
  - Select **Show as initially collapsed** if you want the Schedule section to display in its collapsed state when the alert template is first opened by the alert creator.
  - Select **Show as read-only and prevent publisher from editing** if you want the alert creator to be able to see the Schedule section without being able to edit it.
- Select **Hide Schedule Section** if you do not want users who are creating alerts from the alert template to be able to see the Schedule section.

  Note: If a section is not ready, you cannot make that section read-only or hide it.

3. Click **Apply**.

View alert template details

View the details of an alert template to determine the name and description of the template.

1. In the navigation bar, click **Alerts** > **Alert Templates**. The Alert Templates page displays alert template names, folders, the last updated on date and time, and the next occurrence (for recurring alert templates.)
2. Optionally, hover your cursor over the name of an alert template. A pop-up window appears, displaying the following template details: Name, Description, Alert Title, Alert Body, and Last Published date and time.
3. To open the details page, click the name of the alert template.

   A template details screen appears, displaying information about the template grouped into the following sections:

   - **Alert Template**: Displays the name and description of the alert template, the folder where the alert template is stored, and the Available for Quick Publish and Available for mobile publishing options.
   - **Content**: Displays the severity, type, title, and body for any alert that will be created from the template. Optionally can contain links to additional information or attachments related to the template, a geographic location for the template, and response options for any alert generated from the template.
   - **Target Users**: Displays a summary of the users who will be targeted by any alert created from the template. If dependents are enabled for your organization and in the alert template, the Target Users section displays separate tabs for Sponsors and Dependents. The selected personal devices are displayed. If device delivery preference is enabled for your organization, it is displayed with either the Organization defined, System defined, or User preferred option. When the Organization defined option is displayed, phone group prioritization is not available.
   - **Target Organizations**: Displays each organization that will be targeted by any alert created from the template. Available only if enabled for your organization.
   - **Mass Devices**: Displays the mass devices that will be used to broadcast any alert created from the template. Only available in English-language alert templates.
   - **Schedule**: Displays the start and end dates and duration for any alert created from the template. If relevant, also displays the recurrence settings for the template.
   - **Info**: Displays the name of the person who created the template, the name of the last person to update the template, and the dates the template was created and updated. Depending on your system configuration, it might also contain the Common Name and template ID number.

Search for an alert template

The Alert Templates search engine matches any set of letters or numbers anywhere in a template name and is not case-sensitive.

Note: Wildcards are not supported in searches.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** screen, type or paste all or part of a template name in the search field.
3. Optionally, click **Advanced** and select a folder from the list, or select options to limit the search results to recurring alerts, alerts that are available for quick publishing, or alerts that are available for mobile publishing.
4. Click **Search**.

Filter the alert template list

The alert template list can be filtered by any of the following:

- Folder name
- Recurring alert template status (whether or not recurrence has been activated for an alert template)
- Quick publish status (whether or not quick publishing has been enabled for an alert template)
- Mobile publishing status (whether or not mobile publishing has been enabled for an alert template)

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** screen, click **Advanced**.
3. Optionally, in the **Folder** drop-down list, select the name of a folder to limit the search to only templates within that folder.
4. Optionally, select **Recurring Alerts** to limit the search to only alert templates that have been configured to occur repeatedly.
5. Optionally, select **Available for Quick Publish** to limit the search to only alert templates that have been configured to be available for quick publishing.
6. Optionally, select **Available for Mobile Publishing** to limit the search to only alert templates that have been configured to be available for mobile publishing.
7. Click **Search**. The alert templates list refreshes to display all templates that match the filter criteria.

Remove filters from the alert templates list

After you have filtered the templates list, you can remove any or all of the filters by doing the following:

- To remove all filters and return to the default alert templates list, click **Clear All** under the **Search** button.
- To remove a specific filter, click X on the pill icon for the filter.

Sort the alert templates list

1. In the navigation bar, click **Alerts** > **Alert Templates**. The Alert Templates page displays the following sortable columns: Alert Template Name, Folder, Updated On and Next Occurrence.
2. Click the column header to sort a column. The alert templates display in descending order of the values in the selected column.
3. Optionally, click the same column header again to sort in the opposite direction.

Change the number of templates listed on the alert templates screen

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Scroll to the bottom of the **Alert Templates** screen.
3. Click the drop-down list that appears beside the phrase **items per page**.
4. Select the number of templates you want to display per page.

The screen refreshes and displays the total number of results you specified.

Add custom placeholders for alert template content

Note: This topic explains how to insert alert placeholders, not how to create or import them. For details on those tasks, see Create custom placeholders for alert templates and Import alert placeholder values.

You can add alert placeholders to the following Content sections of an alert template:

- Alert Title field
- Alert Body field
- Response Options text field
- Custom text within Targeted Devices (Available only to Enterprise Administrator and Organization Administrator users.) This option can be specified for an enabled device that has a Custom Text option.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Click an existing alert template to open an editable details screen or **New** to create a new template.
3. In the **Content** section, click + in the **Title**, **Body**, and **Response Options: Response Text** fields.
4. Select the appropriate alert placeholder option for the alert template from the list.

   Double brackets [[ ]] around the alert placeholder name in the selected field indicate that you have added the alert placeholder correctly.
5. Click **Preview and Save**.
6. On the preview screen, review the template content
7. Click **Save**.

An operator must then select the correct alert placeholder values when preparing to publish the alert. If a default placeholder value was selected, it will appear in the alert template. If no default value was selected, the operator must select a value before they can publish the alert.

Edit an alert template

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

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

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Use the search field or scroll down in the alert template list to locate the alert template you want to edit.
3. Click the name of the alert template.
4. Edit values in any of the following sections:
   - Alert Template
   - Content
   - Target Users
   - Target Organizations (if your system is set up for them)
   - Mass Devices (Only available in English-language alert templates)
   - Schedule
5. Click **Preview and Save**.
6. On the preview screen, review the alert template content.
7. Click **Save**.

Duplicate an alert template

Duplicating an alert template creates a copy of it in the system and can be used to speed up creating similar templates. You can duplicate any alert template that contains a check box beside its name.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** page, use the search field or scroll down in the alert template list to locate the alert template you want to duplicate.
3. Select the check box beside the alert template name.

   Note: If the template does not have a check box beside its name, it cannot be duplicated.
4. Click **More Actions** > **Duplicate**.

   A New Alert Template screen appears, displaying all of the values that were part of the original alert template.
5. Make any needed changes to the alert template details.

   Note: At a minimum, you should change the name of the alert template so that you can distinguish it from the original.
6. Click **Preview and Save**.
7. On the preview screen, review the template content.
8. Click **Save**.

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

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

Delete an alert template

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

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

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Use the search field or scroll down in the alert template list to locate the alert templates you want to delete.
3. Select the check box beside each alert template that you want to delete.
4. Click **Delete** at the top of the screen. A confirmation pop-up screen opens, listing the alert templates you are about to delete.
5. Click **Delete**. The Alert Templates screen refreshes to show the alert template list without the alert template or alert templates you deleted.

Import or export an alert template

Operators can import and export alert templates. You can import or export multiple alert templates at the same time. An alert template can be exported from one organization and imported to another organization. Import and export files are JSON text files.

Content in the Alert Template and Content sections of an alert template are included in imports and exports, including location data, custom placeholders, response options, attachments, and translation languages. Alert template settings related to the Content and Alert Template sections are included in imports and exports. The Target Users, Target Organizations, Mass Devices, and Schedule sections are not included.

Imported templates are added to the System Default folder. When an alert template is imported, it is in a Not Ready state until edited by an operator.

All alert template imports and exports are captured in the operator audit trail.

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. On the **Alert Templates** screen, select one or more alert templates.
3. Click **More Actions** and do one of the following:
    - Click **Import**. On the **Import Alert Template** screen, click **Browse** and then browse to and select a JSON file on your computer. You can select a previously exported alert template or click **Download a template file** to download a JSON file and update it with details. Click **Import**.
    - Click **Export** and then on the **Export Alert Templates** dialog, click **Export**. A JSON file downloads to your computer.

Alert template settings

The following topics provide information about managing alert template settings, including placeholders, folders, delivery templates, and audio files.

Placeholders for alert templates

Placeholders provide a way to customize text such as date or time, a building number, or group name in an alert template. When the operator publishes the alert template, the placeholder value is inserted automatically. There are two types of placeholders in alert templates: System and Alert.

View the list of placeholders for your organization

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

The Alert Placeholders screen appears, displaying a list of the alert placeholders you have access to in the system.

Use system placeholders for alert template content

The alert template can contain predefined system placeholders in the title or body of the alert. The placeholders are replaced automatically with the appropriate values when the alert is published.

Note: System placeholders can also be added during alert publishing. Alert placeholders can only be added to alert templates.

The following Content fields support placeholders:

- Alert title
- Alert body
- Response options
- Custom text within Targeted Devices

The following list describes the system placeholders:

- System-related: [[SystemName]], [[OrganizationName]], [[OrganizationID]],
- Date or Time-related: [[Timezone]]
- Publisher-related: [[OperatorFullName]], [[PublishDate]], [[PublishTime]]

1. In the navigation bar, click **Alerts** > **Alert Templates**.
2. Click an existing alert template to open an editable details screen or **New** to create a new alert template.
3. In the **Content** section, click ➕ in the **Title**, **Body**, or **Response Options: Enter Response Text** fields.
4. Select the appropriate alert placeholder option for the alert template.

   Double brackets [[ ]] around the alert placeholder name in the selected field indicate that you have added the alert placeholder correctly.

An operator can then select the correct alert placeholder values when preparing to publish an alert.

Create custom placeholders for alert templates

Note: Alert placeholders can be created at the enterprise or organization level. Inheritance rules can have an impact on who can use them, so verify that you are creating them at the correct organization level. For more information, see “Manage common content with inheritance” in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

You can create alert placeholders for alert templates so that operators can customize the content during publishing. For example, if your organization needs to create alert templates that reference building numbers, you can create an alert placeholder called `building_number`. When operators publish the alert template, they can select the correct building number for that instance of the alert template.

1. In the navigation bar, click **Alerts**.
2. Click **Alert Placeholders**. Alternately, you can access alert placeholders from the **Settings** screen.
3. On the **Alert Placeholders** screen, click **New**.
4. In the drop-down list, select one of the following alert placeholder types:

    - **Multi-select Picklist**: Alert creators can select one or more of the values in the list and have them appear in the alert when it is published.
    - **Single-select Picklist**: Alert creators can select one of the values in the list and have it appear in the alert when it is published.
    - **Text**: Alert publishers are prompted to enter text that conforms to a minimum and maximum length. You can designate how many lines of text to display in the text box as well as set default text.
    - **Date**: Alert creators can accept the pre-set date or manually enter a new date before the alert is published.
    - **Date Time**: Alert creators can accept the pre-set date and time or manually enter a new date and time before the alert is published.
    - **Time**: Alert creators can accept the pre-set time or manually enter a new time before the alert is published

    The Organization field on the screen that appears tells you at which level you are creating the placeholder: Enterprise or organization.
5. In the **Basic** section, enter a name for the alert placeholder. The name must be between 1 and 200 characters and must be unique in the system.
6. Specify values and defaults for the alert placeholder, depending on the type.

    - **Multi-select Picklist**

        - Enter at least two unique values that have between 1 and 50 characters. Angle brackets (<>) are not allowed.
        - You can import the values from an existing text or .csv file. For more information, see Import alert placeholder values.
        - Click the check box of at least one value to set it as the default.
    - **Single-select Picklist**

        - Enter at least one unique value between 1 and 50 characters. Angle brackets (< >) are not allowed.
        - You can import one or more values from a text or .csv file. For more information, see Import alert placeholder values.
        - The name is case insensitive.
        - Select the check box of at least one value to set it as the default.
    - **Text**: Enter numerical values for the minimum length, the maximum length, and the number of lines to show. Angle brackets (< >) are not allowed.

        - Set the Minimum length to a value between 1 and 400 characters.
        - Set the Maximum length to a value between 1 and 400 characters.
        - Set the value for Lines to show to a value between 1 and 5. This value controls the height of the text box on the alert publishing screen.
        - Enter a text string for the Default value, with the number of characters between the Minimum length and the Maximum length.
    - **Date**: Select the default date for the placeholder.
    - **Date Time**: Select the default date and time for the placeholder.

- **Time**: Select the default time for the placeholder.

7. Click **Save**.

The alert placeholder is created and appears in the Placeholder list for all alert creators who have access to the Enterprise or organization the placeholder was created in.

Remove alert placeholders

Important: You cannot remove alert placeholders that are currently in use in an alert template. If you try to delete the alert placeholder, a pop-up screen appears, listing each of the alert templates the alert placeholder is used in.

To remove alert placeholders from the Alert Placeholders screen, complete the following steps:

1. In the navigation bar, click **Alerts** > **Alert Placeholders**. The Alert Placeholders screen appears, displaying a list of all of the alert placeholders you have access to in the system.
2. Click the alert placeholder that you want to remove.
3. On the placeholder details screen, click **Delete**.
4. If the placeholder is used in any alert templates, a list of dependencies will appear. In order to delete the placeholder, you must first remove the dependencies by completing the following steps:

   a. Open each alert template the alert placeholder is being used in.
   b. Manually remove the alert placeholder.
   c. Save your changes.
   d. Return to the placeholder details view and click **Delete**.
5. Click **Delete**.

The alert placeholder is removed from the alert placeholders list.

Import alert placeholder values

You can import values for alert placeholders for single-select and multi-select picklists. Importing the values helps you avoid entering multiple values, especially if you are creating a long list.

Import the values from a .csv file that has one column or one value per line.

Note: Angle brackets (<>) cannot be used in alert placeholders. Placeholder values containing these characters are rejected.

1. In the navigation bar, click **Alerts** > **Alert Placeholders**.
2. On the **Alert Placeholders** screen, click **New**.
3. In the drop-down list that appears, select either the **Multi-select Picklist** or **Single-select Picklist** option.
4. On the **New Placeholder** screen, in the **Values** section, click **Import Values**.
5. On the **Import Values to New Placeholder** screen, click **Browse** and select a .csv file.

   Note: The file must be closed before you try to upload it. If it is open, you will get an error message when you click Open in the next step.
6. Click **Open**.
7. Optionally, select **Replace all current values with the imported values** if you want the new values to overwrite the existing values. If you want to keep existing values and add the new values, leave this check box unselected.
8. Click **Import**.
9. Click **Save**.

Activate an alert template when an alert is received

You can use alert placeholders in alert templates that are triggered by an incoming alert. When set up, the incoming alert type automatically publishes an alert to targets specified in the alert template at publishing time. Response options, locations, and attachments can be included in the triggered alert.

For example, you can set up an alert template that responds to a mobile user when the user sends an emergency alert. To set up the trigger, create an alert template with the alert placeholders. Or, if you receive an incoming alert from a Connect organization, you can forward it to other organizations you are connected to. To learn how to create rules for handling incoming alerts, see "Manage alert rules" in the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

Note: If an incoming alert targets a map location, the location is automatically added to the triggered alert. The alert then targets organizations or users that have locations within the specified map area.

Note: When an incoming Connect or mobile app alert from a connected organization triggers another alert, any attachments in the incoming alert are not included in the triggered alert.

Use the following alert placeholders in an alert template:

- $SenderName$
- $SenderContacts$
- $InboundEventTitle$
- $InboundEventBody$

To add the alert placeholders, complete the following steps:

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Alert Templates**.
3. On the **Alert Templates** screen, click **New** to create a new alert template that will respond to an incoming alert, such as "I have an emergency."
4. In the **Content** section, enter an alert name and a description that will be sent when the incoming alert is received.

   For example,

   Name:

   `Please help!`

   Description:

   ```
   $SenderName$ needs help and sends the following message:
       $InboundEventTitle$
       $InboundEventBody$
       $SenderName$'s info:
       $SenderContacts$
   ```
5. Complete the alert template by selecting your targeted users and devices.

   Note: You should not add a target location. Incoming alerts that have target locations will override locations in the template.
6. Click **Preview and Save**.
7. On the preview screen, review the template content.
8. Click **Save**.
9. Create or edit an incoming alert by following the instructions in the "Configure mobile alert settings" section of the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide. In the **Run Alert Template** list, select the alert template you just created, then click **Save**.

You now have the option to forward or trigger other alerts based on an incoming alert.

Manage alert folders

An alert folder, also known as an alert category, typically corresponds to the type of alerts or source of alerts that are published. For example, folder types can include Weather Alerts, IT Alerts, Commander/CEO Alerts, and Daily News Alerts. Every alert must be associated with an alert folder. Grouping alerts by folder has many benefits, including the ability to use templates to establish a common appearance for all alerts within a folder, facilitate end user subscriptions by folder, and restrict operator publishing privileges to specific folders.

Access the alert folders manager

The Alert Folders Manager centralizes alert folder configuration and management tasks. Only Administrators can access the Alert Folders Manager.

1. In the navigation bar, click **Alerts** > **Alert Folders**. By default, folders display in alphabetical order by name. You can sort by any column.

To sort by a specific column, click the column heading.

To filter folders by name, type letters that the folders contain in the search field, then click **Search**. Wildcards are not supported.

Configure alert folders

You can configure the default settings for alert templates that are associated with an alert folder.

System setup folders can be modified only when accessed from the System Setup (3) organization. Enterprise folders can be modified only when accessed from the organizations in which they were created.

Note: You cannot select the Weather alert folder, if present. If an alert template is associated with the Weather alert folder, it is moved to the system default folder after a system upgrade to release 7.0.0.2 or later release.

1. In the navigation bar, click **Alerts** > **Alert Folders**.
2. Click a folder name.
3. Optionally, on the **Edit Alert Folder** window, edit the folder name or description.
4. Click **Save**.

Create alert folders

Note: Alert folders can be managed at the system, enterprise, or organization level. Inheritance rules can have an impact on who can use them, so verify that you are creating them at the correct organization level. For more information, see "Manage common content with inheritance" in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

Note: When you create a new alert folder, it is immediately available for publishing to all end users.

1. In the navigation bar, click **Alerts** > **Alert Folders**.
2. On the **Alert Folders** screen, click **New**.
3. On the **New Alert Folder** window, type a name in the **Name** field.
4. Optionally, provide additional information in the **Description** field to further identify the purpose of the new folder.
5. Click **Save**.

Delete alert folders

Alert templates and alerts are associated with folders. When you delete a folder, a pop-up screen appears listing the alert templates associated with that folder. The pop-up gives you the option of exporting the list of affected alert templates to an Excel spreadsheet so that you can modify the alert template details manually and associate each alert template to a new alert folder. You can also click **Confirm** to automatically assign the alert templates to the system default folder. If no alerts or alert templates are associated with an alert folder, no pop-up window is displayed and the alert folder is deleted.

Note: You cannot delete Enterprise folders from within a suborganization.

Note: You cannot delete the System Default folder. You can delete the System folder from the System organization.

1. In the navigation bar, click **Alerts** > **Alert Folders**.
2. On the **Alert Folders** screen, click ✖ in the row of the alert folder you want to delete.
3. On the **Delete** window, click **Confirm**.

Manage delivery templates for devices

All delivery devices use templates to communicate alert messages. For example, the template for a desktop pop-up window defines the background color, text color, window size, and any default content that is included in every alert, such as a "Click here for more information" link.

BlackBerry AtHoc ships with system default templates for different devices, including email and desktop pop-ups, but you can select a different template when publishing an alert or creating or editing an alert template.

Use the Delivery Templates manager to modify existing templates and to create custom templates.

When configuring your organizations in the BlackBerry AtHoc management system, BlackBerry AtHoc customer support will work with you to set up the available delivery devices for alerts including email, cell phones, and desktop pop-up windows.

Note: The devices for which delivery templates are available in your system depend on the delivery devices and protocols in your BlackBerry AtHoc configuration. For example, not all types of email delivery and phone delivery have templates.

Access delivery templates

Note: Only administrators can access the Delivery Templates manager. Administrators can only modify delivery templates that have been created within their current organization. All other templates are inherited and are read-only.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Delivery Templates**.

   The Delivery Template screen appears and displays the available templates for the selected device group, such as Desktop Popup, Email, or All.

   Only devices that are enabled for the current organization appear in the list. For more information, see "Configure devices" in the *BlackBerry AtHoc System Settings and Configuration* guide.

   The following columns are displayed in the Delivery Templates table:

   - Template Name
   - Severity
   - Device Group: The device type associated with the template: Desktop Popup, Email, or XML feed.
   - Organization: The organization the alert was created in. The column displays the phrase *System Setup* if the alert was defined at the system level, an enterprise name if the alert was defined within an enterprise organization, and an individual organization's name if the alert was defined within a non-enterprise organization.
   - Locale: The language and region associated with the delivery template.

Device delivery templates are customizable for the devices and protocols being used. You should edit only the desktop pop-up templates. If you need to update templates for other delivery devices, consult BlackBerry AtHoc customer support.

Create delivery templates

Note: Delivery templates can be managed at the system, enterprise, or organization level. Inheritance rules can change who can use these entities. Verify that you are creating them at the correct organization level in the enterprise. For more information, see “Manage common content with inheritance” in the *BlackBerry AtHoc Plan and Manage Enterprise Organizations*guide.

The easiest way to create a delivery template is to duplicate an existing one and then edit it. For information on how to duplicate a template, see Duplicate delivery templates.

1. In the navigation bar, click ⚙ icon.
2. In the **Basic** section, click **Delivery Templates**.
3. On the **Delivery Templates** screen, click **New** and select one of the following options:

    - **Desktop Popup** for alerts that appear on user computer screens.
    - **Email** for alerts that are sent to user email inboxes. If you do not know XML, work with BlackBerry AtHoc customer support to configure the template.
    - **XML Feed** for alerts that are sent to mass devices such as Giant Voice. If you do not know XML, work with BlackBerry AtHoc customer support to configure the template. XML Feed delivery templates are not visible if the XML Feed device is disabled.
4. Enter a **Template Name**, **Description**, and **Common Name**. These should be specific so that users can tell at a glance what the template should be used for.
5. (*Desktop Popup and Email Only.*) Select a **Locale** from the list. The language you select will be used by the system if your alert content is in the same language and if the App Template option for the alert is set to use the default template.
6. Select the **Severity** level that corresponds to the delivery template you are creating. Alert creators can later overwrite the severity level by selecting the **Use Custom Template** option on the **Personal Device Options** screen when an alert is created or edited.
7. (*Desktop Popup and Email Only*) Select **Publishing default for severity/locale above** if you want the current delivery template to be used by default whenever an alert is created that matches the severity level and locale that you selected in steps 5 and 6.

    Note: Selecting this check box allows you to create a consistent experience for users across the system. When each alert level is assigned its own color scheme, font styles, and size, for example, it makes it possible to recognize the severity of any received alert at a glance.
8. If you are creating a Desktop Popup template, in the **Popup Settings** section, select whether to edit the options using the **Standard** controls (buttons and lists) or the **Advanced XSLT** controls. If you do not have much knowledge of XSLT, select **Standard**.

    For the XML Feed and Email templates, you do not have the option to work with Standard controls; you can only work with the Advanced XSLT controls.

    Note: Before working with Advanced XSLT, ensure that you have knowledge about style sheets or work with BlackBerry AtHoc customer support to configure the template.

    The following additional steps apply only to the **Style Settings** section for Desktop Popup templates.
9. Customize the **Font** settings:

    a. For each element, such as **Title** or **Body**, select **Hide** or **Show** in the **Display** drop-down to specify whether to display the element in the popup.
    b. For the text of an element, specify the **Font**, **Font Type**, and font **Size** by selecting options from the drop-down lists and making selections.

c. For the text of an element, specify the color by pointing to it in the color selection panel or entering a hexadecimal color value. Click **Apply**.

10. Choose the **Display** settings:

    a. Specify the **Border Color** of the pop-up by clicking the drop-down list and selecting a color. Click **Apply** to save the color choice.

    b. Select the **Border Size** by clicking the drop-down list and selecting the number of pixels for the width.

    c. Select the **Background Color** of the pop-up by clicking the drop-down list and selecting a color. Click **Apply**.

    d. In the **Display Size** field, select either the **Full Screen** or **Custom** option.

    Note: If you create a custom display size, make sure the width is set wide enough to accommodate the Severity, Type, and Location information that appears automatically at the top of the desktop pop-up when it is sent.

    e. Optionally, choose a **Logo Position** to help brand your organization. You can position the logo in either the top left or top right of the pop-up.

    f. Select the **Logo** file using either the organization default or click **Browse** to upload a custom file. The file can be in .png, .gif, or .jpg format.

11. Specify the **Popup Behavior**:

    a. Select a **Location** on the screen where the pop-up will appear, such as the top right corner.

    b. Select a **Timeout** period after which the pop-up will disappear from the desktop. You can specify the value in Seconds, Minutes, Hours, or Days.

    c. Select the **Entrance Motion**, which is how the pop-up will enter the screen. The pop-up will either slide in from the right or left side of the screen.

    d. Select the **Exit Motion**, which is how the pop-up will leave the screen. The pop-up will either slide out the left or right side of the screen.

12. Click the **Preview** button to view the pop-up. Verify that the layout, colors, fonts, and font sizes are appropriate for the type of alert you are creating.
13. Click **Save**.

Duplicate a delivery template

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Delivery Templates**.
3. On the **Delivery Template** screen, click the check box beside the template you want to duplicate.
4. Click **Duplicate**.
5. On the **Duplicate Confirmation**window, click **Duplicate**. The duplicate template is created with the same name as the original, but with a series of numbers at the end.

Edit template settings

On the Delivery Templates screen, you should edit only the Basic, Styles, and Popup Behavior tabs. Other tabs are for advanced use only.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **Delivery Templates**.
3. On the **Delivery Template** screen, click the name of the template you want to edit.

   Note: As you edit the template, click **Preview** to preview changes to the pop-up. Templates that use the full-screen desktop pop-up option do not display the full screen in the preview window.
4. Optionally, edit the **Template Name**, **Description**, and **Common Name** fields for the template.

   The following additional Popup Settings apply only to Desktop Popup templates.
5. Optionally, change the **Font** settings:

   a. For each element, such as Title or Body, select **Hide** or **Show** to specify whether to display the element in the pop-up.
   b. For the text of an element, specify the **Font**, **Font Type**, and **Size** by selecting the drop-down lists and making selections.
   c. For the text of an element, specify the color by pointing to it in the color selection panel or entering its hex color in the text box above the panel. Click **Apply**.
6. Optionally, change the **Display** settings:

   - Border Color
   - Border Size
   - Background Color
   - Display Size (Full Screen or Custom)

     Note: If you create a Custom display size, make sure the width is set wide enough to accommodate the Severity, Type, and Location information that appears automatically at the top of the desktop popup when it is sent.
   - Logo Position
   - Logo
7. Optionally, change the **Popup Behavior** fields:

   - Location (Where the popup appears on the screen)
   - Timeout (How long the popup remains on the screen)
   - Entrance Motion
   - Exit Motion
8. Click **Preview** to view the edited pop-up.
9. Click **Save**.

Delete a delivery template

1. In the **Delivery Templates** list, select the template to delete.
2. On the **Delete Confirmation** screen, click **Delete**.

Manage audio files

The audio message delivered with an alert can critically affect the way users comprehend the alert message and their subsequent actions. You can configure an audio file to deliver a custom sound with an alert. Use the Audio Files screen to review the catalog of existing audio files and to add and delete audio files.

Access the Audio Files screen

Note: Only administrators can access the Audio Files screen.

1. In the navigation bar, click **Alerts** > **Audio Files**.

   The Audio Files screen opens with the following columns displayed:

   - **Audio File Name**: The name associated with the audio file. This can be different from the actual filename. Hover your cursor over a name to view the audio file name and the description of the file.
   - **Severity**: The severity associated with the audio file. This can be High, Moderate, Low, Informational, or Unknown.
   - **Organization**: Displays the organization where the audio file is stored. Audio files created in System Setup are from the system organization and are available for all organizations in the system. Audio files created in an enterprise organization are available for all its suborganizations.

- **Size**: The size of the audio file. The maximum allowed size is 2 MB.
- **Locale**: Language of the audio file. This can be Any or English (US)

2. Click a file name to view or edit the details for the audio file.

Sort the audio files list

To sort the audio files by a specific column, click the column heading. The files display in descending order of the values in the selected column. Click the column heading again to sort in ascending order.

Filter the audio files list

1. In the **Name** field, type letters that the audio file name contains. Wildcards are not allowed.
2. Click **Search**. Only the audio filenames containing the specified criteria display in the table.
3. To display all audio files again, click **Clear all**.

Add audio files

1. In the navigation bar, click **Alerts** > **Audio Files**.
2. On the **Audio Files** screen, click **New**.
3. On the **New Audio File** window, in the **Audio File Name** field, type a name to associate with the new audio file. The name can be different than the actual filename.
4. Optionally, in the **Description** field, type a brief description of the audio file, which will help identify the audio file when users search for it. The text should include a description of the file contents or its purpose.
5. To upload the audio file, click **Browse**. Browse to the location on your local computer, select the audio file, and click **Open**.
6. Optionally, from the **Severity** list, select a **Severity**.
7. Optionally, select **Use this audio as default for publishing**.
8. Optionally, from the **Locale** list, select a locale.
9. Click **Save**.

Edit audio file details

Only audio files that are stored in the organization you are logged in to are available for editing. The details of audio files can be edited, but the audio track itself cannot be changed after it is uploaded.

1. In the navigation bar, click **Alerts** > **Audio Files**.
2. On the **Audio Files** screen, click to select an audio file.
3. On the **Edit Audio File** window, change the details in any of the following fields:

   - Audio File Name
   - Description
   - Common name
   - Severity
   - Default

   Note: The ID, Size, and Locale fields cannot be edited.
4. Click **Save**.

Download audio files

1. In the navigation bar, click **Alerts** > **Audio Files**.
2. Select the check box beside the audio file you want to download.

   Note: Only one audio file can be downloaded at a time.

3. Click **More Actions** > **Download**.

The selected audio file downloads to your computer.

Play audio files

1. In the navigation bar, click **Alerts** > **Audio Files**.
2. On the **Audio Files** screen, select the check box beside the audio file you want to play.
3. Click **More Actions** > **Play**.

The selected audio file plays over your computer speakers.

Delete audio files

Deleting an audio file from the Audio Files screen does not delete the actual .wav file on your computer. It only removes the audio file from the BlackBerry AtHoc server. Only files that are stored on the organization you are logged in to can be deleted. System default files, audio files that are configured as the default for a severity level, and files that are in use in an alert cannot be deleted.

1. In the navigation bar, click **Alerts** > **Audio Files**.
2. On the **Audio Files** screen, select the check box beside each audio file you want to delete.
3. Click **Delete**.
4. On the **Delete Confirmation** window, click **Delete**.

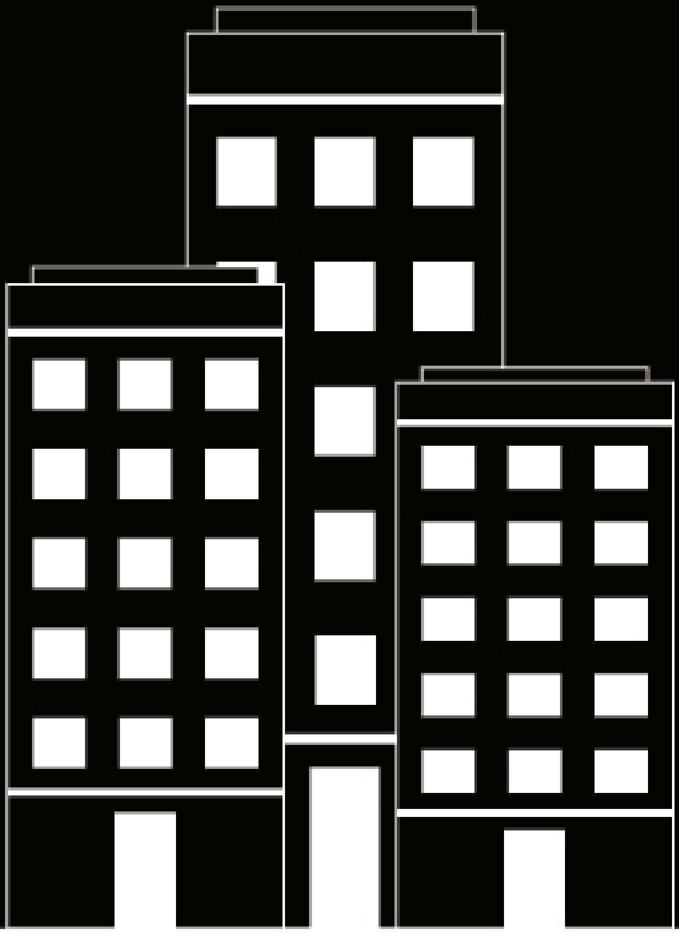
Note: Files that cannot be deleted do not appear in the list even if selected.

Reset a system alert template to the default configuration

System Administrators, Enterprise Administrators, and Organization Administrators can reset a system alert template to the default configuration. Alert templates can be reset on enterprise organizations and suborganizations. When a system alert template is reset on an enterprise organization, the alert template content, targeting, and schedule sections are reset to the out of the box default configuration. When a system alert template is reset on a suborganization, its content is synchronized to the enterprise organization.

Note: Only the ~*** New Alert Template - Configuration Use *** ~ and ~ *** New Template - Configuration Use *** ~ system templates can be reset.

1. Log in to the BlackBerry AtHoc management system as a System Administrator, Enterprise Administrator, or Organization Administrator.
2. Click **Alerts** > **Alert Templates**.
3. On the **Alert Templates** page, click the **~*** New Alert Template - Configuration Use *** ~** or **~ *** New Template - Configuration Use *** ~** system template.
4. On the template details page, click **Reset**.
5. On the **Reset Alert Template** dialog, click **Proceed**.



BlackBerry AtHoc

AtHoc Situation Response

7.16

Contents

What is AtHoc Situation Response?

AtHoc® Situation Response provides a centralized approach to critical event management to properly plan, manage, and remediate crises and improve business continuity. AtHoc Situation Response provides the following benefits:

- Efficient plan management: Create and review plans before a crisis occurs.
- Increased plan awareness: Engage with stakeholders through the plan review process.
- Reduced time to respond: When a crisis occurs, create an incident from a predefined and approved plan.
- Single view for situation awareness: View the alerts, accountability events, and collaborations associated with an incident.
- Ease of regulatory compliance: Review and archiving functions provide a trackable process.

Key use cases

- **Planning and predictive readiness**: Plan for incidents and risks.
- **Incident and disaster response**: Respond within and across organizations.
- **Situational awareness**: View context-rich information.
- **Mission orchestration**: Secure special events and execute mission-oriented tasks.
- **Secure information sharing**: Share real-time peer-to-peer and group collaborations, files, and audio.
- **Audit and continuous learning**: Audit and learn from past responses.

Roles

Operators with the following AtHoc Situation Response roles can perform the listed tasks in the BlackBerry AtHoc management system and mobile app.

Note: Enterprise administrators and organization administrators can also perform any of the following tasks.

Plan Manager

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans
- Create an incident
- Edit an incident
- Publish an incident
- View activity
- Export activity log
- Add new entry in activity log
- Activate plan steps
- Start a collaboration
- View and participate in collaborations

- End a collaboration
- Export ended collaborations

Plan Incident Manager

- View plans in read-only mode
- Create an incident
- Edit a draft incident
- End an incident
- Publish an incident
- View activity
- Export activity log
- Add new entry in activity log
- Export an incident
- Activate plan steps
- Start a Collaboration
- View and participate in collaborations
- End a collaboration
- Export ended collaborations

Collaboration Manager

- Start a collaboration
- View and participate in collaborations
- End a collaboration
- Export ended collaborations

Plan and Respond

Before a crisis, use AtHoc Situation Response to create plans, assign reviewers to plans, and send plans through the review process. During a crisis, create an incident based on your previously reviewed plan. You can also make adjustments to a plan during an incident to respond to events as they occur.

Plan states

This section describes the four states of a plan.

- **Draft**: The plan has been saved, but is not yet approved.
- **Active**: The plan has been approved and can be used to create an incident.
- **Disabled**: The plan cannot be used to create an incident. Any plan that is in the active state can be disabled. You can enable a disabled plan.
- **Archived**: Any plan that is in the active state can be archived. When a plan is archived, it becomes read-only and cannot be reenabled.

Enable AtHoc Situation Response in BlackBerry AtHoc

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Click ⚙.
3. In the **System Setup** section, click **Feature Enablement**.
4. On the **Feature Enablement** screen, click the **IsSituationResponseSupported** row.
5. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True**.
6. Click **Save**.
7. On the **Feature Enablement** screen, click the **IsCollaborationSupported** row.
8. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True**.
9. Optionally, to enable adding attachment steps in plans, in the **Feature Enablement** screen, click the **IsAttachmentsSupported** row.
10. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True**.
11. Click **Save**.

AtHoc Situation Response is enabled.

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

Create a plan

Tip: To create a new plan from an existing plan, see Manage plans in the Plan Manager.

Before you begin:

- Situation Response must be enabled. See Enable Situation Response in BlackBerry AtHoc.
- You must have enterprise administrator, organization administrator, or plan manager permissions to create a new plan.
- Create any alert and event templates that you want to use in the plan.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Do one of the following:
   - In the navigation bar, click **Plan** > **New Plan**.
   - In the navigation bar, click **Plan** > **Plan Manager** > **New**.
3. On the **New Plan** page, in the **Summary** section, select a **Category** from the list.
4. In the **Summary** section, enter a plan name.
5. Optionally, enter a description. The maximum number of characters is 200.
6. In the **Expected Duration** section, select the number of days, hours, and minutes.
7. Optionally, in the **Location** section, click **Add** to include a location for the plan.
   a) On the **Full Map** screen, select a predefined location or create a custom location.
   b) Click **Apply**.

   Note: The map appears as a read-only map on the plan summary. This map cannot be used for targeting alerts or events.
8. Optionally, in the **Reviewers** section, click **Add Reviewers** to add additional reviewers.
   a) On the **Add Reviewers** screen, select available reviewers.
   b) Click **Apply**.

   Any operator in the organization can be added as a plan reviewer. External operators cannot be added as plan reviewers.
9. Optionally, click **Set Approver** to change the default plan approver. The plan manager who creates the plan is the plan approver by default.
   a) On the **Choose Approver** window, select a plan approver. Only operators who have plan manager, enterprise administrator, or organization administrator permissions and who have not been added as a plan reviewer can be selected as the plan approver.
   b) Click **Apply**.
10. In the **Steps** section, select a plan type from the **Select Type** list. Select from the following step types:
    - **Create Alert**: Select an alert template from the pull-down list that appears. Only alert templates that are ready to publish appear in the list.
    - **Create Attachment**: Add up to 5 attachments totaling up to 1 MB. Click **View/Add Attachments**. In the **View/Add Attachments** window, drag files or click **Browse** and then browse to and select the files you want to add and then click **Apply**.
    - **Create Collaboration**: Click **Set Users & Groups**. In the **Set Users & Groups** window, select the **Users or Groups** tab, select the users or distribution lists you want to include in the collaboration, and then click **Apply**. Only users who have registered on the BlackBerry AtHoc mobile app can be added to the collaboration.
    - **Create Event**: Select an accountability event template from the pull-down list that appears. Only event templates that are ready to publish appear in the list.
    - **Free Text**: Enter a maximum of 4000 characters of text.
11. Optionally, for alert and event steps, click **Preview** to open a window that displays the details of the selected alert or event template.
12. Optionally, for collaboration steps, click **Preview** to open a dialog that displays the users and groups who have been invited to join the collaboration.
13. In the **Steps** section, enter a **Step Name**.

    For alert and event type steps, when you select the template, the Step Name field is automatically populated with the name of the template. You can edit this field.
14. Optionally, enter a step description. The maximum number of characters is 200.
15. Click **Save**.

The plan is created and can be viewed and edited in the plan manager. The plan has a draft status and cannot be used to create an incident until the plan has been reviewed and approved.

Review a plan

After a plan manager creates a plan, assigns reviewers and an approver, the plan is ready to begin the review process. When the plan owner assigns a reviewer to a plan, a **Plan(s) to Review** link appears on the BlackBerry AtHoc home page for that reviewer. The plan reviewers review each step in the plan and can create change requests for the plan or for specific steps in the plan. A ← appears beside the name of the reviewer on the plan summary screen in the **Reviewers** section to indicate that the reviewer has submitted a change request for the plan.

When a reviewer creates a change request, the plan owner can access the plan summary page and choose to acknowledge or reject the request. When the plan owner acknowledges or rejects all change requests, the plan reviewers can mark the plan as reviewed. When all reviewers have marked the plan as reviewed, the plan appears in the **Plans waiting for me** list of the plan approver.

Note: If the plan owner edits the plan when it is in draft state, the review process resets and the plan reviewers must mark the plan as reviewed again before the plan can be approved.

When the plan is approved, it moves to the active state and can be used to create incidents.

If you have been added as a reviewer for a plan, access the plans you need to review from the plan manager or from the **Plan(s) to Review** link on the BlackBerry AtHoc home page. When you review the plan, you can request a general change for the plan or for a specific step in the plan.

Tip: You can see if you have plans that require your review or approval on the BlackBerry AtHoc home page in the right pane below the system status. Click the **Plan(s) to Review** link to go directly to the plans waiting for your review or approval in the plan manager.

1. Log in to the BlackBerry AtHoc management system as a plan manager.
2. Click **Plan** > **Plan Manager**.
3. On the **Plans** page, click **All Plans** > **Show plans waiting on me**.
4. Click the plan you want to review.
5. Review each step in the plan.

   Tip: For alert and event steps, click ▸ to expand the details of the step and then click the name of the template to preview the template content. For collaborate steps, click the link to view the users and groups who were invited to the collaboration.
6. Optionally, Create a general change request.
7. Optionally, Request a change to a step.

Your change requests are added to the **Change Requests** section. When the plan owner reviews and accepts or rejects your change requests, you can Mark a plan as reviewed.

Create a general change request

1. On the **Plan** page, click **General Change Request**.
2. On the **Create Change Request** dialog, enter your change in the **Comment** field.
3. Click **Create**.

Your general change request is added to the **Change Requests** section. A ← appears beside your name in the **Reviewers** section to indicate that you have an open change request for the plan. When the plan owner acknowledges or rejects your change requests, the ← is removed.

Request a change to a step

1. On the **Plan** page, click ☰ beside the step you are requesting a change for.
2. On the **Create Change Request** dialog, enter your change in the **Comment** field.
3. Click **Create**.

Your step change request is added to the **Change Requests** section. A ← appears beside your name in the **Reviewers** section to indicate that you have an open change request for the plan. When the plan approver acknowledges or rejects your change request, the ← is removed.

Review plan change requests

If you are a plan owner, you can review and acknowledge or reject all change requests for a plan.

1. On the **Plan Manager** page, click the plan you want to review.
2. On the **plan summary page**, view the **Change Requests** section.

   If there are open change requests, a number appears beside the **Change Requests** section title. Click the number to display only the open change requests. Each change request includes the title of the step, the text of the change request, the reviewer who opened the change request, and a date and timestamp for when the change request was submitted.
3. Optionally, to filter the change requests list to display only general change requests, click G.
4. Optionally, to filter the change requests list to display only change requests for a specific step, click ☰ in that step.
5. Click **Edit**.
6. In the **Change Requests** section, review the content of the change request.
7. Click ✓ to acknowledge the change request, or ⊗ to reject it.

Acknowledged change requests display a ✓. Rejected change requests display a ⊗. When all change requests for a plan are accepted or rejected and the plan approver approves the plan, the plan moves to the active state and can be used to create incidents.

View the list of reviewers

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. On the **Plans** page, click the plan you want to review.
4. On the plan details page, view the reviewers in the **Reviewers** section.

A ← appears beside the name of any reviewer who has an open change request for the plan. A ✓ appears beside name of any reviewer who has marked the plan as reviewed.

Add or remove reviewers

A plan owner can add or remove reviewers from plans that are in a draft state.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. On the **Plans** page, click the plan that you want to modify.
4. On the plan details page, click **Edit**.
5. In the **Reviewers** section, do one of the following:

   - Click **Add Reviewers** to add additional reviewers.

    - Click ✖ beside the name of a reviewer to remove them.
6. Optionally, in the **Reviewers** section, click ✖ beside a reviewer to remove them from the plan.
7. Click **Save**.

Mark a plan as reviewed

When the plan owner accepts or rejects all change requests associated with a plan, the plan reviewers can then submit additional change requests or mark the plan as reviewed.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.

   You can also click the **Plan(s) to Review** link on the BlackBerry AtHoc home page to access plans that are waiting for your review.
3. On the **Plans** page, click the plan you want to mark as reviewed.
4. On the **Plan Summary page** , click **Mark as Reviewed**.

Edit a Plan

A plan owner can edit a plan that is in draft state. If the plan owner edits the plan after reviewers have marked the plan as reviewed, the review process resets and the plan reviewers must mark the plan as reviewed before the plan can be approved.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. Click the plan you want to edit.
4. On the **Plan Summary page**, click **Edit**.

   The following sections can be edited:

   - Category
   - Name
   - Description
   - Expected Duration
   - Location

   The following actions can be performed:

   - Add or remove reviewers
   - Add, edit, delete, or reorder steps
5. Click **Save**.

Add, edit, delete, or reorder steps

Plans that are in draft state can be edited and the plan owner can add, edit, delete, or reorder the steps in the plan.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. Click the plan that you want to edit.
4. On the plan details page, click **Edit**.
5. In the **Steps** section, do any of the following:

   - Click **Add Steps** to add a step.

- Click ✖ beside a step to remove it.
- Click and drag ≣ beside a step to move the step to a new position in the plan.
- Click to edit the title, description, or type for a step.

6. Click **Save**.

Approve a plan

When all reviewers for a plan mark the plan as reviewed, the plan is ready to be approved and moved to the active state.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.

   You can also click the **Plan(s) to Approve** link on the BlackBerry AtHoc home page to access plans that are waiting for your approval.
3. On the **Plans** page, click the plan that you want to approve.
4. On the plan details page, click **Approve**.

Your approval is saved. If all reviewers mark the plan as approved, the plan is moved to the active state and can be used to create incidents.

Manage plans in the Plan Manager

Use the Plan Manager screen to create new plans, and to delete, duplicate, archive, disable, or enable existing plans.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. Optionally, click **All Plans** and select **Show plans created by me** or **Show plans waiting on me** to filter the list of plans.
4. Optionally, click **New** to create a new plan. For details, see Create a plan.
5. Optionally, select one more plans and click **More Actions** to complete any of the following actions:

   - **Delete**: Draft and archived plans can be deleted. Active plans cannot be deleted.
   - **Duplicate**: Only one plan can be duplicated at a time. Draft, active, and archived plans can be duplicated. When a plan is duplicated, all details from the original plan are duplicated. The duplicate plan is created in the draft state.
   - **Archive**: Only active plans can be archived. When an plan is archived, it cannot be re-enabled and incidents cannot be created using it.
   - **Disable**: Only active plans can be disabled.
   - **Enable**: Only disabled plans can be enabled.

Search for a plan

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Plan Manager**.
3. Optionally, click **All Plans** and select **Show plans created by me** or **Show plans waiting on me**.
4. On the **Plans** page, enter a plan name in the **Search by Title** field and click 🔍.

Create an incident

Plans that are in an active state can be used to create an incident.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, click **New Incident**.
4. On the **New Incident** page, select an active plan from the **Plan** list. The Title field automatically populates with the name of the plan. This field is editable. You can enter a title that is between 3 and 100 characters.
5. Optionally, in the **Description** field, enter a description. The maximum length is 200 characters.
6. In the **Expected Duration** section, select the number of days, hours, and minutes.
7. Optionally, click ☰ and drag to change the order of steps.
8. Optionally, for alert and event steps, click **Preview** to open a window that displays the details of the selected alert or event template.
9. Optionally, for collaboration steps, click **Preview** to open a dialog that displays the users and groups who have been invited to join the collaboration.
10. Optionally, add steps to the plan.
11. Click **Review and Create**.
12. On the **Review and Create** page, review the content.
13. Optionally, on the **Review and Create** page, for alert and event steps, click ▸ to expand the details of the step and then click the name of the template to preview the template content. For collaborate steps, click the link to view the users and groups who were invited to the collaboration.
14. Click **Create**.

The incident is live and is added to the incident manager. An operator with plan manager permissions can now Activate plan steps, View plan progress, Track the status of plan steps, Enable, disable, or end steps, or Add steps to a plan.

Activate plan steps

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, optionally, select **Live Incidents** to filter the list of incidents.
4. Select the plan incident you want to activate the steps for.
5. On the incident details page, optionally, for alert and event steps, click ▸ to expand the details of the step and then click the name of the template to preview the template content. For collaborate steps, click the link to view the users and groups who were invited to the collaboration.
6. Do one of the following:
   - For Event or Collaboration steps, click **Run**.
   - For Alert steps:
     a. Click **Edit/Publish**.
     b. On the alert details page, modify any section as needed.
     c. Click **Review and Publish**.
     d. On the **Review and Publish** screen, click **Publish**.
     e. Click **Close** to return to the incident details page.

The **Completion** bar in the **Progress** section updates as each step is activated. The **Pace** section displays the difference between the expected duration of the plan measured against the actual duration. The **At A Glance** section display details about each step that has been activated and run. Click the link next to an alert or event step to view more details in the BlackBerry AtHoc management system. Click the link next to a collaborate step to open the collaboration in a new tab on your browser.

View plan progress

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, select **Live Incidents** to filter the list of incidents.
4. Select the incident you want to view the progress for.
5. On the incident details page, see the **Completion** bar in the **Progress** section.
6. Optionally, view the difference between the expected and actual duration of the plan in the **Pace** section.
7. Optionally, view the details about each step that has been activated and run in the **At A Glance** section. Click the link next to an alert or event step to view more details.

Track the status of plan steps

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, select **Live Incidents** to filter the list of incidents.
4. Select the incident that you want to track the status of steps for.
5. On the **All Incidents >** *incident-name* screen, see the **At a Glance** section. This section lists the type, title, time of creation, and current status for each step in the incident. You can click the link next to an alert or event step to view more details in the BlackBerry AtHoc management system. You can click the link next to a collaborate step to open the collaboration in a new tab on your browser.

Enable, disable, or end steps

When an incident is live, the plan manager can enable, end, and disable steps in the plan. All steps are enabled by default.

Note: No actions can be performed on Free Text steps.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, select **Live Incidents** to filter the list of incidents.
4. Select the incident that you want to enable or disable steps for.
5. On the incident details page, click 🟩, 🟥, or **End** for each step.

   Disabled steps cannot be activated. Disabled steps can be enabled. Enabled steps can be activated. Activated steps can be ended.

Add steps to a plan

When an incident is in a draft state, additional steps can be added to it before it is published. To add steps to a live incident, see Add steps.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Incident Manager**.

3. Select the incident that you want to add steps to.
4. In the **Steps** section, click **Add Step**.
5. Optionally, click ☰ and drag the step to a different position in the incident.
6. Do one of the following:
    - Click **Save Draft**.
    - Click **Review and Create**.

View incidents in the Incident Manager

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, click **All Incidents** and select any of the following options to filter the list of incidents:
    - **Draft Incidents**
    - **Live Incidents**
    - **Ended Incidents**
4. Click any incident to open the incident details page.

View a live incident

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Click **All Incidents** > **Live Incidents**.
4. Click any incident to open the incident details page.
5. Optionally, for any alert or event step, expand the step and click the template link to preview the template content. For collaborate steps, click the link to view the users and groups who were invited to the collaboration.

Add steps

You can add steps to an incident when it is live. To add steps to a draft incident, see Add steps to a plan.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, select **Live Incidents** to filter the list of incidents.
4. Select the incident that you want to add steps to.
5. On the incident details page, click **Add Step** and select one of the following step types:
    - **Alert**
    - **Attachment**
    - **Collaboration**
    - **Event**
    - **Free Text**
6. On the **Add Step** window, do one of the following:
    - For an **Alert** step, select an alert template from the list. Only alert templates that are ready to publish appear in the list. Click **Preview** to open a window that displays the details of the selected template.

- For an **Event** step, select an event template from the list. Only event templates that are ready to publish appear in the list. Click **Preview** to open a window that displays the details of the selected template.
- For an **Attachment** step, click **View/Add Attachments**. On the **View/Add Attachments** window, drag files or click **Browse** and then browse to and select the files you want to add. You can add up to 5 attachments totaling up to 1 MB. Click **Apply**.
- For a **Collaboration** step, click **Set Users & Groups**. On the **Set Users & Groups** window, select the **Users** or **Groups** tab. Select the users or distribution lists you want to include in the collaboration, and then click **Apply**. Only users who have registered on the BlackBerry AtHoc mobile app or operators who have registered on the Collaboration page in the BlackBerry AtHoc management system can be added to the collaboration.
- For a **Free Text** step, in the **Free text instructions** field, enter a maximum of 4000 characters of text.

7. On the **Add Step** window, enter a step name. For alert and event steps, the **Step Name** field is automatically populated with the name of the selected template. You can edit this field.
8. Optionally, enter a step description. The maximum number of characters is 200.
9. Click **Add**.

The step is added to the live incident and can be activated.

View the status of all steps

You can view the status of all steps for a live incident from the incident manager.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, from the **All Incidents** list, select **Live Incidents** to filter the list of incidents.
4. Select the incident that you want to view the status of the steps for.
5. Optionally, on the incident details page, view the status of each step below the **Summary** section.

   Steps in the incident that have been activated and completed display a **Completed** status. Enabled steps display a 🟩. Disabled steps display a 🟥.
6. Optionally, view the overall status of all steps in the incident in the **Progress** section. The **Completion** bar indicates the percentage of steps that have been completed in the incident. The **Progress** section also displays when the incident was started and if any steps are disabled.
7. Optionally, view the difference between the actual and expected duration of the incident in the **Pace** section.
8. Optionally, view details about the status of each step in the **At a Glance** section. The **At a Glance** section updates automatically every 30 seconds. This section lists the type, title, time of creation, and current status for each step in the incident. You can click the link next to an alert or event step to view more details in the BlackBerry AtHoc management system. You can click the link next to a collaborate step to open the collaboration in a new tab on your browser.

Enable or disable steps

When an incident is live, you can enable or disable specific steps within it. Steps in an incident are enabled by default.

Note: You cannot enable or disable Free Text steps.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions.
2. Click **Plan** > **Incident Manager**.
3. Optionally, from the **All Incidents** list, select **Live Incidents** to filter the list of incidents.
4. Select the incident that you want to enable or disable the steps for.

5. Optionally, click 🟢 or 🔴 in the step details section.

View the activity log for an incident

The activity log for an incident displays all actions associated with the incident, including when the incident was started and ended and when steps are enabled, disabled, added, run, or ended. You can add entries to the activity log, flag entries as important, and export the activity log. You cannot edit activity log entries.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager permissions
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, click the incident that you want to view the activity log for.
4. On the incident details page, click **Activity Log**. The activity log for the incident opens and displays information about when the incident was created and when each step was added, run, enabled, disabled, or ended, including the date and time.
5. Optionally, for an alert step, click the **Alert ID:***alert-id* link to open the alert details page.

Flag entries in the activity log as important

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, click the incident that you want to view the activity log for.
4. On the incident details page, click **Activity Log**.
5. On the **Activity Log** page, click ⚐.

The activity log entry appears with a 🚩 above the timestamp in the right column.

Manually add a log entry

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, click the incident that you want to view the activity log for.
4. On the incident details page, click **Activity Log**.
5. On the **Activity Log** page, click **New Entry**.
6. On the **New Activity Log Entry** window, in the **Title** field, enter a title. The maximum number of characters allowed is 100.
7. On the **New Activity Log Entry** window, in the **Body** field, enter a description. The maximum number of characters allowed is 200.
8. Click **Submit**.

The new entry is added to the activity log of the incident.

Export the activity log

You can export the activity log for an incident to a .csv or .pdf file.

1. Log in to the BlackBerry AtHoc management system as an operator with plan manager or plan incident manager permissions.
2. Click **Plan** > **Incident Manager**.
3. On the **Incidents** page, click the incident that you want to export the activity log for.

4. On the incident details page, click **Activity Log**.
5. On the **Activity Log** page, click **More Actions** > **Export to PDF** or **Export to CSV**.

A .csv or .pdf file downloads to your local computer.

View plan and incident entries in the operator audit trail

The following plan and incident actions are logged in the operator audit trail:

- A plan is added
- A plan is updated
- A plan is duplicated
- A plan is activated
- A plan is deleted
- A plan is enabled
- A plan is disabled
- A plan is archived
- A change request is submitted for a plan or plan step
- A change request is approved
- A change request is rejected
- A plan is marked as reviewed
- A plan is approved
- The activity log for an incident is exported to a .csv or .pdf file

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Operator Audit Trail**.
4. Optionally, do any of the following to filter the audit trail results on the **Operator Audit Trail**page:
    - Select a date range from the **To** and **From** fields.
    - Enter an operator name or ID in the **Operator** field.
    - Select **Collaboration**, **Incident**, or **Plan** from the **Entity** list.
    - Select the **Search by Specific Action(s)** option and then select actions from the **Action(s)** list.

For more information, see View the operator audit trail report in the *BlackBerry AtHoc System Settings and Configuration*.

Collaborate

BlackBerry AtHoc Collaborate provides a real-time chat-based collaboration session that can be associated with plans and incidents. Collaborate facilitates cross-organization collaboration through the BlackBerry AtHoc management system and the BlackBerry AtHoc mobile app.

Collaboration managers can create, edit, end, archive, and export archived collaborations. Collaboration managers can participate in multiple collaborations at the same time.

Note: Collaborate is not supported in Internet Explorer.

Enable Collaborate in BlackBerry AtHoc

1. Log in to the BlackBerry AtHoc management system as system administrator.
2. Click ⚙.
3. In the **System Setup** section, click **Feature Enablement**.
4. On the **Feature Enablement** screen, click the **IsCollaborationSupported** row.
5. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True**.
6. Click **Save**.

BlackBerry AtHoc Collaborate is enabled.

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

Add a collaboration

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Collaborate**.
3. On the **Collaboration** screen, click **Add Collaboration**.
4. In the **Collaboration Name** field, enter a name.
5. Click +👥.
6. On the **add users** window, select users and groups to add to the collaboration.

   Any operators or users who have registered for Collaborate from the Collaborate menu on the BlackBerry AtHoc mobile app can be added.
7. Click **Add**.
8. Enter your first message in the **Start typing...** field and press **Enter** or click ➤ to start the collaboration.

The collaboration appears in the left pane of the **Collaboration** window with a live status.

Operators and users who are added to the collaboration and have registered for Collaborate using the BlackBerry AtHoc mobile app receive a notification from BlackBerry AtHoc. Clicking the notification launches the collaboration on the BlackBerry AtHoc mobile app.

Add participants to a collaboration

You can add participants to a live collaboration.

Before you begin: Operators must have collaboration manager permissions and must be registered for Collaborate on the BlackBerry AtHoc mobile app to join a collaboration.

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Collaborate**.
3. On the **Collaboration** screen, select a live collaboration in the left pane.
4. In the right pane, click 👤.
5. On the **add users** window, select users and groups to add to the collaboration.
6. Click **Add**.

The participant is added to the collaboration and can send messages. The participant that you add can view all messages for the collaboration.

Note: Once a user is added to a collaboration, if they are later disabled or deleted in the BlackBerry AtHoc management system, they must be manually removed from the collaboration.

Manage collaboration messages

You can edit, retract, delete, or quote sent messages in a live collaboration.

1. Open the collaboration from the BlackBerry AtHoc management system or the BlackBerry AtHoc mobile app.
2. In the right pane, click ● > **Edit** beside the message you want to edit.
   You can also quote, retract, or delete messages.
3. In the **Editing** field, update the message and click ➤.

A ✎ appears beside the edited message.

Add an attachment

Collaboration participants can add text messages, files, pictures, and videos as attachments to collaboration messages. The maximum file size of an attachment is 10 MB.

1. Open the collaboration from the BlackBerry AtHoc management system or the BlackBerry AtHoc mobile app.
2. In the right pane, click 🗋.
3. Browse to the location of the file on your local system and click **Open**.
   The file name and size are displayed above the **Enter a message.** field.
4. Optionally, click ⊗ to remove the attachment.
5. Click the **Enter a message.** field and press **Enter** or click ➤ to send the attachment as a message. You can also add text to the message before sending it.

Collaboration participants can view the attachment in the message or click to download it.

Tip: Click ⋮ > **View attachments** to filter the messages to display only attachments.

Send a message with high importance

1. Open the collaboration from the BlackBerry AtHoc management system or the BlackBerry AtHoc mobile app.
2. In the right pane, click ⓘ.

3. Enter your message in the **Enter a message.** field and press **Enter** or click ➤.

   A ❗ appears beside the sent message.
4. Optionally, click ⓘ to turn off sending messages with high importance.

View the delivery status of messages

In a live collaboration, the following icons beside each message you send indicate the status of that message:

- ✓: Sent
- Ⓓ: Delivered to at least one participant
- D: Delivered to all participants
- Ⓡ: Read by at least one participant
- R: Read by all participants

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

Remove a participant

Operators with the collaboration administrator role in the collaboration can remove participants from the collaboration.

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Collaborate**.
3. On the **Collaboration** page, click a collaboration in the left pane to open it in the right pane.
4. Click **participants**.
5. Beside the name of the participant that you want to remove, click ⊝ > **Remove Collaboration Participant**.

The participant is removed from the collaboration.

End a collaboration

You can end any collaboration that you are an owner or administrator for.

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Collaborate**.
3. On the **Collaboration** page, click a collaboration in the left pane to open it in the right pane.
4. Click ⋮ > **End Collaboration**.

The collaboration ends and becomes read-only and no additional messages can be sent. The collaboration is archived automatically. The archived collaboration is no longer visible in the Collaboration Manager. To view an archived collaboration, see View archived collaborations.

View collaborations in the collaboration manager

All live collaborations appear in the collaboration manager in the left pane. Collaborations that have unread messages appear in bold. Collaborations that have been ended are archived and do not appear in the collaboration manager.

To view an archived collaboration, see View archived collaborations.

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Collaborate**.
3. On the **Collaboration** page, click a collaboration in the left pane to open it in the right pane.
4. Optionally, in a collaboration, click **participants** to view details about the collaboration participants.

   A 🔑 beside a participant name indicates that the participant has collaboration manager permissions and is the administrator for the current collaboration. A 🔑 beside a participant name indicates that the participant has collaboration manager permissions, but is not the administrator for the current collaboration.

View archived collaborations

When a collaboration manager ends a collaboration, it is automatically archived.

1. Log in to the BlackBerry AtHoc management system as an operator with collaboration manager permissions.
2. In the navigation bar, click **Collaborate** > **Ended**.
3. On the **Ended Collaborations** page, click a collaboration in the left pane to open its details, including all messages, in the right pane.
4. Optionally, click ⋮ > **Download attachment** to download a <*collaboration-name*>.zip file that contains the attachments sent during the collaboration.

View collaboration entries in the operator audit trail

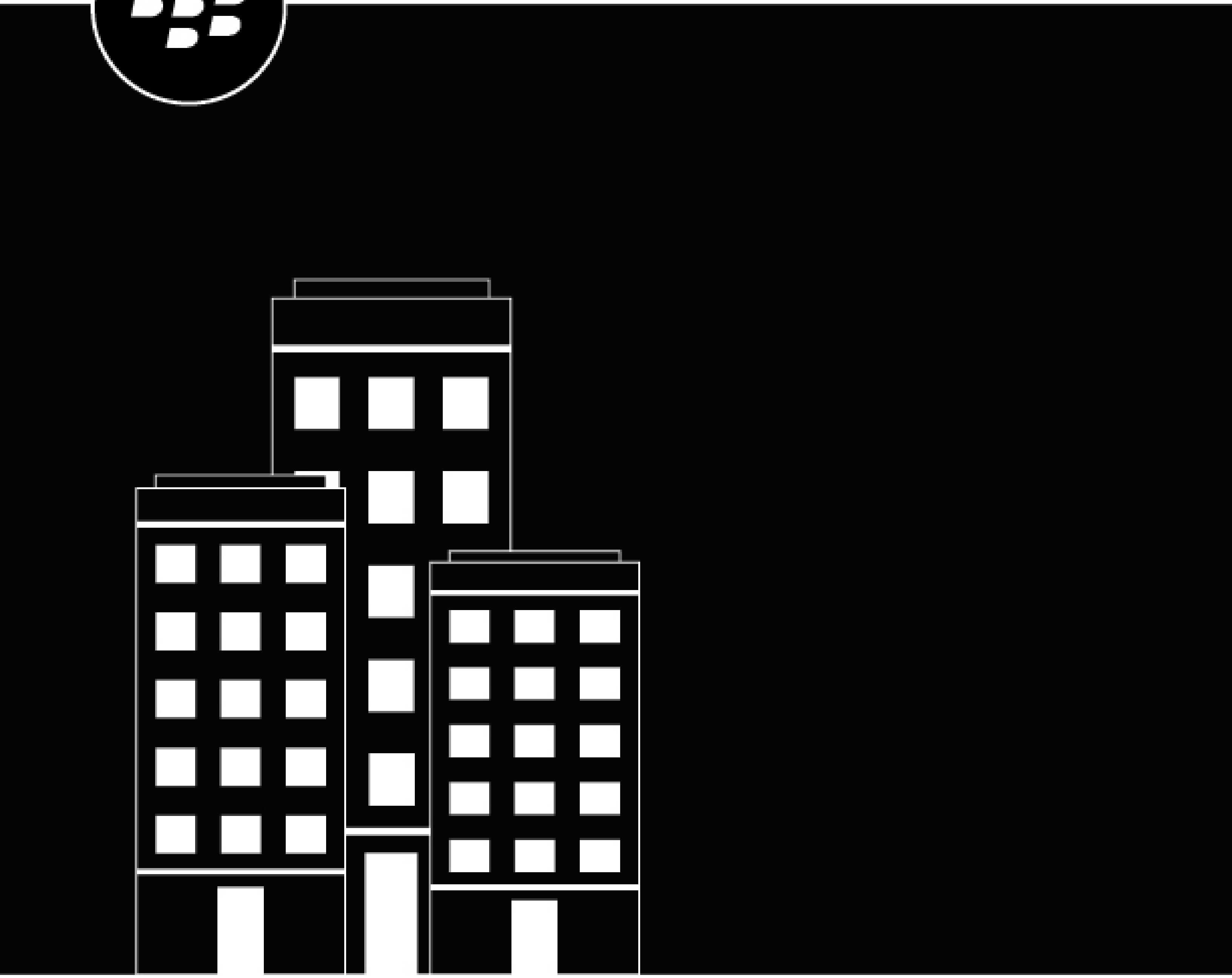
The following collaboration manager activities are added to the operator audit trail:

- Create a collaboration
- End a collaboration
- Add a participant
- Remove a participant
- Promote a collaboration participant

Note: The operator audit trail retains data for 6 months.

1. Log in to the BlackBerry AtHoc management system as Collaboration Manager.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Operator Audit Trail**.
4. Optionally, on the **Operator Audit Trail** page, do any of the following to filter the results:
   - Select a date range from the **To** and **From** fields.
   - Enter an operator name or ID in the **Operator** field.
   - Select **Collaboration** from the **Entity** list.
   - Select the **Search by Specific Action(s)** option and then select actions from the **Action(s)** list.

After you finish: For more information, see View the operator audit trail in the *BlackBerry AtHoc System Settings and Configuration* guide.



BlackBerry AtHoc

AtHoc Account

7.16

Contents

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 unnacounted-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.

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.

1. Log in to the BlackBerry AtHoc management system as an organization administrator, enterprise administrator, or system administrator.
2. Click the **Users** tab.
3. Click on a user you want to grant accountability officer permissions to.
4. On the user profile page, click **Edit Operator Permissions**.
5. On the **Operator Permissions** screen, click **Operator Roles** > **Accountability Officer**.
6. 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 organizational 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**.
3. Click **Users**.
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**.
2. Click **Accountability Templates**.
3. On the **Accountability Templates** screen, click **New** or select one of the out-of-the-box templates.
4. 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 Officer Messages
   - Schedule
5. After you have reviewed the template details, click **Save**.

Access the Accountability Templates screen

1. In the navigation bar, click **Account**.
2. Click **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.
3. 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**.
2. Click **Accountability Templates**.
3. On the **Accountability Templates** screen, click **New** to open the **New Accountability Template** screen, or select one of the out-of-the box templates.

4. 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.
5. 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.
6. 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 **Type** field, select the type of event or event template.
4. 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.
5. Optionally, to insert a placeholder into the event or template title, click ⊞ and select the placeholder from the list that appears.
6. 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.
7. Optionally, to insert a placeholder into the event or template body, click ⊞ and select the placeholder from the list that appears.
8. 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 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.
9. 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.

Important: Always use caution when including attachments in events and alerts. Alerts and events with a large number of targeted users and attachments will experience a significant delay in the expected delivery time. (The delivery time is the total time 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.

Note: 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.

10. 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.
11. If you entered a URL in Step 10, click **Test URL** to verify that the link works.
12. 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.
13. 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** page, 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

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**.
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.

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 on general attributes, organization hierarchies, geolocation, user attributes, or device types. To target or block users based on advanced query criteria, complete the following steps:

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

1. In the **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. From the **Select Attribute** list, select **User Last Updated Source**.
5. Select an operation from the **Select Operation** list.
6. In the blank field that appears, enter the source that you want to target 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	• 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. **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.
	App Audio	• Select whether to use the default or a custom audio sound. The default audio is predefined by your organization. • If you choose **Use Custom Audio**, you can pick from any existing audio sound. • **Best Practice:** Click ► to preview audio selections

Device Type	Options	Explanation
	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	• 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. **Note:** If you select a custom template and your email delivery system does not support it, the default template is used.
	Email Message Content	• Select **Alert Title and Body** to use the information in the alert title and body fields as the email message content. • Select **Custom Text** to enter a custom title and message body as the email message content.
	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.
Text Messaging	Content Sent Via Text	• Select **Alert Title and Body (Short)** to use the first 1250 characters of the alert title and body as the text message content. The text message content is truncated at the first space before the 1250th character. If the content is truncated, the text message includes a link users can click to view the complete alert text. This is the default option. • Select **Alert Title** to use 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 *How does AtHoc SMS support sending text messages to countries abroad?* on the BlackBerry AtHoc customer support site.

Device Type	Options	Explanation
Pager	Content	• Select **Alert Title and Body** to use the information in the alert title and body fields as the pager message content. • Select **Custom Text** to enter a custom message as the pager message content. Custom text must be between 5 and 150 characters.
Cisco IP Phone Display	Alert Image	• Select **None** if you do not want an image to accompany the alert. • Select **Image** to select an image from a predefined list. • Select **Online Image** to enter the URL for an image that you want to accompany the alert.
	Ringtone	• Select **No Ringtone** if you do not want a ringtone to play before the alert • Select **Use Ringtone** to select a ringtone from a predefined list. The tone will sound before the alert content plays.
	Audio Broadcast	• 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.

Device Type	Options	Explanation
Phone	Phone Message Content	- Select **Send Alert Title and Body** to use the information in the alert title and body fields as the phone message content. - Select **Send Custom Text** to enter a custom title and message body as the phone message content. - Select **Send Recorded Message** to create and upload a custom recorded message that will be played for the alert recipients. For 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.
	Recipient Answers the Call	Select what you want to happen after the recipient answers the call: - **Deliver alert without any authentication** - **Deliver alert only after the provided PIN is entered** - **Deliver alert only after user validation**
	Recipient Does Not Answer the Call	Select what you want to happen if the call is not answered: - **Deliver alert as voice mail** - **Leave callback information in the voicemail** - **No voice mail**
	Requires Acknowledgment	Select if the alert has no response options. The acknowledgment steps are provided at the end of the alert.
	Stop Calling Options	Select the criteria you want to use to stop calls from being made to the alert recipient: - **Recipient acknowledged the message** - **Recipient listened to entire message** - **Entire message left on voicemail**
	Call Attempts	Enter the number of attempts the system 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	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. • **None**: Send the alert notification once. • **Default**: Use the default time that has been defined for the selected severity. • For alerts with a severity level of **High**, the default is one notification a minute for 10 minutes. • For alerts with a severity of **Moderate**, **Low**, **Informational**, or **Unknown**, the default is one notification a minute for 2 minutes. • **Custom**: • Select how long to repeat the notification if the user does not respond. • Select how long to pause between each repetition. **Note:** Ensure that the pause time is smaller than the repetition time frame. For example, you can set the **Stop Repetition After** value for 5 minutes, and the **Pause between Notifications** value to 30 seconds - the notification can be repeated up to 9 times. However, if the **Stop Repetition After** value is 5 minutes, but the **Pause between Notifications** value is 6 minutes, the notification is repeated only once. Alert notifications repeat until one of the following occurs: • 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	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. Select **No** to prevent the mobile device from playing any sounds. Alerts of any severity are delivered silently.

Create a custom recorded message for an 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 theBlackBerry 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.

1. In the **Accountability Officers** section of accountability template or event, click **Add Accountability Officers**.
2. On the **Add Accountability Officers** dialog, select the check box next to each user you want to add as an Accountability Officer to the accountability event or template. Only users who are Accountability Officers in the organization are available for selection. You can click **Advanced** and add search conditions to filter the list of Accountability Officers. Any Accountability Officers who are targeted in the Affected Users section are preselected. If affected users are targeted by advanced query in the **Affected Users** section, the same search criteria are prepopulated in the Add Accountability Officers dialog.
3. Click **Apply**.
4. Click **Save**.

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.

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 the event creator to be able to see the Accountability Officer Messages section without being able to edit any fields within it.
   - 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.
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, status attribute, or by date.
4. Optionally, for enterprise organizations, in the **Advanced Filter** window, select an organization from the **Event From** list to view accountability events from suborganizations.
5. Optionally, for 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.

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. 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.

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.

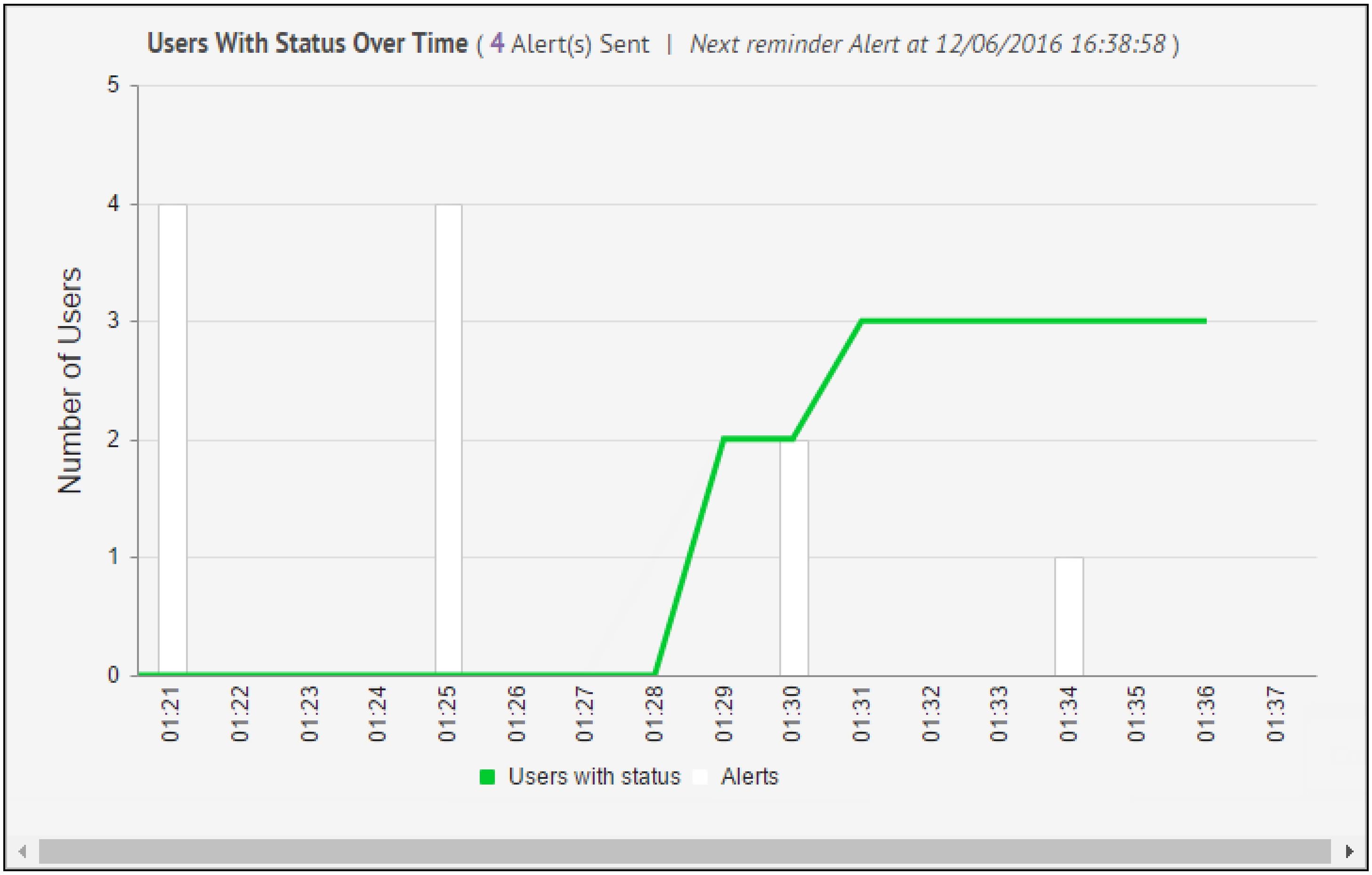
While the event is live, an **Update status on behalf of users** button appears next to these fields. Clicking it takes you to the Users tab where you can manually update user statuses. After an event ends, this button disappears and you can no longer update user statuses.

Status chart

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

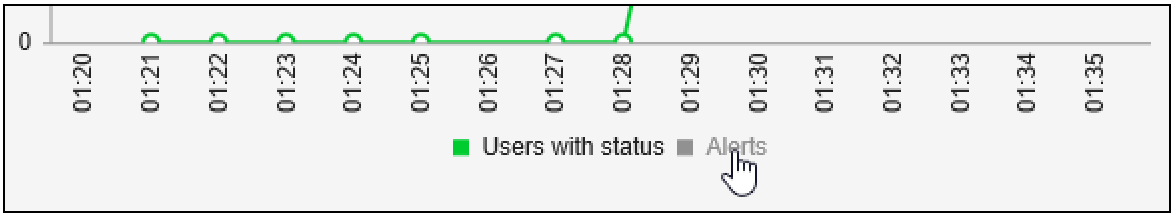
White vertical bars display the total number of users targeted in the initial and all subsequent alerts. This number normally decreases over time as more users provide their statuses and are excluded from subsequent reminder alerts. The final alert is sent to all users to notify them that the event has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

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 of 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.

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* includes 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 organizational 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 an 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 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
- 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.

The Affected Users section on the Details tab contains a link to the Users tab, which provides event-related status information about each user. 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.

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 and Publisher Maps* guide.

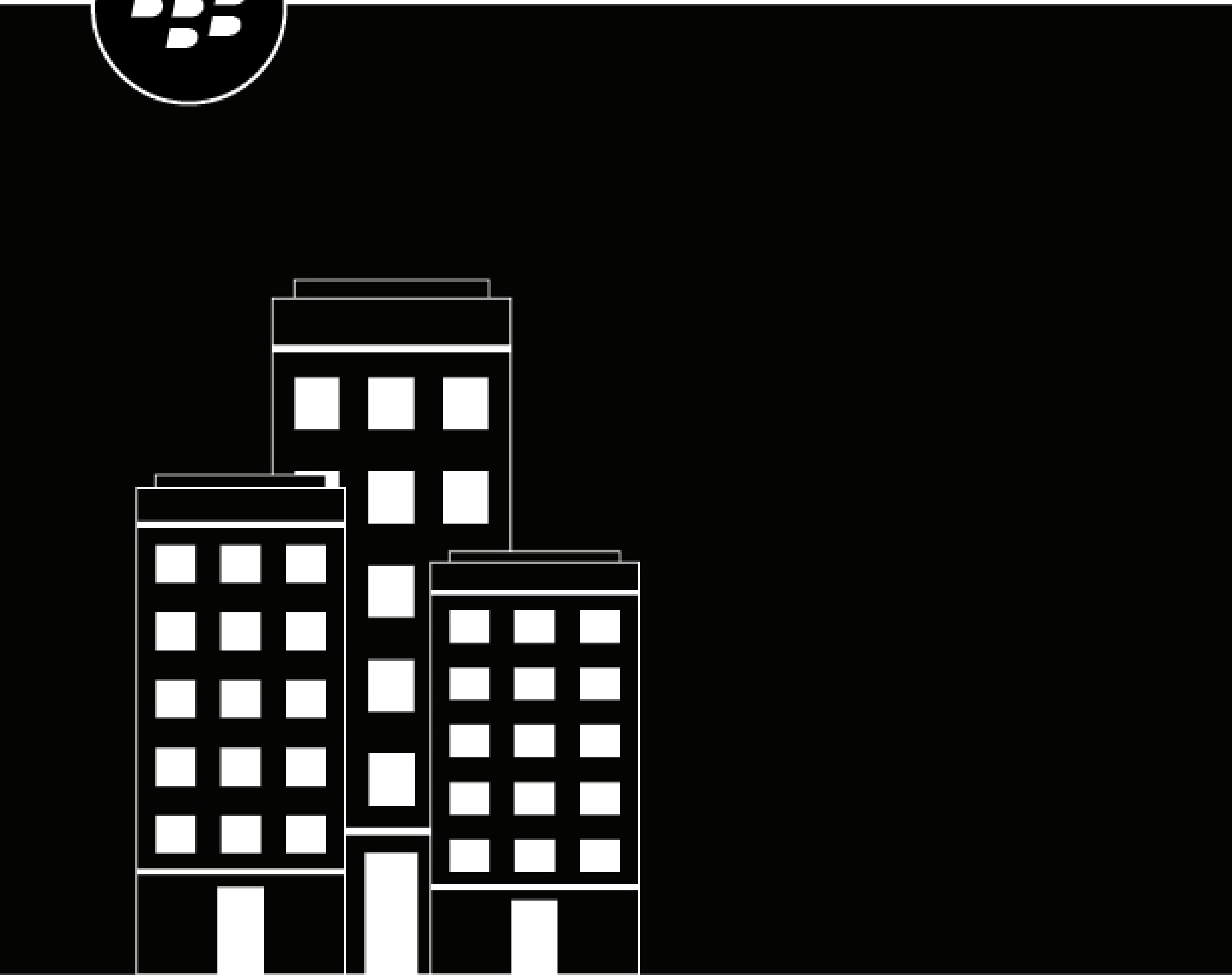
The map displays all live accountability events and alerts for your organization. If you are logged in to an enterprise organization, it also displays live events from your sub organizations.

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

AtHoc Connect

7.16

Contents

Connect organizations with AtHoc Connect

AtHoc® Connect brings together organizations from government, industry, commercial, and healthcare sectors to improve communication during an emergency.

You can send and receive alerts with other BlackBerry® AtHoc® customers that are Connect organizations in BlackBerry AtHoc. A Connect organization is a BlackBerry AtHoc customer that has signed up for AtHoc Connect to participate in cross-organization communication.

With AtHoc Connect, you can connect to other organizations and publish to these connections. You can also receive incoming alerts from connected organizations that target your organization.

To join AtHoc Connect, contact BlackBerry AtHoc customer support.

Prerequisites

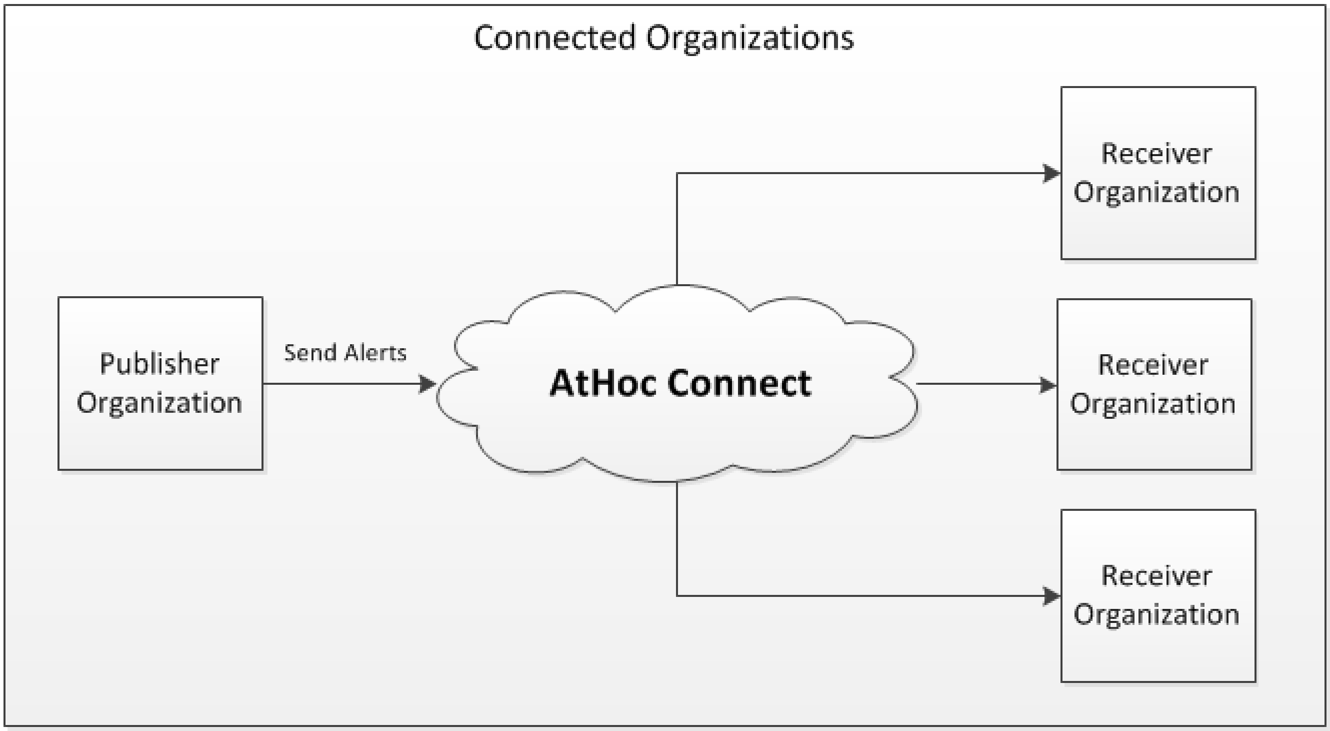
AtHoc Connect requires configuration in the BlackBerry AtHoc management system, Notification Delivery Service (NDS), and registration with BlackBerry AtHoc customer support.

Before you can use AtHoc Connect, you must complete the following prerequisites:

- Configure the AtHoc Connect gateway and device.
- Create an organization in the BlackBerry AtHoc management system for each Connect organization.
- Configure incoming alert types to see incoming alerts in the inbox.
- Log in as an operator with the Connect Agreement Management role.

What is AtHoc Connect?

AtHoc Connect provides a way for operators to target other BlackBerry AtHoc organizations in an alert. For example, the emergency manager for a city might want to send alerts to organizations in the area such as hospitals, schools, military bases, and other groups that are affected by emergencies.



AtHoc Connect includes organizations that connect with each other to share critical information during an emergency. The following are some key terms and concepts within AtHoc Connect:

- **Organization**: An entity within BlackBerry AtHoc that can join AtHoc Connect. An organization can be stand-alone or a member of an enterprise.

  An outside organization can be invited to join the network.
- **Invitation**: A request made to an outside organization to join the AtHoc Connect network.
- **Connect request**: A request made to an AtHoc Connect organization to be connected.
- When sending a request or invitation, you can choose to do one or both of the following:
  - Send Alerts: You invite the organization to receive alerts from you that impact their organization.
  - Receive Alerts: You invite the organization to add you to their target list for alerts that impact your organization.
- **Connected organizations**: The list of AtHoc Connect organizations that have agreed to send or receive alerts from other organizations.
- **Incoming Alerts**: Messages received from outside organizations. For instructions on how to set incoming alert types to trigger alert templates that alert the operator, see "Activate an alert template when an alert is received" in the *BlackBerry AtHoc Alert Templates* guide.

View your organization connections

Note: You must have connect agreement manager, organization administrator, or enterprise administrator permissions to access the Organization menu and screens and to change AtHoc Connect settings.

The Connected Organizations screen provides a summary of your AtHoc Connect network. From this screen you can perform the following tasks:

- View a list of organizations and public feeds you are connected to.
- View the details of a connected organization or subscription
- Add a new connection
- Respond to connect requests from other organizations

1. In the navigation bar, click **Organizations** > **Connected Organizations**. The Connected Organizations screen opens and displays all organizations that have accepted connection requests from your organization. You can also see all organizations your organization has accepted invitations from.
2. Use the **Search** field to locate your connections.
3. Click **Add New Connection** to view options for expanding your network.

Search for a connected organization

The organization search matches any set of letters or numbers anywhere in the organization title and description, and is not case-sensitive. Wildcards are not supported in searches.

1. In the navigation bar, click **Organizations** > **Connected Organizations**.
2. On the **Connected Organizations** screen, in the search field, type or paste a word found in the organization name or description.
3. Click **Search**.

Search and filter the all organizations list

The organization search matches any set of letters or numbers anywhere in the organization title and description, and is not case-sensitive. Wildcards are not supported in searches.

To search and filter the organization list, use the following options from the All Organizations screen.

1. In the navigation bar, click **Organizations** > **All Organizations**.
2. On the **All Organizations** screen, in the search field, type or paste a word found in the organization name or description.
3. Optionally, to filter the organization list by status, under the search field, click ⌄ > **Connected** or **Request Pending**.
4. Optionally, to filter the organization list by industry group, select a value from the **Sector** drop-down list
5. Click **Search**.

View the details of an organization

1. In the navigation bar, click **Organizations**.
2. Click **Connected Organizations** or **All Organizations**.

Note: Outside organizations you have sent an AtHoc Connect network invitation to do not appear in the list if they have not registered for AtHoc Connect .

3. Click the organization that you want to view. The details view opens, showing the organization name, description, sector, contact information, physical address, and a map location.
4. View the status of your relationship with the organization at the top of the screen. An icon and text indicates whether or not you are connected, or if a connect request is pending.
   - **Not Connected**/**Unsubscribed**: No request has been accepted or is pending.
   - **Pending**: Request has not been accepted. To cancel the invitation, click **Cancel Invitation**.
   - **Connected**/**Subscribed**: Connected. You can disconnect from the organization or unsubscribe:
     a. Click **Disconnect** or **Unsubscribe**.
     b. Confirm that you want to disconnect or unsubscribe.

        The status at the top of the Details screen refreshes.

Add a new connection to your AtHoc Connect network

Note: To access the Organization menu and screens and to change AtHoc Connect settings, you must have connect agreement manager, organization administrator, or enterprise administrator permissions.

A connection is an organization within the BlackBerry AtHoc network that you can receive alerts from or send alerts to. You can add a connection to your network using the following methods:

- Add existing organizations from AtHoc Connect to your network of organizations. You send a connect request to the organization to join your network so that you can receive their alerts and they can send alerts to your organization. For details, see Send a connect request to another organization.
- Add an organization that is not a customer of BlackBerry AtHoc to join the AtHoc Connect network. Send a registration invitation to them for AtHoc Connect, so that you can connect and share alerts. For details, see Invite an unlisted organization to join AtHoc Connect.

Search the organizations list

You can search for organizations you are not connected to by name or key word, and by sector. You can search for an organization that you are not connected to, but only organizations that have already registered for AtHoc Connect are displayed in the list.

1. In the navigation bar, click **Organizations** > **All Organizations**.
2. On the **All Organizations** screen, enter the name of the organization or key words, such as "health" or "security".

   Note: Enter simple strings. No wild cards are accepted.
3. Optionally, specify a sector from the drop-down list to filter the list.
4. Click **Search**.

Send a connect request to another organization

1. In the navigation bar, click **Organizations** > **All Organizations**.
2. On the **All Organizations** page, click **+Connect** to add an organization as a connection to your network.
3. On the **Connection Request** screen, select any of the following alerting options:

   - **Send Alerts**: You can send alerts to the organization.
   - **Receive Alerts**: You can receive alerts from the organization.

   Note: If you want to modify these choices later, you can change the connect agreement.
4. Enter custom text to provide a personal invitation to join your network. The custom text can provide information about your organization and the purpose of connection.
5. Click **Send Request**. The connection appears in the Organizations list with the 🕓 to show that an invitation is pending.

When you send a connect request, the Connect invitation template is triggered. Go to **Alerts** > **Alert Templates** > **Connection Invitation** to modify the recipients who will receive the connection invitation.

If the receiving organization accepts the invitation, a connect agreement is created, based on the choices made in the invitation.

If your organization has set up incoming alerts to trigger an alert template, you can see invitations on the Sent Alerts screen.

Invite an unlisted organization to join AtHoc Connect

There might be times when you want to send alerts to organizations that are not yet in the AtHoc Connect network. If you have their contact information, you can invite them to join BlackBerry AtHoc by sending an invitation to an email address. The invitee can fill out a registration form and sign up for a Basic license account from BlackBerry AtHoc.

1. In the navigation bar, click **Organizations** > **All Organizations**.
2. On the **All Organizations** screen, click **Invite Unlisted Organization**.

   Note: You can also invite an unlisted organization from the **Sent Invitation** screen.
3. On the **Invite Unlisted Organization** dialog, enter the name and email address of the invitee organization.

   Note: To improve the chances of the organization accepting the invitation, include the name of a contact and provide a custom message so that the organization knows that this invitation is coming from a known contact.

The organization receives an email inviting them to register for AtHoc Connect. After they register and join AtHoc Connect, you are automatically connected.

Subscribe to a public feed

You can subscribe to public feeds that have been made available on the AtHoc Connect network, such as weather alerts. When you subscribe to a public feed, you receive feed updates as a connection to your network.

1. In the navigation bar, click **Organizations** > **All Organizations**. A directory of AtHoc Connect organizations and public feeds opens. Public feeds display a **Subscribe** button instead of a **Connect** button in the **Connection Request** column.
2. Click **Subscribe** to receive updates as a connection to your network.
3. On the **Subscribe** screen, click **Get Alerts**.

The subscribe request is processed immediately.

Manage connect requests and invitations

There are two places where you view and respond to connect requests, and view and resend invitations to outside organizations.

- For connect requests from or to an AtHoc Connect organization, go to **Alerts** > **Inbox**. Any communication between you and another organization in the AtHoc Connect network is available in the Inbox, including connect requests, or messages about accepted and declined connection requests.

  You can also access recent requests from the Home page under the Organization(s) link in the system status area. Click the **View** link after Request(s) to open the Inbox.
- To view invitations that you have sent to outside organizations, including the status of each one, click **Organizations** > **Sent Invitations**.

View organization connect requests from other organizations

Note: You must have connect agreement manager, organization administrator, or enterprise administrator permissions to access the Organization menu and screen and to change AtHoc Connect settings.

You receive and respond to connection request from other Connect organizations in the alert Inbox.

1. Open the Inbox and do one of the following:
   - From the Home page, click **View** next to Request(s) in the System status panel.
   - In the navigation bar, click to **Alerts** > **Inbox**. The Inbox displays all incoming alerts, including connect requests. Connect requests have a type of “Connect Update.”
2. To filter the list for Connect Updates, complete the following steps:
   a. Click **Advanced** > **Select Alert types**.
   b. Expand the list under **Connect Update** and select the types of updates you want to view in the list.
   c. Click **OK** and return to the list.
   d. Click **Search**.
3. In the **Inbox**, select a Connect update to view the contents in the details pane.
4. Depending on the type of request, complete one of the following steps from the detail pane:
   - Click the name link below the title to view the organization details.
   - Click **Mark as Reviewed** to indicate that you have read the request or update.
   - Click **Accept** or **Decline** to respond to a connection request.

Respond to a connect request from another organization

1. In the navigation bar, click **Alerts** > **Inbox**.
2. From the **Inbox**, click **Accept** or **Decline** for the request that you want to respond to.

View alerts from AtHoc Connect organizations

When an alert is published between organizations, the sender sees the alert from their homepage.

The receiver can see the incoming alert in the following locations:

- In the **Recently Received Alerts** section on the homepage

- In the incoming alerts list in the **Inbox**

The receiver can click **Reply** in the alert row to respond to an incoming alert. The receiver can also click **Forward Alert** to forward the incoming alert to the local organization or to other AtHoc Connect organizations.

View invitations sent to outside organizations

View the **Sent Invitations** list to see the outside organizations that you have invited to join the AtHoc Connect network.

1. In the navigation bar, click **Organizations** > **Sent Invitations**.
2. On the **Sent Invitations** screen, complete any of the following tasks:
   - Search for an invitation by organization name or email address.
   - Sort on any column.
   - Invite additional outside organizations.
   - View the status of any invitation:
     - Pending
     - Failed
     - Expired
     - In Network-Connected
     - In Network-Unconnected
   - Resend an invitation if its status is “Failed” or “Expired.”

Disconnect from a connection

Note: You must have connect agreement manager, organization administrator, or enterprise administrator permissions to access the Organization menu and screens and to change AtHoc Connect settings.

When you disconnect from an agreement to send or receive messages with another organization, you disconnect from the entire relationship. For example, if you have added a connection to your local police force to send and receive alerts and you decide to disconnect, you are disconnected from both types of alerts.

If you want to disconnect from only one type of alert, you can change the connect agreement instead.

1. In the navigation bar, click **Organizations** > **Connected Organizations**.
2. Click the connection from that you want to disconnect from.
3. Click **Disconnect**.
4. Click **Confirm**.

The relationship with the other organization is disconnected immediately.

Unsubscribe from a public feed

1. In the navigation bar, click **Organizations** > **Connected Organizations**.
2. On the **Connected Organizations** screen, click the public feed that you want to unsubscribe from.
3. Click **Unsubscribe**.
4. Click **Confirm**.

Change the connect agreement with an organization

A connect agreement represents the accepted request between two organizations for sending and receiving alerts.

To change the connection agreement with the other organization, you must cancel the current agreement and send a new invitation.

1. In the navigation bar, click **Organizations** > **Connected Organizations**.
2. Click the organization that you want to change the connect agreement with.
3. Click **Disconnect**.
4. Click **Confirm**. The connection status at the top of the screen updates to "Not Connected."
5. Click **Connect** beside the organization to create a new request.
6. On the **Connection Request** screen, select any of the following alerting options:
    - **Send Alerts**: You can send alerts to the organization.
    - **Receive Alerts**: You can receive alerts from the organization.
7. Enter custom text that explains the change in the agreement.
8. Click **Send Request**.

You will receive a notification when the other organization accepts the request.

Send an alert to your BlackBerry AtHoc connections

Prerequisite: Create an alert as described in the *BlackBerry AtHoc Create and Publish Alerts* guide.

1. In the **Content** section of the alert details screen, click **Type** and specify the alert type, such as Fire, Geophysical, or Meteorological.
2. Click **Severity** and specify a severity for the alert.
3. Optionally, if you want responses from the other organization, select one or more options from the **Response Options** list. Add response options to provide predefined responses in the alert for the receiving organization. If the other organization uses a triggered alert template to alert end users, the end users can respond using the options. You can verify that the organization has responded in the tracking report.
4. Optionally, if you want to provide additional information, add a URL to the **More Info Link** field.
5. Optionally, in the **Location** field, click **Add** and then select organizations in a geographical area. Organizations in the shape area are targeted.
6. Optionally, in the **Attachments** field, drag and drop files or click **Browse...** and then navigate to and select files to add to the alert. You can include text, audio, and video files as attachments.

   Note: Attachments must be enabled for the organization. You can add a maximum of 5 files totaling up to 5 MB. The following attachment types are supported: .pdf, .doc, .docx, .xlsx, .xls, .txt, .jpeg, .jpg, .bmp, .png, .mp4, .gif, .mp3, .html, .xml, and .kml.
7. In the **Target Organizations** field, select each organization that you want to send the alert to.

   To select all organizations, select the **Include all connected organizations** option at the top of the **Target Organizations** section.

   Tip: The “Include all connected organizations” option is dynamic. If you use this option in an alert template, all future connections will be added to the list.
8. Complete and publish the alert. The alert is sent to the AtHoc Connect organization and appears as an alert in the Recently Received Alerts section of the homepage or Inbox of the receiver.

If the alert has response options, users in the receiving organization can respond to the alert from the Inbox.

If the receiving organization has triggered an alert template that sends incoming alerts to end users, the response options are provided. When the end user responds to the alert, the originating organization can track the response as a response from the receiving organization.

When an incoming Connect or mobile app alert from a connected organization triggers another alert, any attachments in the incoming alert are not included in the triggered alert.

Configure AtHoc Connect in the BlackBerry AtHoc management system

This section describes how to enable and configure AtHoc Connect for your organization by setting up the delivery and device, customizing visibility settings, and setting up the correct operator permissions so that you can connect with other organizations.

Enable the connect device on the BlackBerry AtHoc server

The first step in configuring devices for BlackBerry AtHoc is to enable the device on the BlackBerry AtHoc server. When you enable the device, it appears in the list of gateways on the Settings screen and in the list of devices.

1. On the server that hosts BlackBerry AtHoc, log in as an administrator.
2. Navigate to the following folder: `../Program Files (x86)/AtHocENS/ServerObjects/Tools`.
3. Open the following application: `AtHoc.Applications.Tools.InstallPackage%;`.
4. On the **Configure Device Support** screen, select the check boxes beside each device that your organization needs.
5. Click **Enable**.
6. Click **Close**.

Configure the BlackBerry AtHoc management system for AtHoc Connect

Each group of BlackBerry AtHoc users is associated with an organization. When you set up your organization, you might also need to configure your system to work with other BlackBerry AtHoc organizations.

Enable BlackBerry AtHoc cloud services polling for the system

To enable BlackBerry AtHoc cloud services polling you must be a system administrator in the System Setup (3) organization.

1. Log into the **System Setup (3)** organization as a system administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **System Settings**.
4. Click **Edit**.
5. In the **Advanced Settings** section, go to the **BlackBerry AtHoc Cloud Services** section and select the **Required** check box beside the **Enable Cloud Services** field.
6. In the **Server Address** field, specify the PSS server address.
7. Click **Save**.

Create a health monitor

Global health monitors monitor the connectivity between AtHoc cloud services (PSS) and the BlackBerry AtHoc management system.

1. Log in to the **System Setup (3)** organization as a system administrator.
2. In the navigation bar, click ⚙.
3. Under **System Setup**, click **Global System Health**.

4. On the **System Visibility Console** screen, click **Create new monitor**.
5. On the **New Health Monitor** screen, enter a name for the new monitor.
6. Select the Health Monitors that you want the new health monitor to be associated with.
7. Select the **Show errors and warnings for this monitor on the Home Page** check box.
8. Select the **Show this Health Monitor in the Organization Visibility Console** check box.
9. In the **How does this Monitor test the system?** section, in the **Choose a test** field, select the **Web Url Test** option.
10. In the **Test Configuration** field, enter a test configuration using the same URL as the NDS server that was used to configure the AtHoc Connect gateway.
11. Leave all of the other fields on the screen unchanged.
12. Click **Save**.

Create an organization for each connection

For each Connect organization, you must create a BlackBerry AtHoc organization on your system.

To create and configure a new organization in the system, you must be a system administrator with permissions to switch between organizations in the BlackBerry AtHoc management system.

1. Log in to the **System Setup (3)** or the **Enterprise** organization that you want to create a child organization for.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Organizations Manager**.
4. On the **Organizations Manager** screen, click **New**.
5. On the **New Organization** dialog, enter a name for the new organization and select an administrator from operators that exist in the system.
6. Click **Save**.
7. In the navigation bar, click your username, and then click **Change Organization**.
8. On the **Change Organization** screen, click the new organization.
9. Click **OK**.

After you finish: Complete the other typical organization set up steps with users, and alert templates. From **Settings** > **General Settings**, you can define the URLs, name, logo images, default alert templates, and Self Service defaults.

Create and enable an organization for a basic account

AtHoc Basic provides a limited set of features for the draft account to publish alerts between AtHoc Connect organizations. A draft organization is used by users that primarily publish alerts across organizations.

1. To create the organization, complete the following steps:

    a. Log in to **System Setup (3)** with an administrator account.
    b. In the navigation bar, click ⚙.
    c. In the **System Setup** section, click **Organizations Manager**.
    d. On the **Organizations Manager** page, click **New**.
    e. On the **New Organization** dialog, enter a name for the new organization.
    f. Select the **Basic** organization type and click **Save**. Details of the new organization appear in the organizations manager with default values appearing for the display name, time zone, and homepage URL.
2. To log in to the account that you set as the administrator, complete the following step:

    a. In the navigation bar, change to the organization that you created. The system refreshes and then displays the new organization. You can confirm that this has happened by looking at the name of the current organization in the top menu bar on the screen.

The homepage opens. If you see a Terms and Conditions page instead of the homepage, do not click the Accept button. Contact BlackBerry AtHoc customer support. The Terms and Conditions should only be shown to the first administrator of the Basic account.

3. To create the draft administrator for the account, complete the following steps:

    a. In the navigation bar, click **Users** > **Users**.
    b. On the **Users** screen, click **New**.
    c. On the **New User** screen, enter a username, password, and email address.
    d. Click **Save**.
    e. On the user details screen, click **Grant Operator Permissions**.
    f. From the **Operator Roles** list, select **Basic Administrator**.
    g. Click **Save**.

Next Steps: You have completed the set up for the Basic organization. The next step is to send the username and password to the Basic administrator so that they can log in to their account.

Configure the AtHoc Connect gateway

Use the AtHoc Connect gateway to set up organizations.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **AtHoc Connect**.
3. On the **AtHoc Connect** screen, enter the URL of the production PSS server.
4. Enter the username and password values for the PSS server.
5. Click **Save**.

Configure the AtHoc Connect device

Note: You must have enterprise administrator permissions to perform this task.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, click the **Mass Devices** tab.
4. Click **AtHoc Connect**.
5. On the **AtHoc Connect** screen, click **Edit**.
6. In the **Details** section, complete the following fields if they are not already populated:
    - Name: **AtHoc Connect**
    - Common Name: **UAP-IAC**
    - Device Group Order: Select a value from the drop-down menu.
    - Contact Info Edit: Select from the following values: **None**, **End Users**, **Operators**, or **All**.
7. In the **Help Text** section, optionally complete the following fields if they are not already populated:
    - Targeting Help Text: **You are about to publish to other Organizations via AtHoc Connect.**
    - Contact Info Help Text
    - Contact Info Tool Tip
8. In the **Delivery Gateways** section, verify that **AtHoc Connect** appears in the list.
9. Click **Save**.
10. Click **More Actions** > **Enable**.

For more information on device configuration, see View and edit device details in the *BlackBerry AtHoc System Settings and Configuration* guide.

Add connect permissions

Operators must have connect agreements manager permissions to manage connections, see the Organizations menu and screens, and view and edit AtHoc Connect settings.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** page, search for the operator you want to add permissions for.
3. Click the name of the operator that you want to add the role to.
4. On the user details screen, click **Edit Operator Permissions**.
5. On the **Operator Permissions** screen, click the **Operator Roles** drop-down list and click to select each of the Connect roles.
6. Click **Save**.

Set up visibility in your connect profile

Note: You must have connect agreement manager, organization administrator, or enterprise administrator permissions to access the Organization menu and screens and change AtHoc Connect settings.

You can use the Add New Organization screen (the AtHoc Connect directory) to choose whether organizations in certain sectors can see your organization. By default, your organization is visible to all other organizations. The visibility setting lets you select relevant sectors. For example, if your organization is in the Federal Defense sector, you can specify that only organizations in the Federal Defense sector can see your organization in the AtHoc Connect directory.

If you are connected to an organization that is outside your selected sectors, your organization is still visible to them in the AtHoc Connect directory. However, if either of you disconnects from sending or receiving notifications, the other organization can no longer see your organization in the directory.

1. In the navigation bar, click **Organizations** > **Connect Profile**.
2. On the **Connect Profile** screen, in the **Visibility** section, select one of the following options:

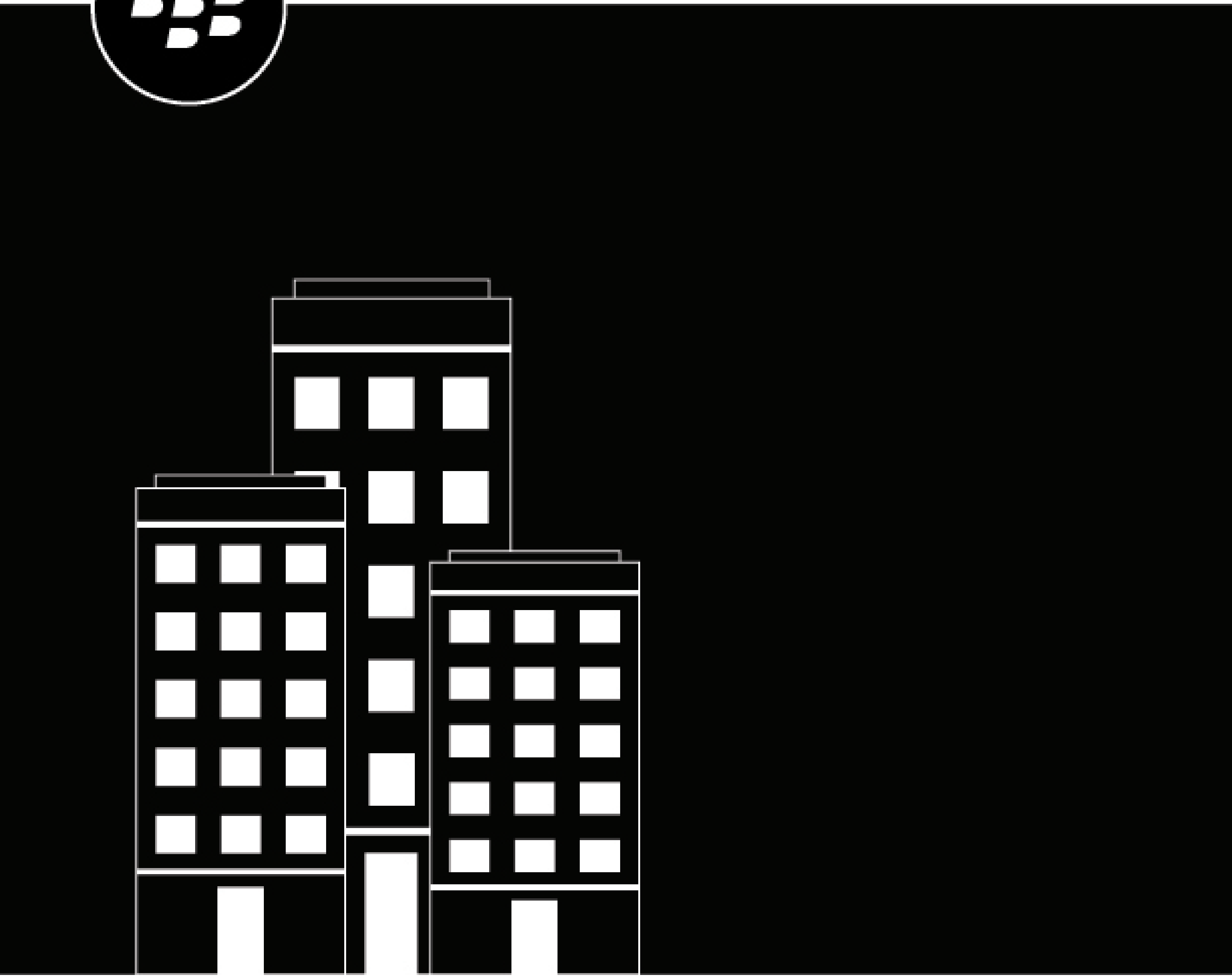
   - Select **All Sectors** if you want to allow any organization to send connect invitations.
   - Select **Selected Sectors** if you want to limit your visibility by sector.

     a. Click the drop-down list under the **Selected Sectors** option.

     b. Select one or more sectors that connect with your organization. For example, if you choose Education, only organizations in the Education sector can view your organization in the Organizations list.

        Note: If you choose **All Sectors**, all current sectors are selected and can see your organization. However, if sectors are added to AtHoc Connect, organizations in the new sectors will not be able to see your organization because they will not have been selected.

     c. Remove sectors by clicking ☒ inside the related sector pill.
3. Click **Save**.



BlackBerry AtHoc

Integrated Weather Alerts

7.16

Contents

What is Integrated Weather Alerts?

Organizations that require the latest information about severe weather events can enhance their BlackBerry® AtHoc® system by using AtHoc Integrated Weather Alerts (IWA). To stay informed about potential weather incidents such as tornadoes, floods, and dust storms, IWA subscribers receive critical warnings and forecasts from the National Weather Service (NWS.) All weather-related information can be incorporated into targeted alerts using a variety of delivery devices available in the BlackBerry AtHoc system.

- **Instant alerts of critical weather conditions to targeted personnel**

  IWA can be configured to automatically send alerts to the appropriate personnel. IWA distributes emergency weather alerts to targeted personnel using network-connected devices including computers, SMS, and mobile phones. Emergency operators can decide if they want the system to alert their center first so they can qualify the situation before sending out an alert, or have the system automatically send alerts to predefined groups once threats are identified.
- **Flexible weather information sources**

  IWA includes out-of-the-box integration with the NWS. It can also be configured to work with other standard GeoJSON-based weather data feeds.
- **Automatic monitoring of specific weather conditions**

  Operators set criteria for the types of weather situations that qualify as emergencies. The system automatically monitors events and alerts personnel when the criteria are met. For example, the system can be configured to alert emergency operators only when hurricanes in the region reach a specific severity level. The qualifications of a threat differ for each installation and each site can customize the alerting preferences to meet its requirements. Automatic monitoring provides increased accuracy, quick delivery of alerts, and the ability to receive events during off-duty hours.
- **Pre-programmed actions for specific weather conditions**

  Operators can pre-program specific alert templates that are activated automatically when a specific weather situation is identified.
- **Target users with geo-targeting**

  Refine your alert targeting using geo-targeting. Select a location on a map to alert users in a specific location about weather events that are the most relevant to them.
- **Assured alert delivery and acknowledgment**

  The BlackBerry AtHoc system tracks who has received the alert, and if relevant, acknowledges its receipt. This assures that the appropriate personnel received the notification.

How Integrated Weather Alerts works

BlackBerry AtHoc Integrated Weather Alerts polls weather feeds from the NWS and records them in the BlackBerry AtHoc database. IWA processes incoming feeds based on event location, type, and severity. When a feed matches the configured conditions, an alert is triggered and sent to end users.

Plan your AtHoc IWA system

All use cases for AtHoc IWA require some planning and use of different BlackBerry AtHoc features such as creating weather alert rules and alert templates.

Begin planning by answering the following questions and gathering the information required for configuration. Take into consideration that you will need to create weather alert templates and rules for each organization in your BlackBerry AtHoc system.

Define alert conditions

- **Locations to monitor**

  What US states/territories and counties do you want to monitor weather events for? Enable geo-targeting to further refine the weather alerts received by targeted users.

  IWA supports all territories covered by the NWS.
- **Weather events to monitor**

  What types of weather events do you want to monitor? Examples include floods, thunderstorms, and hurricanes.
- **Event severity**

  What is the severity of weather events that you want to monitor? You can select to monitor minor, moderate, severe, extreme, and unknown weather events. You can also select to monitor weather events of any severity, or any combination of levels of severity.

  IWA supports all severity levels provided by the NWS.
- **Message type**

  What type of messages do you want to monitor? You can select to monitor for advisory, alert, danger, outlook, statement, warning, and watch message types. You can monitor all message types, which is the default. You can select any combination of message types to monitor.

Select alert rule actions

What alert templates do you want to trigger when specific weather conditions are met? You can create weather alert rules that trigger sending predefined alert templates. The operator can then select the alert template, and then decide if they want the map in the alert template to be overridden by the map in the weather feed. For more information, see Enable geofence targeting.

Incoming weather events that affect the selected counties are delivered to targeted recipients using selected delivery devices such as PCs, mobile phones, and sirens. You can create multiple rules. Each rule can be for a specific location or type of event. For example, you can create one rule for San Mateo county that monitors for tsunamis, and a separate rule for San Francisco county that monitors for earthquakes.

Configure AtHoc IWA

The general procedure to configure IWA is:

1. Enable IWA for each organization in your BlackBerry AtHoc system.
2. Create alert templates for each organization that has enabled weather alert rules.
3. Create alert rules for each organization that specify the weather event severity, type, message type, and location.
4. Enable the feed poller and feed processor jobs on your BlackBerry AtHoc system.

How to use geo-targeting with IWA

Weather feeds from the NWS contain geolocation information that can provide a more precise area for targeting weather related alerts than by county alone. When a weather alert feed contains a geolocation, depending on how you configure your weather alert template and alert rules, you can use the geolocation from the feed to define the targeting of users based on their location. You can enable geolocation targeting by selecting a location on the map in a weather alert template and selecting to target users in those locations.

Geo-targeting settings

The following matrix shows how the geotargeting settings in alert templates and alert rules impact the use of maps from the alert template and feed in triggered alerts. In the matrix, a 🌐 means that the map from the weather feed is used in the triggered alert. A 📁 means that the map from the alert template is used.

If:												
Alert template	Has Map	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
	Has Geo Targeting – Users	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓
	Has Geo Target – Organizatic	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓
Feed	Has Polygon	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓
Alert rule	Uses Geo Informatioı from feed	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✓
		⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
Then:												
Triggered alert	Has Map	✗	✗	✗	🌐	📁	✗	✗	📁	📁	📁	🌐
	Geo Targeting – Users	✗	✗	✗	✗	✗	✗	✗	📁	📁	📁	🌐
	Geo Targeting – Organizations	✗	✗	✗	✗	✗	✗	✗	✗	📁	📁	🌐

Configure the Integrated Weather Alerts Module

This section explains how to configure BlackBerry AtHoc IWA.

Note: The BlackBerry AtHoc system must be installed and configured at your site before configuring AtHoc IWA.

Enable AtHoc IWA

AtHoc IWA is included in the BlackBerry AtHoc system, but is disabled by default.

You must enable IWA for each organization in your system.

1. Log in to the database server.
2. From the NGADDATA database, run the following script:

   ```
   INSERT INTO PRV_CONFIG_TAB VALUES (providerId,'Features
   Matrix','IsWAMSupported','true','key to enable disable wam weather feed')
   ```

Create weather alert templates

Note: You must create weather alert templates on each organization in your system that you want to send integrated weather alerts from.

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Alerts** > **Alert Templates**.
3. On the **Alert Templates** screen, click **New**.
4. On the **New Alert Template** window, complete the required template sections to define alert template content, target users, and select personal devices.

For complete instructions on how to create a new alert template, see the *BlackBerry AtHoc Alert Templates* guide.

Use placeholders for weather alerts

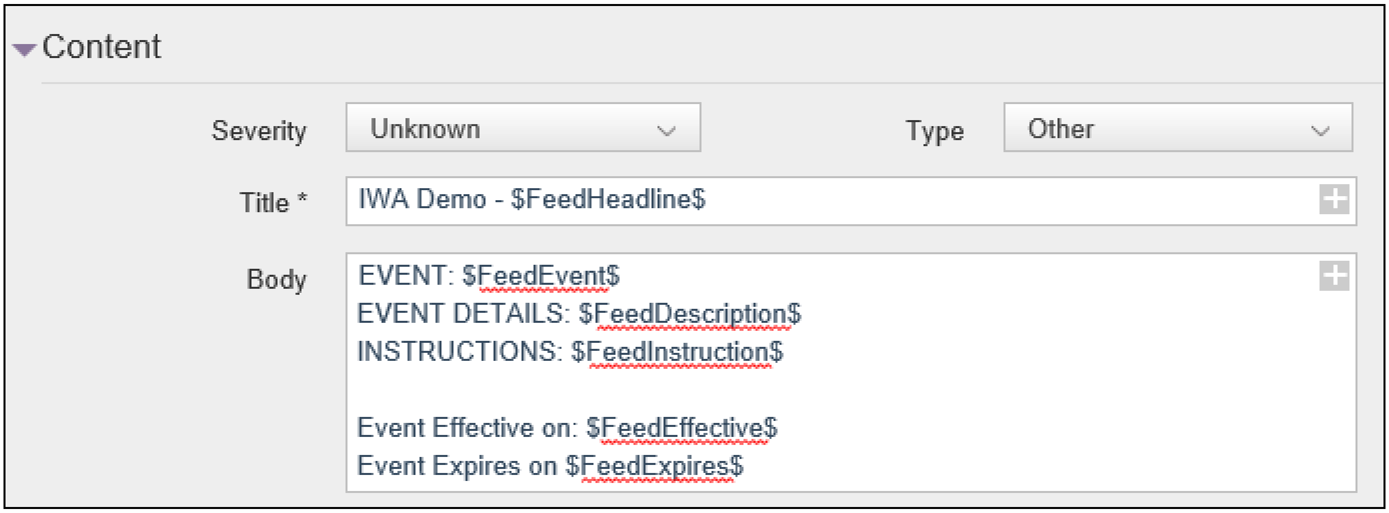
You can use weather alert placeholders to update the content in your weather alert template with the information from an incoming weather feed. When an alert is triggered by a weather feed, the alert is sent out with the title and body from the alert template, unless a weather alert placeholder is used. If the weather alert template includes placeholders and text in the title and body, the triggered alert contains the text from both the alert template and from the weather feed.

The following placeholders are available for weather alerts:

- $FeedHeadline$
- $FeedEvent$
- $FeedDescription$
- $FeedInstruction$
- $FeedSenderName$
- $FeedEffective$
- $FeedExpires$

For a sample weather feed that resolves these placeholders, see Sample weather feed.

Your alert templates can include only placeholders, only text, or a combination of placeholders and text. The following is a sample alert template that includes both text and placeholders:


Content

Severity: Unknown

Type: Other

Title *: IWA Demo - $FeedHeadline$

Body:

```
EVENT: $FeedEvent$
EVENT DETAILS: $FeedDescription$
INSTRUCTIONS: $FeedInstruction$

Event Effective on: $FeedEffective$
Event Expires on $FeedExpires$
```

You can also use the predefined Weather Feed Alert template, which includes all of the available weather alert placeholders.

Define alert template content

The Content section is used to define the key parts of an alert or alert template in the system: title, body, type, response options, website links, locations, and attachments.

1. To create an alert or alert template in a language other than the default language displayed on the screen, click the button beside the Type field and select a language. This does not change the language displayed on the screen. Instead, it changes the language that the message is delivered in. If text-to-speech is enabled, the audio portion of the sent alert will be in the language you selected.
2. In the **Severity** field, select the severity level from the list.

   Important: High severity is reserved for extreme emergencies. On the mobile application, it overrides the device sound settings to emit any sounds associated with the alert template.
3. In the **Title** field, enter a one-line summary that communicates the purpose of the alert or alert template. The maximum number of characters is 100. The title is required. However, this title is over-written by the Headline field of an incoming NWS feed. For more information, see Use placeholders for weather alerts.
4. In the **Body** field, enter up to 4000 characters of text that communicate why the alert has been sent and provide instructions to the target audience. Note that the content in the Body field is over-written by the Description field of an incoming NWS feed. For more information, see Use placeholders for weather alerts.
5. In the **Type** field, select the type that fits with the alert template you are creating.
6. In the **Response Options** field, do one of the following:

   - Click **Custom Response Options** to view a list of preset responses.
   - Click **Add Response Option** to define one or more responses that alert recipients can send to let you know that they have received the message. If the response involves a call bridge, select the **Call Bridge** checkbox, then, in the two fields that appear below the checkbox, enter the call bridge number and passcode users need in order to respond.
7. Optionally, in the **More Info Link** field, enter a URL that opens a web page where users can go to get more details about the alert when it is sent out.
8. Optionally, if you entered a URL in the previous step, click **Test URL** to verify that the link works correctly.
9. Optionally, in the **Location** section, click **Add** to access a map where you can select a geographic area for the alert or alert template. This location can also be used to target users by location. For more information, see Target users by location.
10. Configure the Target Users section.

Target users

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

Target users by groups

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

You can also block recipient groups (exclude them from alert delivery.)

The Group target categories displayed are:

- **Organizational Hierarchy**: If your system is set up for them
- **Distribution Lists**: Static and dynamic
- **Targetable Attributes**: Any attributes that have been selected as targeting criteria

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

1. In the **Target Users** section, click the **By Groups** tab if it is not already selected.
2. In the **Groups** field, select the checkbox next 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, they can be manually deselected by clicking the checkbox next to its name. If you select all of the sub-groups or sub-distribution lists manually, the parent group or distribution list is not selected automatically.

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

Target users by location

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

You can also target users in a specific US county or counties by selecting those counties in a weather alert rule.

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

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

   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 Targeting Summary section updates to display the total number of locations on the map that will be used to target recipients.

4. In the **Target Users** section, click **By Advanced Query**. By default, users who have a location attribute in the selected locations and who have a Last Known Location attribute updated within the last 4 hours are targeted.
5. Optionally, 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 **Targeting Summary** section, click the number beside **By Location** to open a map that shows the targeted locations.
8. Optionally, to target users with geofence targeting, see Enable geofence targeting.

Select personal devices

After selecting the users or groups you want to include in the alert template, you must select the personal and mass devices to use to contact the target group.

1. In the **Target Users** section, click the **Select Personal Devices** tab. A list of all available personal devices appears with information about the total number of selected users who can be reached by each device type.
2. Select the check box next to each personal device you want to include. As you select devices, the pie chart on the side of the screen updates to show the number of reachable and unreachable users based on your current selections.
3. Optionally, click the number beside the **Total Users** field to view a User Listing screen that displays the username and organizational hierarchy for each of the users in the target group.
4. Optionally, click the numbers in the **Reachable Users** and **Unreachable Users** fields to view separate pop-up screens that provide user details for those subgroups.

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

Create a weather alert rule

To begin processing Integrated Weather Alerts, you must create alert rules that are designed to trigger alert templates. Each weather alert rule must contain a selected county and an alert template before it can be enabled.

You must create weather alert rules for each organization you want to send integrated weather alerts from.

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Alerts** > **Alert Rules**.
3. On the **Alert Rules** page, click the **Weather** tab.
4. Click **New Rule**.
5. On the **New Rule** page, in the **General** section, enter a name for the rule and select the option to enable the rule.
6. In the **Condition** section, click **Select** beside **Counties**.
7. On the **Select Counties** window, on the **All Counties** tab, select one or more counties. You can click ⌄ **All States** to filter counties by state. You can also search for a specific zip code.
8. Optionally, click the **Selected Counties** tab to verify the counties you selected.
9. Optionally, click **Modify** to change your county selection.
10. Click **Apply**. You are returned to the New Rule page. The counties you selected appear in the Counties area.
11. Optionally, select a **Weather Severity**. The following severities are available: Extreme, Severe, Moderate, Minor, and Unknown. You can select one, multiple, or all severities.
12. Optionally, select a **Weather Type**. You can select one, multiple, or all weather types. See Weather types for the list of available weather types.
13. Optionally, select a **Message Type**. The following message types are available: Alert, Cancel, and Update. You can select one, multiple, or all message types. Select **Alert** to send an initial alert to targeted users. Select **Update** to update and replace an existing alert. Select **Cancel** to cancel an earlier alert.
14. In the **Action** section, select an alert template.

15. Optionally, select the **Override Geo Information** option. When selected, the map from the incoming weather feed overrides any map in the alert template. If the alert template has geo-targeting enabled, the alert is triggered for the location from the feed. If not selected, the map and geo-targeting from the original alert template is used in the triggered alert.
16. Click **Save**. The new weather alert rule is created and enabled by default.

One alert is generated per rule when an incoming feed matches the rule criteria. All conditions you specify must be met by a weather feed before an alert is triggered. For example, if you select Extreme for Weather Severity, and Coastal Flood Warning for Weather Type for San Mateo county, only weather feeds that are extreme severity coastal flood warnings that target San Mateo county trigger the selected alert template.

Weather types

The following weather types are available when creating a weather alert rule:

- Avalanche Warning
- Avalanche Watch
- Blizzard Warning
- Coastal Flood Warning
- Coastal Flood Watch
- Dust Storm Warning
- Earthquake Warning
- Extreme Wind Warning
- Fire Warning
- Flash Flood Statement
- Flash Flood Warning
- Flash Flood Watch
- Flood Statement
- Flood Warning
- Flood Watch
- High Wind Warning
- High Wind Watch
- Hurricane Statement
- Hurricane Warning
- Hurricane Watch
- Severe Thunderstorm Warning
- Severe Thunderstorm Watch
- Severe Weather Statement
- Snow Squall Warning
- Special Marine Warning
- Special Marine Statement
- Special Weather Statement
- Storm Surge Warning
- Storm Surge Watch
- Tornado Warning
- Tornado Watch
- Tropical Storm Warning
- Tropical Storm Watch
- Tsunami Warning
- Tsunami Watch
- Volcano Warning
- Winter Storm Watch
- Winter Storm Warning

Note: BlackBerry AtHoc supports weather types from the National Weather Service (NWS.) For more information, see https://www.weather.gov/nwr/eventcodes.

Enable geofence targeting

Use the Location section of the weather alert template Content section to select a location on a map to target weather alerts and to enable geo-targeting.

Prerequisites

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

1. Open the weather alert template you want to enable geofence targeting for.
2. In the **Content** section of an alert or alert template, in the **Location** section, click **Add** to access a map on which you can select a geographic area for the alert or alert template.
3. 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.

4. Click **Apply**. The Targeting Summary section updates to display the total number of locations on the map that will be used to target recipients.
5. In the **Location** section, select **Enable Geofence Targeting**.
6. In the **Target Users** section of the weather alert template, click **By Advanced Query**. By default, users who have a location attribute in the selected locations and who have a Last Known Location attribute updated within the last 4 hours are targeted.
7. Optionally, click **map selection(s)** to change the selected locations.
8. Optionally, enter a number and select **Minute(s)**, **Hour(s)**, or **Day(s)** to change the timeframe for the Last Known Location attribute.
9. Optionally, in the **Targeting Summary** section, click the number beside **By Location** to open a map that shows the targeted locations.
10. Click **Select Personal Devices** and select the check box beside each personal device you want to include.
11. Click **Review and Publish**.
12. Optionally, on the **Review and Publish** screen, click **Preview and Publish** to preview how the alert will appear to end users.
13. Click **Publish**.

Enable the feed poller and processor jobs

After configuring your weather alert templates and rules, you must enable the feed poller and feed processor jobs on your BlackBerry AtHoc system to start receiving weather feeds from the NWS.

1. Log in to the BlackBerry AtHoc management system.
2. Click the down arrow beside your log in name and select **Change Organization**.
3. Change to the **System Setup (3)** organization.
4. In the navigation bar, click ⚙.
5. In the **System Setup** section, click **System Jobs**.
6. Click the **Feed Poller** system task.
7. On the **Feed Poller** screen, in the **Task Details** section, click **Click to Enable**.
8. Click **Back** to return to the System Tasks screen.
9. Select the **Feed Processor** system task.
10. On the **Feed Processor details** screen, in the **Task Details** section, click **Click to Enable**.

Export weather feed information

Weather feed information is retained in the BlackBerry AtHoc system for 15 days. If you want to view weather feeds that were recorded in the last 15 days, you can export them to a .csv file. You can export weather feed information even if the Integrated Weather Alerts feature is not yet enabled for your specific organization.

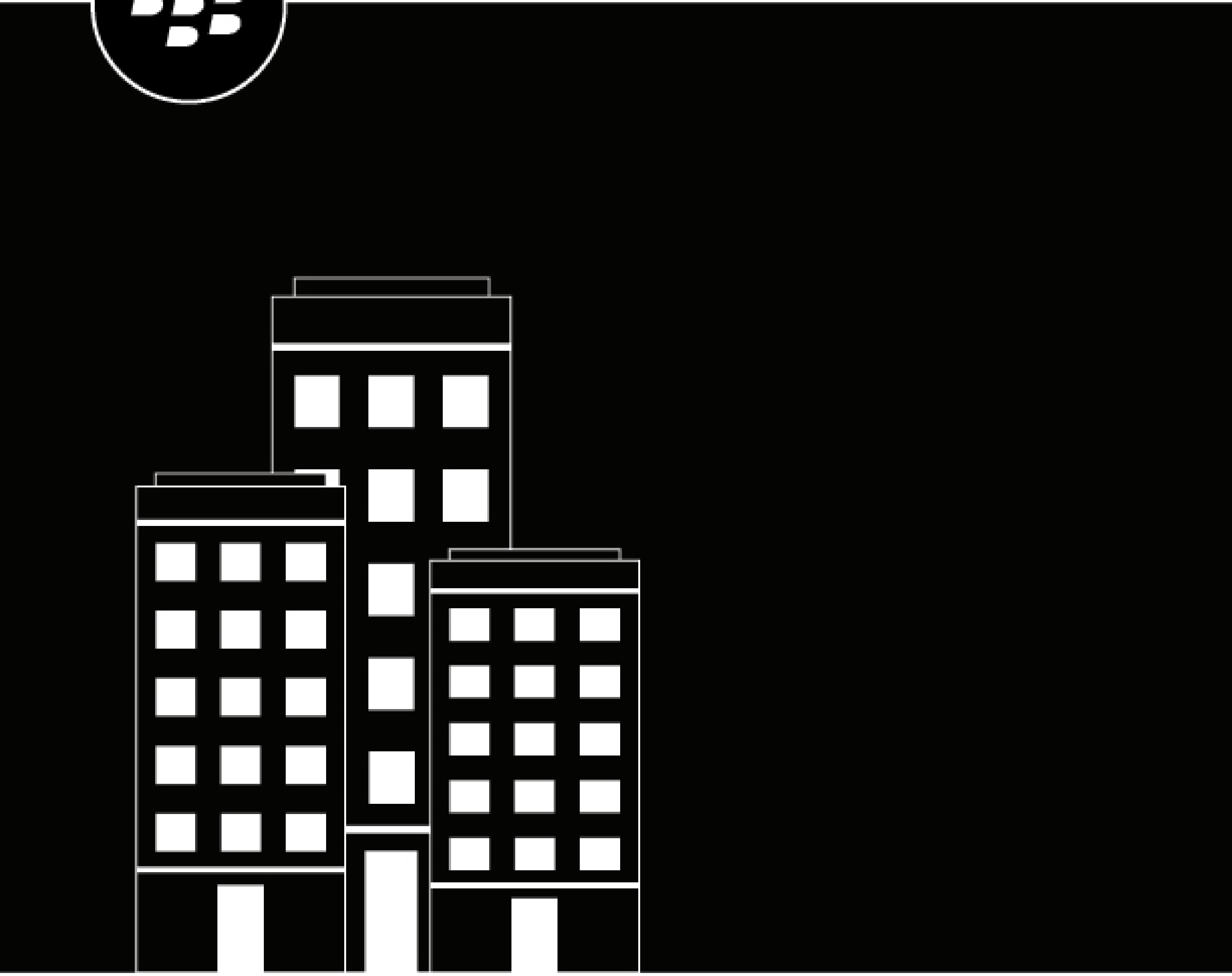
You can also export all weather alert rules defined for your organization.

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click ⚙.
3. In the **Basic** section, click **Alert Rules**.
4. On the **Alert Rules** page, select the **Weather** tab.
5. Select the check boxes beside the weather alert rules you want to export.
6. Click **Export CSV** > **Rules**.
7. In the Windows pop-up, choose to open or save the .csv file to your local system.
8. Select **Feeds** from the **Export CSV** list.
9. On the **Export Feeds** window, select the check boxes beside the counties you want to export weather feed information for. You can narrow the list by selecting a state from the All States list, or by searching by zip code.
10. Click **Export**.
11. On the Windows pop-up, choose to open or save the .csv file to your local system.

Sample weather feed

The following is a sample weather feed. The bolded fields are resolved by the weather placeholders listed in Use placeholders for weather alerts.

```
       {
  "@context": [
  "https://raw.githubusercontent.com/geojson/geojson-ld/master/contexts/geojson-base.jsonld",
  {
   "wx": "https://api.weather.gov/ontology#",
   "@vocab": "https://api.weather.gov/ontology#"
  }
 ],
 "type": "FeatureCollection",
 "features": [
  {
   "id": "https://api.weather.gov/alerts/NWS-IDP-PROD-2358285-6219777",
   "type": "Feature",
   "geometry": {
    "type": "Polygon",
    "coordinates": [
     [
      [
        -156.29,
        20.68
      ],
     [
      -156.45,
      20.70
     ],
     [
      -156.47,
      20.79
     ],
     [
      -156.47,
      20.88
     ],
     [
      -156.27,
      20.92
     ],
     [
      -156.29,
      20.68
     ]
    ]
   ]
  },
  "properties": {
   "@id": "https://api.weather.gov/alerts/NWS-IDP-PROD-2358285-6219777",
   "@type": "wx:Alert",
   "id": "NWS-IDP-PROD-2358285-6219777",
   "areaDesc": "Maui",
   "geocode": {
    "UGC": [
     "HIZ018",
     "HIZ017"
    ],
    "SAME": [
     "015009",
     "015009"
    ]
   },
   "references": [
    "https://api.weather.gov/alerts/NWS-IDP-PROD-2358285-6219776"
   ],
   "sent": "2017-07-26T17:39:56+00:00",
   "effective": "2017-07-26T17:39:56+00:00",
   "onset": "2017-07-11T17:39:00+00:00",
   "expires": "2017-07-28T19:15:00+00:00",
   "ends": "2017-07-28T19:15:00+00:00",
   "status": "Actual",
   "messageType": "Update",
   "category": "Met",
   "severity": "Moderate",
   "certainty": "Likely",
   "urgency": "Expected",
   "event": "Flood Advisory""sender": "NWS Honolulu HI",   "headline":"Flood
 advisory issued July 27 at 2:34AM HST expiring July 28 at 5:30PM HST by NWS
 Honolulu HI"   "description""instruction": "Stay away from streams, drainage
 ditches and low lying areas prone to flooding. Rainfall and runoff will also
 cause hazardous driving conditions due to ponding, reduced visibility and poor
 braking action.",
   "response": "Avoid",
   "parameters": {
    "VTEC": [
     "/O.EXT.KREV.FA.Y.0010.000000T0000Z-170516T1915Z/"
    ],
    "PIL": [
     "REVFLSREV"
    ],
    "BLOCKCHANNEL": [
     "CMAS",
     "EAS",
     "NWEM"
    ],
    "eventEndingTime": [
     "2017-07-16T19:15:00Z"
    ]
   }
  }
 }
],
  "title": "Current watches, warnings, and advisories"
}
```



BlackBerry AtHoc

Activity Log

7.16

Contents

Manage the Activity Log

This guide describes how to manage and view the Activity Log.

Note: The Activity Log is an advanced feature that requires additional licensing, so it is not available by default. Contact your BlackBerry® AtHoc® representative if you are interested in using the Activity Log.

If you are an Activity Log Manager or Activity Log Viewer and have a license for the Activity Log feature, you can use the Activity Log to view and create log entries, such as phone calls, incidents, meeting minutes, or other relevant information for your organization. You can also forward published alerts to additional recipients or organizations.

Add an entry to the Activity Log

You can add entries to the Activity Log to record an action or event, such as a response to a distress call.

1. In the navigation bar, click **Alerts** > **Activity Log**.
2. On the **Activity Log** screen, click **New**.
3. On the **New Log Entry** window, enter a title and body for the log entry.
4. Optionally, in the **More Info Link** field, enter a URL that users can click to access related information.
5. Select a severity level.

   If the log entry is published as an alert, the severity level will be used. You can change the severity level when you review the content before publishing the alert.
6. Click **Save** to save the log entry or click **Save and Forward as Alert** to open the **Review and Publish** screen where you can publish the content as an alert.

When you create a log entry and forward it as an alert:

- The alert title, body, additional link, and severity are copied to the alert.
- An entry is added to the Activity Log with the log type: Alert Published.

Publish a log entry as an alert

1. In the navigation bar, click **Alerts** > **Activity Log**.
2. On the **Activity Log** screen, select the log entry to be published and click **Forward Alert** in the details pane.
3. On the **New Alert** screen, complete the alert Content and Target Users sections and then publish the alert.

Note: Published activity log entries can be forwarded, but not edited, and have the Alert Published log type.

Forward published alerts

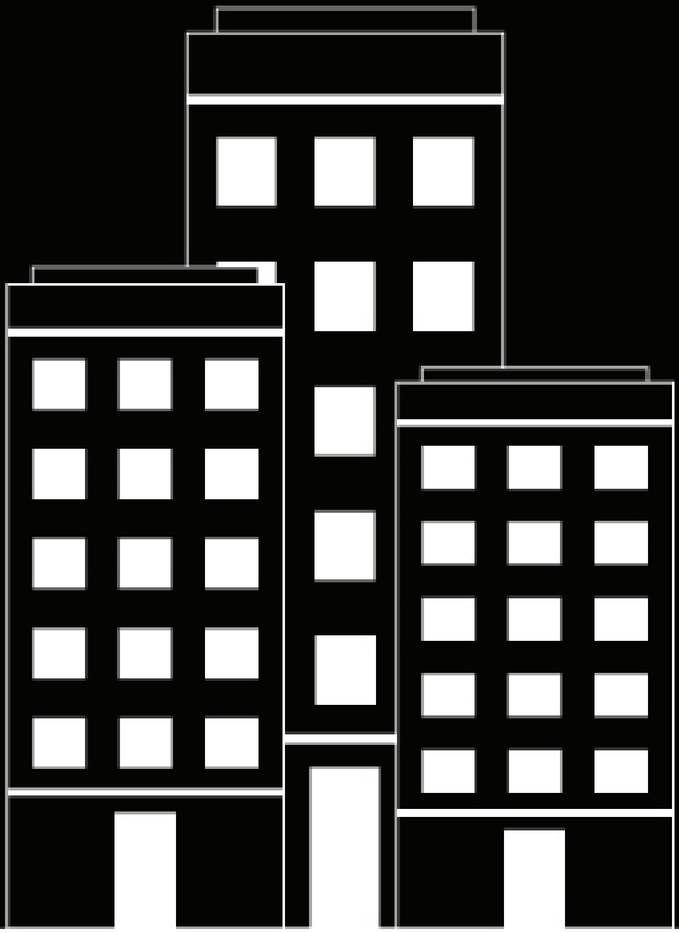
1. In the navigation bar, click **Alerts** > **Activity Log**.
2. Select the alert to be forwarded and click **Forward as Alert** from the details pane.
3. On the **New Alert** screen, complete the alert Content and Target Users sections and then publish the alert.

Export the Activity Log to PDF or CSV

1. In the navigation bar, click **Alerts** > **Activity Log**.

2. On the **Activity Log** screen, click **Export**
3. On the **Export Log** window, select a date range for the entries to be exported.
4. Click **Export PDF** or **Export CSV**.

The export file downloads to your local system.



BlackBerry AtHoc

Operator Roles and Permissions

7.16

Contents

Operator roles and permissions

Only BlackBerry® AtHoc® System Administrators, Enterprise Administrators, and Organization Administrators can access the Edit Operator Permissions button on the user details page. The Edit Operator Permissions button displays the Operator Permissions page. The Operator Permissions page is used to grant or revoke a user's operator rights and assign operator roles. The Operator Permissions page also allows authorized users to define the user base of each operator. The user base is the subset of end users a publisher can target alerts to.

Operators cannot update their own roles and permissions. Administrators cannot assign or revoke permissions for a higher-level role than their role. For example, an Organization Administrator can grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

An enterprise organization displays users and operators in each suborganization. An operator in a suborganization can be made an operator in the enterprise by using the Edit Operator Permissions button on the user details page in the enterprise organization. For more information, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations*.

User base overview

A user base is a subset of end users that an operator can target alerts to and access through the Users and the Distribution Lists screens. Operators who have an unrestricted user base can target and access any user in the BlackBerry AtHoc system, while operators who have a restricted user base can target only the end users in their user base.

Operators who have a restricted user base cannot view information about users outside of their authorized user base, including in advanced reports, alert report summaries, delivery summary .csv files, or from the Details tab of a sent alert. A banner indicates how many users out of the total number are accessible for an operator with a restricted user base.

Note: If an operator with a restricted user base creates another operator, the new operator has the same user base restrictions. The parent operator can further restrict the user base of the new operator, but cannot assign them a less restricted user base.

The user base of an operator consists of end users from the following sources, which can be assigned using the User Base and Distribution Lists Permissions tabs of the operator:

- **Organizational nodes** (Optional. Not available on all systems): Users are selected based on membership in selected organizations.
- **Standard or customized user attributes assigned to end users**: Users are selected based on specific attributes such as department, job function, or location.
- **Distribution lists**: Users are selected based on their inclusion in selected distribution lists. Using distributions lists to identify users might result in the inclusion of people outside the designated user base of an operator.
- **Dependents**: Users are selected based on their relationship to a sponsor user.

The following table summarizes operator access privileges for features based on their user base.

User Base Restricted by....	Targeting Privileges	Distribution Lists Manager can...	End Users Managers can...
Custom or standard end user attributes	Operators can target only users who meet the specified attribute conditions	• Access the Distribution Lists screen • Assign users in their user base to static distribution lists	• View users in their user base • Edit custom and standard user attributes • Edit users device addresses and alert delivery schedules
Distribution lists (DLs)	Operators can target only the DLs they have Publishing privileges to. Static DLs can include users outside the user base. Dynamic DLs include only users in user base.	• Access the Distribution Lists screen • Access only the DLs they have View/ Manage privileges to	• Edit user memberships in static DLs
Organizational nodes	Operators can target all members of a selected organization.	—	• Assign user base to any organization to which operator has access privileges

User Base Restricted by....	**Targeting Privileges**	**Distribution Lists Manager can...**	**End Users Managers can...**
Dependents	Operators can target the dependent users of targeted sponsors.	—	• View and Edit dependents

Switch a user base from unrestricted to restricted

If you have the necessary permissions, you can change the user base of an operator from unrestricted (the default) to restricted within BlackBerry AtHoc.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the name of the operator.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and then select the **Restricted** option.
5. Click **Save**.

Note: For complete details on how to set up restrictions on a user base, see Restrict a user base by attributes.

Note: You can also switch a user base from unrestricted to restricted with the Import Operators feature. For more information, see Importing and exporting operators.

Restrict a user base by attributes

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

If a parent operator has an unrestricted userbase, they can use either the AND or OR operators when assigning permissions to other operators. If a parent operator has a restricted userbase, they can only use the AND operator when assigning permissions to other operators. This prevents operators with a restricted userbase from assigning another operator permissions to access a less restricted userbase.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and select **Restricted**.
5. Click **Modify**.
6. Select the AND/OR operator. When AND is selected, the user attribute must meet all conditions to restrict the user base. When OR is selected, attributes that match any of the conditions are included. The default is AND.
7. On the **Create Conditions** screen, click **Select Attribute** and select the first attribute you want to use as restriction criteria.
8. In the **Select Operator** field, select the operator that you want to assign to the attribute.

   Note: The list of operators varies depending on the type of attribute selected.
9. In the next field that appears, enter or select a value for the attribute.
10. Optionally, click the **Add Condition** button and then repeat steps 7 through 9 for each additional attribute condition you want to add.

    Tip: You can restrict a user base using the User Last Updated Source attribute. For more information, see Restrict a user base with the User Last Updated Source attribute.
11. Optionally, if your organization is set up to display organizations, in the **Organization Hierarchy** section of the **User Attribute** drop-down 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.
12. When you are done creating restriction criteria, click **Apply**.
13. Optionally, on the **Operator Permissions** screen, view the list of end users who meet the criteria by clicking **View users** in the **User Base** section.
14. Click **Save**.

Restrict a user base with the User Last Updated Source attribute

Operators can restrict a user base with the User Last Updated Source attribute. The following table lists the possible sources and the search terms available to restrict a user base by source.

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

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and select **Restricted**.
5. Click **Modify**.
6. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
7. Click **Select Attribute** and select **User Last Updated Source**.
8. Select an operation from the **Select Operation** list.
9. In the blank field that appears, enter the source to restrict the user's user base permissions 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.
10. Click **Apply**.
11. Click **Save**.

Restrict operator access to dependents

When an operator's access to dependents is restricted, the operator cannot view, edit, or delete a dependent user. The operator cannot target dependents in alerts or events, view them in reports, or export their data.

Operators have access to view, manage, and target dependents by default.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the **Operator Permissions** screen, scroll down to the **User Base** section and deselect the **Enabled** check box in the **Manage and Publish to Dependents** section.
5. Click **Save**.

Grant operator permissions to a user

When you grant operator permissions to a user, you select which roles the user has in BlackBerry AtHoc. The roles a user has determine the BlackBerry AtHoc features they can access. The roles that can be assigned to users are determined by the enable features in an organization.

Only Organization Administrators, Enterprise Administrators, and System Administrators can grant operator permissions to users. Operators cannot update their own permissions. Operators cannot assign or revoke higher level operator permissions than their own permissions. For example, an operator with Organization Administrator permissions can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

1. Create a user or select an existing user. After you create a new user and click **Save**, the user details screen appears.
2. Click **Grant Operator Permissions**.
3. On the **Operator Permissions** screen, click the **Operator Roles** list and select the roles you want to assign to the user.

   As you select roles, they appear on the screen under the Operator Roles drop-down list. If you select more than three roles, the first three are displayed, and the rest can be seen by clicking the scrollbar that appears in the field.

   Tip: Click **Operator Roles and Permissions Matrix** to view a complete mapping of BlackBerry AtHoc roles and their capabilities.
4. Optionally, enter and confirm a password that meets the specified requirements.
5. Optionally, select the check boxes to specify if the user must change their password at next login, and whether the password expires.
6. Click **Save**.

Note: You can also grant operator permissions using the Import Operators feature. For more information, see Importing and exporting operators.

Edit operator permissions

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

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the operator name in the list.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the **Operator Permissions** screen, click the **Operator Roles** drop-down list and select the roles that you want to assign to the user.

   Note: Only operator roles that are at the same or lower-level than your role appear in the list. For example, if you are an Organization Administrator, you cannot assign the Enterprise Administrator role to another operator.
5. To remove an operator permission, click the **X** beside the name.
6. Click **Save**.

Note: You can also edit operator permissions with the Import Operators feature. For more information, see Importing and exporting operators.

Revoke operator permissions

You can only revoke the permissions of an operator whose permissions are at the same or lower level than your permissions.

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

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the operator you want to revoke permissions for.
3. On the user details screen, click **More Actions** > **Revoke Operator Permissions**.

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

Note: You can also revoke operator permissions using the Import Operators feature. For more information, see Importing and exporting operators.

Revoke operator permissions from the External Operator Permissions screen

Use the External Operator Permissions settings page to revoke permissions for an operator who has permissions in another organization. You can only revoke the permissions of an operator whose permissions are at the same or lower level than your permissions. Only Organization Administrators, Enterprise Administrators, and System Administrators can revoke operator permissions.

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

1. Log in to the management system as an administrator and change to the organization you want to assign roles in.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **External Operator Permissions**. A list displays the operators who have operator permissions in an organization that you also have operator permissions in.
4. On the **External Operator Permissions** screen, click the name of the operator. The user details screen opens, displaying the information for that user in the system.
5. Click **Revoke**. A warning screen appears, asking "Are you sure you want to revoke Operator Permissions for this user?" and informing you that this action cannot be reversed. Revoking operator permissions cannot be reversed, but you can later assign the permissions to the operator again using the **Edit Operator Permissions** button on the user details screen. If you want to remove only one or more operator permissions for a user, click the **X** in the pill for that role in the **Operator Roles** section.

Revoke operator permissions automatically

If you are an Organization Administrator, Enterprise Administrator, or System Administrator, you can configure your BlackBerry AtHoc system to automatically revoke operator permissions. When configured, operators who have not logged in to the system for the specified time have their permissions revoked. The operator's inactivity period is calculated using the Last Login Date attribute. If the operator has not logged in to the system, the inactivity period is calculated based on the date the operator was granted permissions on. When automatic revocation of operator permissions is enabled, a system job runs every 24 hours to revoke operator permissions based on the operator's last successful login.

Tip: Use the Last Login Date attribute to identify and notify operators whose permissions will be automatically revoked due to inactivity.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Revoke Operator Permissions** section, click **Add Condition**.
4. Select one or more roles from the **Operator Roles** list.

   Note: You can only revoke permissions for operators who have the same or lower-level permissions that you have. For example, if you are an Organization Administrator, you cannot revoke the permissions of Enterprise or System Administrators.
5. Select the number of days of inactivity from the **Auto Revoke Permissions after** list.
6. Optionally, click **Add Condition** to add an additional revocation rule. You can add up to three rules.
7. Optionally, click ⊟ to remove a revocation rule.
8. Click **Save**.

Assign distribution list permissions

In each organization, someone is usually assigned the role of Distribution Lists Manager. The Distribution Lists Manager can create, edit, delete, and import distribution lists. This is a distinct and more powerful role than being able to edit a distribution list and use it to target alerts. Operators with the Advanced Alert Publisher or Draft Publisher role cannot manage distribution lists, but can select lists as recipients for an alert.

Note: You can assign distribution list permissions to an operator in another organization using the External Operator Permissions screen.

Note: You can only assign distribution list permissions to distribution lists that you have access to.

Assign distribution list permissions from the User Details screen

You can only assign distribution list permissions to distribution lists that you have access to.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the name of the user to whom you want to assign distribution list permissions.
3. On the user details screen, click **Edit Operator Permissions**.
4. In the **Distribution Lists** section, do one of the following:
   - Keep the default settings of **Unrestricted** for the Publish and Manage fields to allow the user to manage and publish alerts to all existing distribution lists in the organization that the user is associated with.
   - Set one or both fields to **Restricted** if you want to limit the distribution lists that a user can manage or publish.
5. If you selected the first option in Step 4, go to Step 8. If you selected the second option in Step 4, continue to Step 6.
6. When you select the **Restricted** option next to the **Publish or Manage** field, a **Modify** link appears next to it.
7. Click **Modify** to open the **Distribution Lists** screen, which displays all distribution lists in the system.
   - To allow the operator to publish to a specific list, select the check box in the **Publish** column for that list.
   - To allow the operator to view and edit a specific list, select the check box in the **View/Manage** column for that list.
8. Click **OK**.

The distribution list permissions of the user are updated in the system.

Assign distribution list permissions from the External Operator Permissions screen

You can only assign distribution list permissions to distribution lists that you have access to.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **External Operator Permissions**.
3. On the **External Operator Permissions** screen, click the name of the operator you want to give distribution list permissions to. You can search by username to narrow the list of operators.
4. On the operator details screen, in the **Operator Roles** section, select **Dist. Lists Manager** from the **Operator Roles** list.
5. Optionally, to grant the operator access to publish to all distribution lists, select the **Publish Unrestricted** option in the **Distribution Lists** section. This is the default option.

6. Optionally, to grant the operator access to publish to specific distribution lists, in the **Distribution Lists** section, select the **Publish Restricted** option, and then click **Modify**. On the **Distribution Lists** screen, select the check box in the **Publish** column for each distribution list you want to give the operator permissions to publish to. Click **OK**. You are returned to the operator details screen.
7. Optionally, to grant the operator access to manage all distribution lists, in the **Distribution Lists** section, select the **Manage Unrestricted** option. This is the default option.
8. Optionally, to grant the operator access to manage specific distribution lists, in the **Distribution Lists** section, select the **Publish Restricted** option, and then click **Modify**. On the **Distribution Lists** screen, select the check box in the **View/Manage** column for each distribution list you want to give the operator permissions to publish to. Click **OK**. You are returned to the operator details screen.
9. Click **Save**.

Importing and exporting operators

The Operator Import and Export feature enables Enterprise Administrators and Organization Administrators to add a large number of operator accounts to their BlackBerry AtHoc organization by using a .csv file. Enterprise Administrators can also import and export operators for all suborganizations from an enterprise organization.

The Operators Import and Export feature is enabled for all organizations by default. This feature can be disabled for any organization, if needed. For more information, see "Enable and disable features" in the *BlackBerry AtHoc System Settings and Configuration* guide.

The Operator Import and Export feature enables administrators to perform the following actions for up to 500 operators in a single operation:

- Add operator roles to existing users
- Add restrictions to existing users
- Remove operator roles and restrictions from existing users.
- Revoke all operator permissions
- Add or remove operator user base restrictions
- Add or remove operator access to static distribution lists, dynamic distribution lists, user bases, and folders
- Update password expiration settings
- Update the "User must change password at next login" setting
- Add or remove an operator's ability to manage dependents or publish alerts to dependents

The following are prerequisites and restrictions for importing and exporting operators:

- You must be an Enterprise Administrator or Organization Administrator.
- Operators cannot update their own permissions.
- Operators cannot assign or revoke higher level operator permissions than their own permissions. For example, an Organization Administrator can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.
- Only existing enabled users in the given organization can be imported as operators.
- If an import includes an Organization column and you are performing the import from an enterprise organization, operators are imported for both the enterprise and suborganizations. Only Enterprise Administrators can import or export operators across the enterprise and suborganizations.
- If no Organization column is included in the import file, operators are imported only to the current organization.
- When updating a user base restriction for an operator, there is a limit of 10 conditions. You can use the OR or AND operators to update a user base restriction. You must enclose each condition and operand with double quotation marks (""). For example, `"username" "contains" "abc" OR "organizational hierarchy" "at or below" "xyz"`.
- All distribution lists, folders, and attributes being imported for an operator account must already exist in your organization.
- Only users with unique user names and mapping IDs in the system can be granted operator permissions.
- Partial import is not supported. (If an attribute for an operator in the import .csv file is incorrect, the operator is not imported.)
- Up to 500 operators can be imported in a single import.
- Parallel imports are not supported. Only a single operator or user import can be processed at a time.

Import operators using a .csv file

Important: When you import operator details into BlackBerry AtHoc using a .csv file, the values that exist in the .csv file overwrite any existing values in the database. If the file contains blank fields, the current values in the database are replaced by empty values. You should make sure that all required fields are populated before you upload the file.

To import operators from a file, the file must be correctly formatted. If you do not know how to format the file, see Format an operator import file.

If duplicate operators (identified by username or mapping ID) are found in the .csv file, they are not imported and one of the following error messages is displayed:

```
[Username]: <username> already exists in the payload
```

```
[Mapping ID]: <mapping id> already exists in the payload
```

The remaining non-duplicate operators in the .csv file are imported.

If a username contains a space or one of the following characters, the user is not imported and an error message is displayed:

[ ] : : | = , + * ? < >

Leading or trailing spaces are ignored and trimmed during the import process. After the spaces are trimmed, the username is accepted and the operator is imported.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click **More Actions** > **Import** > **Operators**.
3. Optionally, to download a blank .csv file to use as a template for your import operator file, click the **Download a template CSV file**. Save the file to your computer and fill in the appropriate operator information.

   Note: Using the template ensures that all of the mandatory attribute columns are included in the import file.
4. Click **Browse**.
5. Navigate to the location of the import operator file on your computer.
6. Open the file to enter or modify the operators' data.

   Note: Microsoft Excel hides some characters from view. If you edit the file in Microsoft Excel, it might format your entries with extra characters. The incorrect format might cause the import operation to fail. If you are using anything other than a text editor to modify the .csv file, open the file in a text editor such as Microsoft Notepad, review the syntax for problems, then save the modified file as a .txt file. Edit the file name to change the extension from .txt to .csv. This method preserves the formatting in the text file.
7. Verify that columns with multiple values have the correct format to import correctly.

   - The entire entry must be enclosed within double-quotes. This rule is true even if a multi-select picklist has only a single entry.
   - Use a comma to separate each value. Do not include spaces before or after the comma.
   - If you are importing user base restrictions, you must enclose each value with double quotation marks ("").
8. After you have entered your data, save and close the file.
9. Click the filename, and click **Open** to upload the file into the system.

   The filename appears in the Operator CSV File field on the Import Operator screen. Each of the columns from the import file are listed in the **Select the columns to import** section.
10. Select the columns of data you want to import or click **Select All**.
11. Review the **Columns that cannot be imported** list to verify that it does not contain important data that you must be able to view within BlackBerry AtHoc. If the list contains important columns of information, contact BlackBerry AtHoc Customer Support for help.
12. Click **Import**. The Importing Operators window opens.

When the import completes, the Import Details: Import Completed screen displays the following information:

- Total number of operators in the import file
- Total number of operators who were processed

- Number of operators who were successfully processed
- Number of operators who failed to be processed
- Username of the person who imported the file
- Time the file import process started and ended

Tip: Click **Download Log** on the Import Details: Import Completed screen to download a .csv file that includes information about the sync status of the operator import.

Format an operator import file

In order to import a .csv operator file, the following formatting standards are required:

Field Name	Description	Is Mandatory?
Username	The Username is a value that can be used to identify a user in the BlackBerry AtHoc system and the user repository (for example, LDAP or Microsoft Active Directory) within your organization. The Username column must contain a unique value. The username cannot contain spaces or any of the following characters: [ ] : ; | = + * ? < >. Leading or trailing spaces are trimmed during the import process. After the leading or trailing spaces are trimmed, the username is accepted and the operator is imported.	Yes

Field Name	Description	Is Mandatory?
Roles	Use the Roles column to assign roles and their associated permissions with an operator. To include multiple roles, use a comma-separated list with no spaces. The following roles can be included: • Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Basic Administrator • Basic Operator • Connect Agreement Manager • Dist. Lists Manager • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Report Manager • SDK User • User Manager **Note:** The roles that can be imported depend on the type of organization that you are importing operators in to (suborganization, enterprise organization, or system setup). For more information about BlackBerry AtHoc roles and permissions, see BlackBerry AtHoc roles.	Yes
Permission expiration date	Set a date in the format configured for your organization in General Settings, or leave the cell blank to have no expiration date. The date must be equal to or later than the current date.	No
Alert Folders manage/ publish	Enter the names of alert folders to give the operator permission to create, rename, delete, and publish alerts to them.	No
User base manage/ publish	Enter the user attributes you want to restrict the operator's access to. Leave this column blank to import operators with an unrestricted user base. You must enclose each value with double quotation marks (""). **Tip:** Open the user profile of a user in your organization that has a restricted user base and click 📋 in the **User Base** section to copy the attributes.	No

Field Name	Description	Is Mandatory?
Dependents manage/ publish	Enter **Yes** to enable the operator to create, delete, edit, and publish alerts to dependent users. Enter **No** to restrict the operators permissions to manage and publish alerts to dependent users. If a value is not entered, it is treated as a **No** value.	No
Distribution List publish	Enter the names of static or dynamic distribution lists the operators will have permission to publish alerts to.	No
Distribution List manage	Enter the names of static or dynamic distribution lists the operators will have permission to manage.	No
Password never expires Yes/No	Enter **Yes** to configure the operators' passwords to never expire.	No
Change password next login Yes/No	Enter **Yes** to require operators to reset their password at next login.	No
Organization	Use the Organization column to assign operator roles to operators in organizations across the enterprise (including both the enterprise and suborganizations.) **Note:** The Organization column does not assign users to organizations, it assigns operator roles in the specified organization.	No

Stop the import operators process

Important: When you import operator details into BlackBerry AtHoc using a .csv file, the values that exist in the .csv file overwrite any existing values in the database. If the .csv file contains blank fields, the current values in the database are replaced by empty values.

While the import operator process is underway, click **Cancel** or **Back** to stop the import.

Records that have already been added are not removed and records that have been updated are not restored to previous values. To download a .csv file that contains information about the operators that were imported before the import was stopped, click **Download Log** on the **Import Details: Stopped** window.

Undo the import operators process

The import operators process cannot be undone after it runs. The only way to undo the import is to reimport the original data that was overwritten.

Export operators to a file

You must be an Enterprise Administrator or Organization Administrator to export operators. Only enabled users with operator roles can be exported. The export operator process exports all roles and permissions for the selected operators in the current organization. Enterprise Administrators can export operators from the enterprise organization for all operators in the enterprise and suborganizations. The Export Operator feature must be enabled for the organization.

1. In the navigation bar, click **Users** > **Users**.
2. Select the check boxes beside the usernames that you want to export.
3. Click **More Actions** > **Export** > **Operators**. The Exporting Operators window opens while the export is in progress.

When the export is complete, a .csv file is downloaded. The .csv filename has the following format: AtHoc-{*provider-name*}ExportCSV_{*current-date-and-time*}.

The downloaded .csv file contains the following information for the exported operators:

- Username
- Firstname
- Lastname
- Displayname
- Roles
- Permission expiration date
- Alert Folders manage/publish
- User base manage/publish
- Dependents manage/publish Yes/No
- Distribution List publish
- Distribution List manage
- Password changed date
- Password never expires Yes/No
- Change password next login Yes/No
- Last login date
- Organization. (For enterprise organizations only.)

Switch organizations

1. In the navigation bar, click the username that is logged in.
2. Click **Change Organization**.

   Note: If your username is associated with only one organization, the Change Organization link does not appear.
3. On the **Change Organization** screen, click the name of the organization you want to switch to.
4. Click **OK**.

Subscribe users to organizations

This section describes how to subscribe users to suborganizations other than their home organization using the BlackBerry AtHoc management system or the .csv user import process. For instructions on how to subscribe to organizations from Self Service, see the *BlackBerry AtHoc Self Service User Guide*.

For more information about organization subscriptions, see Manage organization subscriptions in the *BlackBerry AtHoc Manage Users* guide.

Before you begin: Before users can be subscribed to organizations, the following conditions must be met:

- The Organization Subscriptions feature must be enabled on the enterprise organization.
- The Enterprise Administrator must configure the subscription organizations.

The Organization Subscription for End Users option must be selected in the Customization > Self Service section in General Settings in a suborganization for end users to be able to subscribe to that organization from Self Service.

Subscribe a single user

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select a user from the list.
4. On the user details screen, click **Edit User**.
5. On the user details screen, in the **Organization Subscriptions** section, click **Add Subscription**.
6. On the **Subscribe Organization** screen, select an organization from the list.
7. Click **Apply**.
8. In the **Organization Subscriptions** section, enter a date or click 📅 to select a start date for the subscription.
9. Optionally, click 📅 to set an end date for the subscription.
10. Optionally, repeat Steps 5 to 9 to subscribe the user to additional organizations. You can subscribe the user to a maximum of 10 available organizations.
11. Click **Save**.

The user can now be targeted in alerts and events from the subscribed organizations.

Subscribe multiple users

You can also use the .csv user import process to delete or modify organization subscriptions for multiple users.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select the users you want to subscribe to organizations.
4. Click **More Actions** > **Export** > **Users**.
5. On the **Export Users** screen, in the **All Columns** list, select **Subscribed Organizations** > **Add >**.
6. Click **Export CSV**.
7. Save the .csv file to your local system.
8. Open the .csv file.

9. Update the **Subscribed Organizations** column to add, remove, or modify the organizations for each user. You can subscribe each user to a maximum of 10 available organizations.
10. Optionally, in the **Subscribed Organizations** column, add start and end dates for the subscription. Separate the start and end dates with a pipe (|) character. Use the date format of your current organization. For example: `Sub-Org1: 4/5/2021|8/8/2021, Sub-Org3: 5/5/2021|, Sub-Org4|7/7/2021`.
11. Save the .csv file.
12. In the BlackBerry AtHoc management system, click **Back** to return to the Users screen.
13. Click **More Actions** > **Import** > **Users**.
14. On the **Import User File** screen, click **Browse** and select the .csv file on your local system.
15. Click **Open**.
16. In the **Select the columns to import** section, select **Subscribed Organizations**.
17. Click **Import**.
18. Optionally, on the **Import Details** window, click **Download Log** to view the results.

The updated users can now be targeted in alerts and events from their subscribed organizations.

Assign permissions for a different organization

If you have users that need to have access to multiple organizations, you grant access using the same account for each organization. You can create the user once and grant that user operator permissions in another organization, as long as the other organization is in the same system. This gives operators access to multiple organizations without the need to have multiple accounts.

The following section describes the two primary situations in which you need to assign permissions for an operator to another organization.

Assign roles for a different enterprise

Use the External Operator Permissions settings page to give permissions to an operator who has permissions in another organization.

1. Log in to the BlackBerry AtHoc management system as an administrator and change to the organization you want to assign roles for.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **External Operator Permissions**.

   A list displays the operators who have operator permissions in an organization that you also have operator permission in.
4. Click **Add** to add existing operators from external organizations to the list. The Add Operator Permissions to External Operator window opens.
   a. Search for the operator in the **Search By Username** field and then select an operator. The user details page opens.

      The user account must be an operator in their home organization before they appear in this list. You must also be an administrator in the home organization of the user.
   b. Select the roles that you want the operator to have from the **Operator Roles** list. A full list of BlackBerry AtHoc roles is provided, including all administrator roles. If the user should be an administrator, use the following guidelines:
      - In System Setup, select the System Administrator role. With this role, the operator has administration privileges for settings privileges (no user management or alerting privileges) for all organizations in the system.
      - In an enterprise organization, select the Enterprise Administrator role. With this role, the operator has administration privileges for the enterprise organization and all suborganizations.
      - In a suborganization, select the Organization Administrator role. With this role, the operator has administration privileges for the local suborganization.
      - In a Basic organization, select the Basic Administrator role. With this role, the operator has administration privileges for the local organization.
   c. Select the distribution lists the administrator can work with.
      - Publish: When selected for a distribution list name, the administrator can publish alerts to the members of the list.
      - Manage: When selected for a distribution list name, the administrator can view and manage the list.
5. Click **Save**.

Note: To change the roles for an existing administrator, click the user name and modify the details pages as described in Step 4.

Assign roles for the enterprise from a member organization

If you have an enterprise installation, certain operators in member organizations need access to the enterprise level. This enables the operator to send alerts from the enterprise or manage the enterprise. For more information, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

If a user in a member organization needs access to the enterprise organization, you can edit their operator permissions at the enterprise level.

1. Log in to the BlackBerry AtHoc management system as an Enterprise Administrator and change to the enterprise organization.
2. In the navigation bar, click **Users** > **Users**.
3. On the **Users** screen, click the operator whose permissions you want to edit.
4. On the user details screen, click **Grant Operator Permissions**.
5. Click the **Operator Roles** list and then select the roles you want to assign to the user.

   Granting the Enterprise Administrator role will give this user full administrator permissions to all member organizations.
6. To remove an operator permission, click **X** beside the name.
7. Click **Save**.

View operator roles in multiple organizations

If an operator has roles and permissions in multiple organizations, you can view the operator's roles in the organization you are currently logged in to from the Permissions section of the operator's profile page. You can also view the operator's roles in other organizations from the user manager page and from the operator's profile page.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** page, do one of the following:
   - In the **Roles** column, click **Roles in {x} other organizations**.
   - Click the row for the operator you want to view. In the user profile page, in the **Permissions** section, click **This user has roles in {x} other organizations**.

The **Roles in other organizations** window opens and displays the roles the operator has in each additional organization.

Manage access to alert folders

The Alert Folders Manager centralizes alert folder configuration and management tasks. You can grant access to alert folders to operators in other organizations. You can only grant access to alert folders that you have access to.

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **External Operator Permissions**.
3. On the **External Operator Permissions** screen, click the name of the operator you want to give access to alert folders to. You can search by username to narrow the list of operators.
4. On the operator details screen, in the **Operator Roles** section, select a role that has alert publishing permissions from the **Operator Roles** list.
5. Optionally, in the **Alert Folders** section, select the **Publish/Manage Unrestricted** option to grant access to all alert folders in the organization.
6. Optionally, in the **Alert Folders** section, select the **Publish/Manage Restricted** option to grant access to specific alert folders in the organization. The folders list appears. Select the folders you want to give the operator access to.
7. Click **Save**.

After you finish: You can also manage access to alert folders using the Import Operators feature. For more information, see Importing and exporting operators.

BlackBerry AtHoc roles

Enterprise Administrators, Organization Administrators, and System Administrators can grant operator permissions to any user who needs access to the BlackBerry AtHoc management system. Granting operator permissions includes selecting which roles the user has when they are logged in, as well as setting any restrictions. Roles are additive: you can assign multiple roles and they build on one another, such as End Users Manager and Advanced Alert Publisher.

Administrators cannot assign or revoke higher level operator permissions than their own permissions. For example, an Organization Administrator can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

The role that a user is assigned to determines what BlackBerry AtHoc features they can access. Roles that are associated with specific features in BlackBerry AtHoc can only be assigned to users when that feature is enabled for that user's organization. The features in the following table are restricted to specific roles.

Feature	Roles
Account	• Accountability Manager • Accountability Officer
Activity Log	• Activity Log Manager • Activity Log Viewer
Connect **Note:** Connect is enabled and the Connect Agreement Manager role becomes available when organizations are connected.	• Connect Agreement Manager
Situation Response	• Plan Manager • Plan Incident Manager
Collaborate	• Collaboration Manager

The following sections describe the roles that are available in BlackBerry AtHoc.

For more information, see the *BlackBerry AtHoc Roles and Permissions Matrix*.

Accountability Manager

Account

- View, create, duplicate, search for, and delete accountability templates
- Create, delete, search for, and end accountability events
- Change the end time for accountability events
- Use the live map
- View accountability event dashboards
- Export accountability event reports
- Report status on behalf of others

Publisher map

- Export users list

Basic settings

- Manage accountability template settings

Accountability Officer

Account

- Search for accountability events
- Use the live map
- View accountability event dashboards
- Export accountability event reports
- Report status on behalf of others

Activity Log Manager

Alerts

- View, search, and export the activity log
- Create, modify, and edit the activity log

Activity Log Viewer

Alerts

- View, search, and export the activity log

Alert Manager

Give the Alert Manager role to an operator who needs to manage alerts and users, but should not have access to all settings. The Alert Manager role provides the maximum publishing privileges.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen

- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Manage distribution lists
- Mange user attributes
- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Reports

- View personnel, alerts usage, and user summary reports

Basic settings

- Configure alert template settings
- Configure alert folder settings

System setup settings

- Access the operator audit trail

User settings

- Configure user attribute settings
- Translate custom user attributes

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Advanced Alert Manager

Give the Advanced Alert Manager role to operators who need to manage alerts and users, but should not have access to all settings. The Advanced Alert Manager role provides the maximum publishing privileges as well as access to alert rules, delivery templates, audio files, placeholders, and user settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Manage alert rules
- Create and edit alert placeholders

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Manage distribution lists
- Mange user attributes

- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Reports

- View personnel, alerts usage, and user summary reports

Basic settings

- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rules

System setup settings

- Access the operator audit trail
- View geocoding summary and logs

User settings

- Configure user attribute settings
- Translate custom user attributes

Map settings

- Manage map settings
- Set default map view

- Add shape layer
- Add distribution list

Alert Publisher

Give the Alert Publisher role to operators who need to create and publish alerts but should not have access to all settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export the users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Advanced Alert Publisher

Give the Advanced Alert Publisher role to operators who need to create and publish alerts and configure alert settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export the users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Basic settings

- Configure alert template settings
- Configure alert folder settings

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings

Basic Administrator

The Basic Administrator role is available only in the BlackBerry AtHoc Basic edition.

Alerts

- Create and publish alerts
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates

Users

- Manage users
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Organizations

- View Connected organizations
- Connect with organizations
- View all AtHoc Connect organizations
- View sent invitations
- Access the Connect profile
- Configure AtHoc Connect profile

Basic settings

- Configure alert placeholder settings

- Configure delivery template settings
- Configure audio file settings
- Configure alert rule settings

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Basic Operator

The Basic Operator role is available only in the BlackBerry AtHoc Basic edition.

Alerts

- Create and publish alerts
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts
- Create, edit, import, export, search for, delete, and duplicate alert templates

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- Publish a quick alert

Basic settings

- Configure accountability template settings

Collaboration Manager

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Connect Agreement Manager

Give the Connect Agreement Manager role to the people in your organization who need to manage AtHoc Connect.

Alerts

- View, search for, and mark alerts as reviewed from the Inbox

Organizations

- View Connected organizations
- Connect with organizations
- View all Connect organizations
- View sent invitations
- Access the Connect profile

AtHoc Connect settings

- Configure Connect profile settings

Distribution Lists Manager

Users

- Manage distribution lists

Reports

- View Personnel reports

Draft Alert Creator

Give the Draft Alert Creator role to operators who should write but not send alerts.

Alerts

- Create and publish alerts
- Create and save a draft alert
- Create, edit, duplicate, end, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

End Users Manager

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Prioritize personal devices

Publisher map

- Export users list

Reports

- Access personnel reports

System Setup Settings

- View geocoding summary and logs

Enterprise Administrator

The Enterprise Administrator role is used by customers who have multiple organizations to manage as part of the enterprise. Enterprise Administrator is the most powerful role in the enterprise and should be reserved for users who need to have access to everything in it. See the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide for more information about enterprise alerting.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Search for, view, and export alerts from suborganizations from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Reset system alert template to default values
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates

- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Move and subscribe users from their suborganization to other suborganizations
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists
- Manage user attributes
- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Account

- View, create, search for, duplicate, and delete accountability templates
- Create, search for, delete, and end accountability events
- Change the end time for accountability events
- Use the live map
- View accountability event dashboards
- Export accountability event reports

- Report status on behalf of others

Reports

- View personnel, alerts usage, and user summary reports

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View all Connect organizations
- View sent invitations
- Access the Connect profile

Plan

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Plan Incidents

- Create an incident
- Edit an incident
- End an incident
- Publish an incident
- Export an incident
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Basic settings

- Configure general settings
- Configure dependent profile page layout
- Configure organization subscription
- Configure alert placeholder settings

- Configure accountability template settings
- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings
- Configure map settings
- Configure external events settings

AtHoc Connect settings

- Configure AtHoc Connect profile settings

System setup settings

- Configure security policy settings
- Configure system health settings
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail
- View geocoding summary and logs

User settings

- Grant external operator permissions
- Disable and delete end users
- Configure distribution list folders

  Note: The Enterprise Administrator can access distribution list folder settings from a standalone enterprise organization with no suborganizations.
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication
- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings
- Configure mass device endpoints
- Configure desktop app settings
- Configure mobile app settings

Device Manager

- Access the device manager
- View device details
- Enable and disable devices
- Set device delivery preference

Organization Administrator

The Organization Administrator role provides the maximum privileges in a single organization.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Reset system alert template to default values
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Move and subscribe users from their suborganization to other suborganizations
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists
- Manage user attributes
- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Account

- Use the live map

Reports

- View personnel, alerts usage, and user summary reports

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View sent invitations
- Access the Connect profile

Plan

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Plan Incidents

- Create an incident

- Edit an incident
- End an incident
- Publish an incident
- Export an incident
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Basic settings

- Configure general settings
- Configure dependent profile page layout
- Configure alert placeholder settings
- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings
- Configure map settings
- Configure external events settings

AtHoc Connect settings

- Configure AtHoc Connect profile settings

System setup settings

- Configure security policy settings
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail
- View geocoding summary and logs

User settings

- Grant external operator permissions
- Disable and delete end users
- Configure distribution list folders
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication

- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings
- Configure mass device endpoints
- Configure desktop app settings
- Configure mobile app settings

Device Manager

- Access the device manager
- View device details
- Enable and disable devices
- Set device delivery preference

Plan Incident Manager

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Plan

- View Plans in read-only mode

Incidents

- Create an incident
- Edit a draft incident
- End an incident
- Publish an incident
- View activity
- Export activity log
- Add new entry in activity log
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Plan Manager

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Plan

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Incidents

- Create an incident
- Edit a draft incident
- End an incident
- Publish an incident
- View activity
- Export the activity log
- Add new entry to activity log
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Report Manager

Alerts

- Search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

Reports

- View Personnel reports

SDK User

The SDK User role is used by external applications to perform tasks such as sending alerts and creating users.

- This is the primary role needed to access all V1 APIs.
- This role performs all actions supported by the BlackBerry AtHoc SDK.

In the BlackBerry AtHoc management system, an SDK User can also perform the following actions:

Device settings

- Configure SDK settings
- Configure web API login settings

System Administrator

Designed for the people responsible for maintaining the entire system of servers, who are often IT staff. This role hides user information by default, but can increase its own roles if needed to accomplish more tasks. This role can only be given in the System Setup (3) organization.

Alerts

- Search for, view, and export alerts from suborganizations from the Sent Alerts screen
- Reset system alert template to default values

Users

- Grant operator permissions
- Revoke operator permissions

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Basic settings

- Configure general settings
- Update the organization code in General Settings
- Enable dependents
- Configure dependent profile page layout
- Enable organization subscription
- Configure alert placeholder settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings

- Configure map settings
- Configure external events settings

System setup settings

- Configure security policy settings
- Configure global system health settings
- Configure system settings
- Configure system health settings
- Access and export the diagnostic log
- Clear the diagnostic log
- Access archive settings
- Access the organizations manager settings
- Configure feature enablement
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail
- View geocoding summary and logs
- Enable the SMS Opt-in service URL

User settings

- Grant external operator permissions
- Revoke operator permissions
- Configure distribution list folders
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication
- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

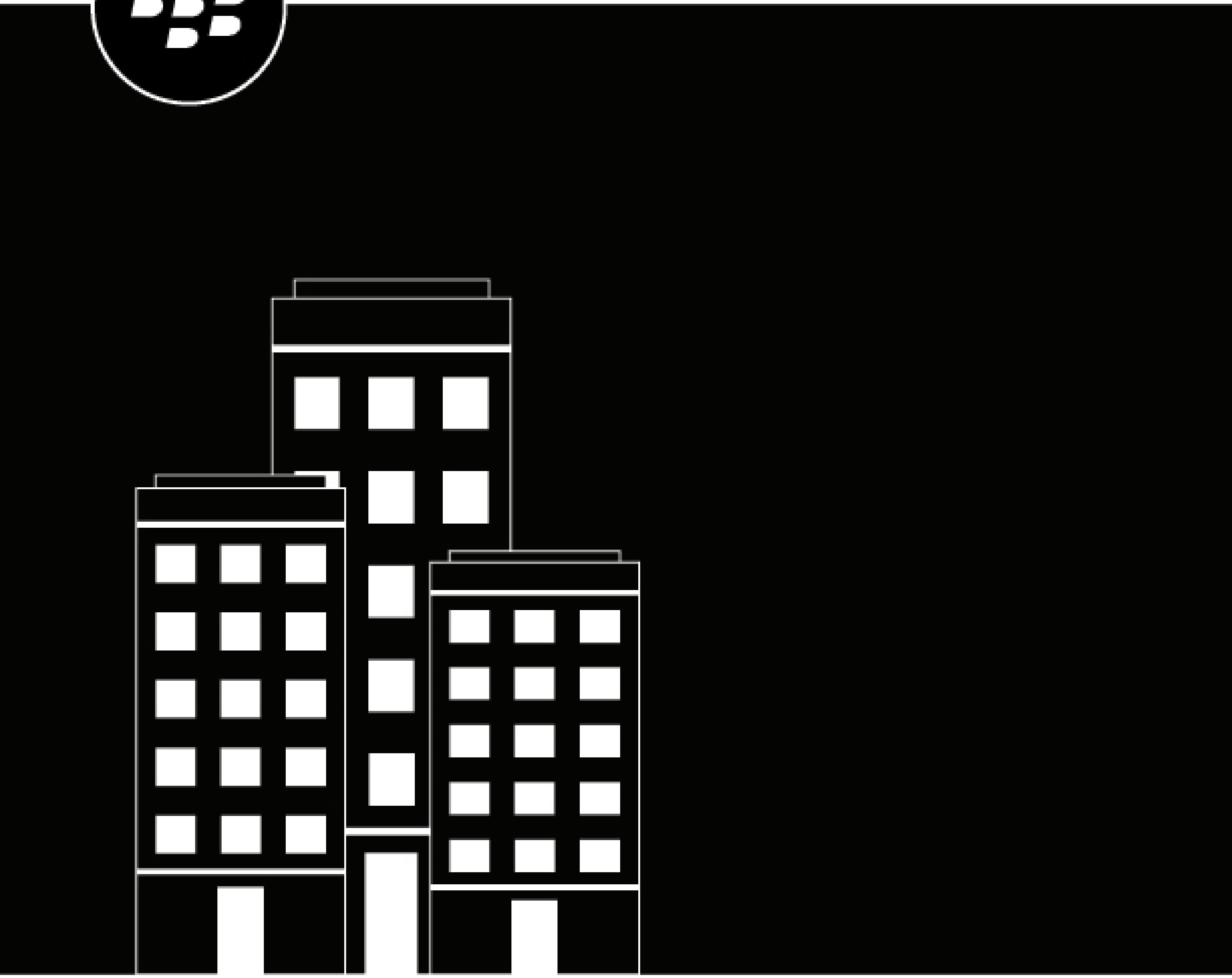
Device settings

- Configure device settings
- Configure mass device endpoints
- Configure desktop app settings

Device Manager

- Access the device manager
- View device details
- Enable and disable devices

- Edit devices
- Copy devices
- Delete devices
- Set device delivery preference
- Update device name



BlackBerry AtHoc

Install and Configure BlackBerry AtHoc

7.16

Contents

Getting started

BlackBerry® AtHoc® critical event management is a solution that turns an existing IP network into a comprehensive emergency mass notification system. It is an easily customizable system, which is why military, government, and commercial organizations use BlackBerry AtHoc to provide physical security, force protection, and personnel accountability for their workforce.

BlackBerry AtHoc customers are able to effectively leverage notifications to ensure that critical information reaches the right audiences in a timely manner.

This guide describes the configuration options for the BlackBerry AtHoc product, specifies the installation requirements, and details the installation process.

How to use this guide

Read the overview of BlackBerry AtHoc components and configuration in Main modules, BlackBerry AtHoc physical configuration, and Support for products, processes, procedures, and protocols.

- To upgrade an existing installation, follow the instructions in Upgrade BlackBerry AtHoc and Postinstallation or upgrade configuration.

For more information about advanced topics, including migrating a pre-installed server, configuring IIS processor affinity, increasing the maximum file upload size, and other topics, see Advanced server configuration.

System overview

The BlackBerry AtHoc critical event management solution is a flexible, commercial software solution for enterprise-class, subscription-based mass communication. The BlackBerry AtHoc system consists of the following basic elements that are illustrated in Figure 1, BlackBerry AtHoc System Elements.

- AtHoc server
- Operators (administrators and publishers)
- AtHoc desktop app

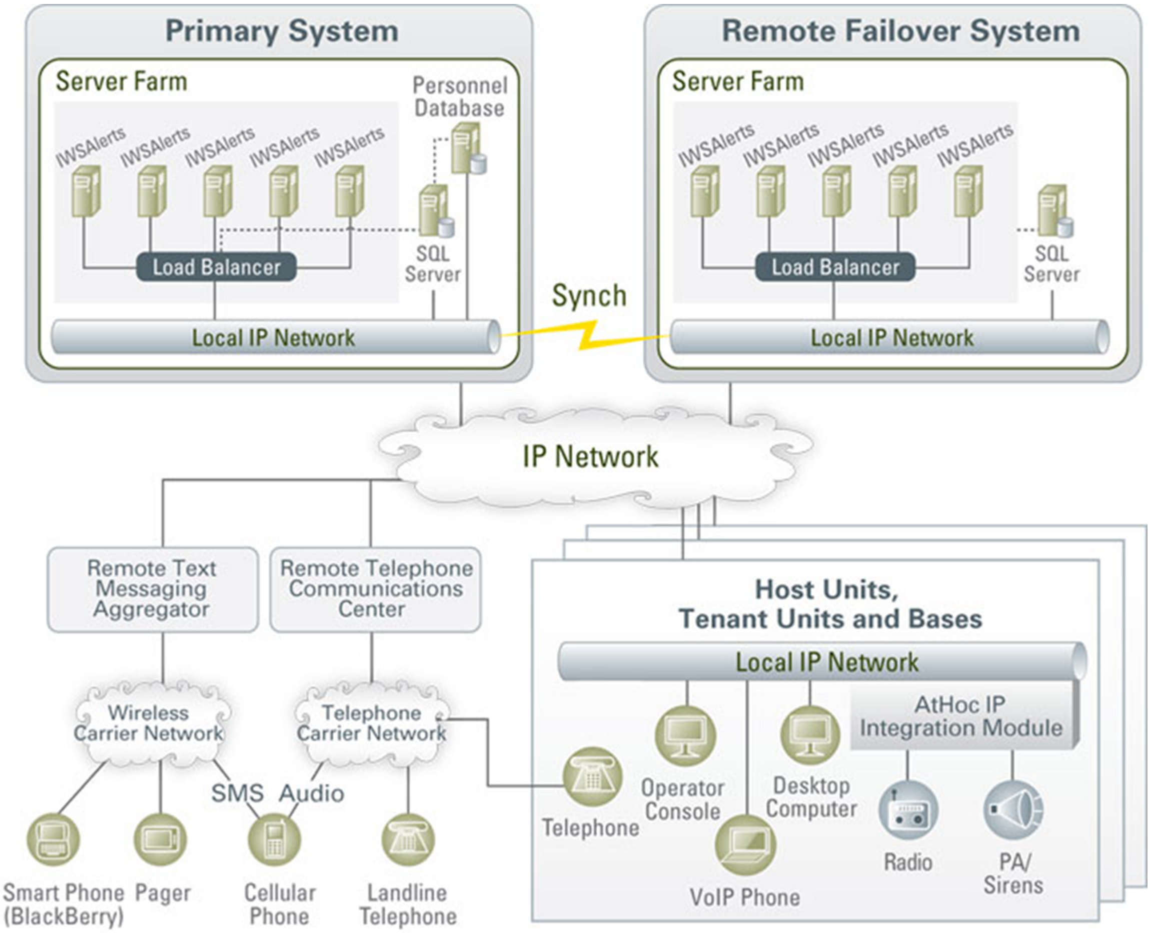


Figure 1: BlackBerry AtHoc system elements

AtHoc server

The AtHoc server does the following:

- Provides central application functionality, a web-based user interface for user subscription, delivery preferences, and system administration.
- Enables message routing to targeted users through its delivery engine depending on user-delivery settings and preferences. The Store-and-Forward capability saves alerts for desktop delivery when a user is offline and delivers them once a user's presence is detected, provided the alert is still alive.
- Schedules recurring alerts for the purposes of performing tests or issuing repeated reminder messages.
- Enables target alerts across multiple systems through cross-systems setup. Alert cascading is also available.
- Provides response tracking, reporting, and archiving features. Extensive audit reports detail operator actions within the system and can help pinpoint the sources of security violations. Real-time aggregated alert delivery and response summary reports are available in a graphical view (bar, graph, or pie charts.)
- Stores alerts history for each user automatically.
- Includes APIs and integration modules to alert delivery and dissemination systems such as Telephony Alerting Systems (TAS), SMS aggregators, and wide area speaker array (Giant Voice) systems.
- Integrates with external user directories such as LDAP or Active Directory for user synchronization and import, and end-user authentication.
- Enables windows authentication for BlackBerry AtHoc by adding a new Logon in SQL Server for the domain account and makes the new Logon the owner of all AtHoc databases.

- Provides APIs for integration with external systems and an Agent Platform that enables monitoring of external information sources and generating alerts according to subscription rules.

Operators (administrators and publishers)

Operators serve the following functions in BlackBerry AtHoc:

- Operators are users who can manage the BlackBerry AtHoc system, initiate alerts to be disseminated, and track and report alert publishing information.
- Operators can have multiple roles depending on their assigned tasks and responsibilities. For example, they can be publishers or administrators.
- Operators use a rich web-based interface to perform management and administration activities as defined by their permissions.

AtHoc desktop app

The AtHoc Desktop App appears as a small purple globe in the end user’s system tray. The AtHoc desktop app serves the following functions in the BlackBerry AtHoc system:

- When new alert content is published, the AtHoc desktop app displays an audio/visual notification as a desktop pop-up.
- Users can dismiss the desktop pop-up, choose a response option (when sent), and click a link to obtain additional information about the emergency condition.
- Additional delivery devices include: web delivery, email, mobile devices, phones, pagers, TTY/TDD devices, SMS, Giant voice, LMR, and instant messaging.
- The BlackBerry AtHoc desktop app can be installed on a Windows or macOS client.

Note: The available BlackBerry AtHoc features and functionality depend on the licensed BlackBerry AtHoc edition. If you have questions, contact your BlackBerry AtHoc account manager.

System components and configuration

Main modules

The BlackBerry AtHoc platform is composed of two types of server components:

- **Database server**: The database server is based on Microsoft SQL Server.
- **Application server (one or more servers)**: The application server acts as a web-based application server that provides all user-related interactions. The application server also runs the BlackBerry AtHoc services, which are responsible for scheduling events, providing notification delivery, and running background batch processes used for integration with external applications and content sources.

The database and application servers interact with the BlackBerry AtHoc desktop app, web browsers, and various delivery gateways such as telephony and SMS. Additionally, the servers provide integration points with enterprise application suites, such as LDAP, Active Directory, HR, and your organization's portals.

In cases where redundancy is needed, a BlackBerry AtHoc disaster recovery solution can be implemented so that notification capabilities can be transferred to an alternate site if the primary BlackBerry AtHoc platform becomes unreachable.

BlackBerry AtHoc physical configuration

Although all server components can be installed on the same server, you should install each server on different servers. The database server should be located on one server, and each application server installed on another server.

Database server

The database server can be installed in a clustered database configuration, providing hot failover between the database servers.

Application servers

It is easy and safe to add and remove machines to and from the web farm without affecting the end-user experience.

The web farm provides HTTP/HTTPS service to the web browsers and the AtHoc desktop app.

IWS Services is a website that runs web applications under IIS. The services schedule jobs (such as processing alerts and importing users), poll PSS, and track and report alert responses. Each application runs in its own application pool and the load can be configured on each application server, based on the anticipated load.

You can set up a disaster recovery site in an active-passive configuration to support continuous operation in cases of a primary site failure.

Application servers and common system resources

The application servers use common system resources that include the following:

- **Database server**: Application servers must be able to connect to the database server. The connection string is stored in the registry of each application server.
- **Microsoft Message Queuing (MSMQ)**: BlackBerry AtHoc uses MSMQ to queue jobs and events. MSMQ is configured on each application server.

The following graphic illustrates the BlackBerry AtHoc physical configuration in a typical redundant setup for a single site.

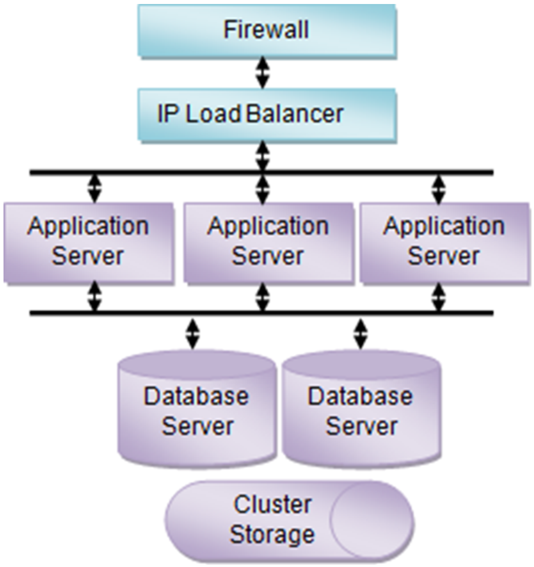


Figure 2: BlackBerry AtHoc physical configuration in a redundant setup (single site)

Support for products, processes, procedures, and protocols

The following third-party components are used to support the BlackBerry AtHoc implementation:

- Backups
- System maintenance and operation monitoring
- Connectivity
- Delivery gateways

Backups

Backups refer to the following:

- Database backup products and processes
- Application server backup products and processes

System maintenance and operation monitoring

System operation monitoring systems include examples such as OpenView and Tivoli.

Connectivity

Connectivity refers to the following items:

- **Local connectivity**: Local connectivity provides the connection between the local computers that BlackBerry AtHoc is installed on. Specifically, it is connectivity between the application server (or servers) and the database machine (or machines.)
- **Serving HTTP or HTTPS**: The application servers provide HTTP or HTTPS service to web browsers and the BlackBerry AtHoc desktop app. For HTTPS configuration, a Web PKI certificate must be installed on the web servers.

- **Accessing external HTTP or HTTPS sources**: External HTTP or HTTPS sources are used for integration with external applications and data sources used by the application server IWS Services. This connectivity can be configured through a proxy (an authenticating proxy is not supported). If an external telephony calling service is used, web connectivity from the application servers to the calling service must be established.
- **A firewall**: To protect the BlackBerry AtHoc platform.

IPv6 support

The BlackBerry AtHoc critical event management solution is compatible with IPv6 networks. Both servers and clients can operate in an IPv6-only infrastructure as well as in a hybrid IPv4/IPv6 environment.

Delivery gateway

- AtHoc Cloud Delivery Service East and AtHoc Cloud Delivery Service West are available out of the box and can deliver alerts through telephony, SMS, and email.
- OEM Cloud Delivery Service (East) and OEM Cloud Delivery Service (West) are available out of the box and can deliver alerts through email.

BlackBerry AtHoc account requirements

You can use a non-system account for the AtHoc application pool identities.

Required group policies

The following account policies and their values are the defaults on Windows Server before any changes are made due to Security Technical Implementation Guide (STIG) or Group Policy Object (GPO.) Any service account that is used to replace the AtHoc application pool identities or IIS_IUSRS must be a user or group member of the policies as shown in the following table.

Policy	Values
Adjust memory quotas for a process	AtHoc application pools
Create global objects	SERVICE
Generate security audits	AtHoc application pools
Impersonate a client after authentication	IIS_IUSRS SERVICE
Log on as a service	AtHoc application pools SERVICE
Replace a process level token	AtHoc application pools

Upgrade BlackBerry AtHoc

This chapter describes how to upgrade an existing installation of BlackBerry AtHoc.

Upgrade preparation

This section describes the steps that you need to complete before you upgrade to a new release.

Note: Before you perform an upgrade, make sure that BlackBerry AtHoc and any modules are fully functional. After the upgrade, verify that BlackBerry AtHoc and any modules are working.

Note: All live alerts and events are ended automatically during the upgrade.

Supported upgrade path

The supported upgrade path is 7.15 to 7.16.

Database server preparation

Complete the following preparation tasks to upgrade the database server.

All versions preparation steps

Required unless indicated.

Backup critical data

Backup databases, archive alerts, and clean up old alerts and diagnostic logs that are no longer needed.

Databases

- Stop any replication or failover activities with Double Take software, or with operating system-level replication.
- To avoid overwriting critical data, save the database backups on a different drive than the drive that the AtHocENS folder and the SQL Server files are located on.
- Name the backup files with the correct database names. Using the correct names helps you to recover the correct files during a failure. For example, name the backup file for the ngaddata database as `ngaddata_upgrade_7312013.bak`.

Alerts and user data

- To reduce upgrade time, reduce the size of the database and the Diagnostics log.
  - Purge old or unneeded alerts to decrease the database size. For example, if you need to save alerts for one year, purge alerts older than a year to reduce the database size. Use the System Archive Task in each organization to purge the alerts.
  - Purge the Diagnostic log by exporting or archiving the Diagnostic log data and then clear the log.

Application server preparation

The following sections describe actions that you need to take to prepare to upgrade the application servers.

The following pre-installed Windows components may need to be upgraded:

Component	Notes
.NET Framework v. 4.7.2	If an earlier version is installed, upgrade to version 4.7.2. If a later version is installed, uninstall it and then install version 4.7.2.
dotnet-hosting-3.1.27-win	This version is included in the asp .net hosting bundle which can be found in the AtHoc repo at: .../IWS/Server/7.16.0.0/Prereqs/dotnet-hosting-3.1.27-win.exe.
Windows PowerShell	Windows PowerShell 5.1 **Note:** Windows Server 2016 and 2019 include Windows PowerShell 5.1 by default.

Stop services

- Stop IIS: Set World Wide Web Publishing Service to Manual: netservice stop w3svc
- Stop web app workers: iisreset -stop

In a multiple application server environment, repeat the above step on each application server.

Back up custom code

Back up custom code if it exists.

Back up duplicated device configurations

If you duplicated any devices, save the XML files for the duplicated devices that are in the following directories to a temporary directory:

- `\AtHocENS\ServerObjects\utils\AddOnModules\Packages`
- `\AtHocENS\ServerObjects\utils\AddOnModules\IIM\Enable`

Important: After you complete the upgrade, copy the files back to these folders.

Database server upgrade

1. Run the setup kit on the database server to upgrade it.
2. Download the BlackBerry AtHoc setup kit .zip file to the server.
3. Right-click the setup kit .zip file and select **Properties** > **General** > **Unblock** to unblock the file.
4. Extract the contents of the setup kit .zip file into a temporary directory.

   Important: Due to Windows OS file path length limitations, some of the included utilities may not extract correctly. To avoid this issue, use a short path for the extraction directory. For example, C:\setup. Keep the total number of characters to 20 or less, including the drive letter, colon, and slashes.

5. Use the `<setupkit_root>/user.yml` configuration file to provide product-specific setup parameters.

   This file is included in the setup kit as a template with blocks of related parameters that are commented out and a brief description for each block. To use the parameters in a block, remove the # from the parameter, update it, and save the file.

   Note:

   YAML is indent-sensitive. When you remove the # from a parameter in the block, make sure that you keep the original indentation. You must also remove the # from the block header, even if you update only one parameter in the block. You can validate the YAML at https://yaml-online-parser.appspot.com/ before you save the file.

   You can also specify parameters in args block from the command line while you are running the main script. Command line parameters take priority.

```
include:
   - comp_db

# args:
#    sql_server_instance: '.'
#    sql_server_auth: 'sql'
#    sql_server_login: 'sa'
#    sql_server_passw: 'your_DB_sa_password_here'
#    ngad_passw: 'App_DB_user'
```

```
include:
   - comp_db

  args:
     sql_server_instance: '.'
     sql_server_auth: 'sql'
     sql_server_login: 'sa'
     sql_server_passw: 'your_DB_sa_password_here'
     ngad_passw: 'App_DB_user'
```

6. Execute the main script.

   a. Run Windows PowerShell as an administrator.
   b. Run the `<setupkit_root>/Setup.ps1` script to install the AtHoc database server.

      The following table describes the command line arguments allowed by the main script.

Parameter	Alias	Example	Purpose
SetupParamtersFile	paramsfile	'.\setupconfig.yml' 'C:\conf\setup.yml'	The path to user-provided setup parameters Default: '.\user.yml'
include		comp_db comp_web	Components to install
exclude		comp_db comp_web	Components to exclude from the installation
sql_server_auth	dblauth	'currentuser' 'sql'	Determines whether to use SQL or Windows authorization

Parameter	Alias	Example	Purpose
		'windows'	'sql': Use the SQL server sysadmin username and password 'currentuser': Use the current user login information "windows': User impersonation with specific Windows user login Default: 'currentuser'
sql_server_login	dbuser	'user123'	Database user (for SQL authentication)
sql_server_passw	dbpassw	'@THOC789'	Database password (for SQL authentication)
repoUser		username	User with read access to the artifactory
repoPassw		'p@55w0rd!'	Password for the artifactory user
artifactory_api_key	repoApiKey	'asdflk435145kfdasd0f...'	API key for artifactory REST API access

7. The main script starts the upgrade process and completes the following tasks:

    - Parses setup parameters.
    - Creates log directory and writes to log files.
    - Downloads necessary product components.
    - Installs each product in the following order: database, application, support modules.
    - Reports result and elapsed time.

    Note: You can run the main script in verbose mode to display and log debug information while the script runs. Use the `.\Setup.ps1 -verbose` command to run the script in verbose mode.

Application server upgrade

Note: If you update the application and database servers on separate servers, you must run the AtHoc setup kit once on each application server.

1. Download the BlackBerry AtHoc setup kit .zip file to the server.
2. Right-click the setup kit .zip file and select **Properties** > **General** > **Unblock** to unblock the file.
3. Extract the contents of the setup kit .zip file into a temporary directory.

Important: Due to Windows OS file path length limitations, some of the included utilities may not extract correctly. To avoid this issue, use a short path for the extraction directory. For example, C:\setup. Keep the total number of characters to 20 or less, including the drive letter, colon, and slashes.

4. Use the `<setupkit_root>/user.yml` configuration file to provide product-specific setup parameters.

   This file is included in the setup kit as a template with blocks of related parameters that are commented out and a brief description for each block. To use the parameters in a block, remove the # from the parameter, update it, and save the file.

   Note:

   YAML is indent-sensitive. When you remove the # from a parameter in the block, make sure that you keep the original indentation. You must also remove the # from the block header, even if you update only one parameter in the block. You can validate the YAML at https://yaml-online-parser.appspot.com/ before you save the file.

   You can also specify parameters in args block from the command line while you are running the main script. Command line parameters take priority.

   For the application server, you only need to specify the following:

   ```
   exclude:
       - comp_db
   ```

5. Execute the main script.

   a. Run Windows PowerShell as an administrator.

   b. Run the `<setupkit_root>/Setup.ps1` script to install the AtHoc database server.

      The following table describes the command line arguments allowed by the main script.

Parameter	Alias	Example	Purpose
SetupParamtersFile	paramsfile	'.\setupconfig.yml' 'C:\conf\setup.yml'	The path to user-provided setup parameters Default: '.\user.yml'
include		comp_db comp_web	Components to install
exclude		comp_db comp_web	Components to exclude from the installation
sql_server_auth	dblauth	'currentuser' 'sql' 'windows'	Determines whether to use SQL or Windows authorization 'sql': Use the SQL server sysadmin username and password 'currentuser': Use the current user login information windows': User impersonation with

Parameter	Alias	Example	Purpose
			specific Windows user login Default: 'currentuser'
sql_server_login	dbuser	'user123'	Database user (for SQL authentication)
sql_server_passw	dbpassw	'@THOC789'	Database password (for SQL authentication)
repoUser		username	User with read access to the artifactory
repoPassw		'p@55w0rd!'	Password for the artifactory user
artifactory_api_key	repoApiKey	'asdflk435145kfdasd0f...'	API key for artifactory REST API access

6. The main script starts the upgrade process and completes the following tasks:
   - Parses setup parameters.
   - Creates log directory and writes to log files.
   - Upgrades each product in the following order: database, application, support modules.
   - Reports result and elapsed time.

   When the upgrade is complete, BlackBerry AtHoc is upgraded and running.

   Note: You can run the main script in verbose mode to display and log debug information while the script runs. Use the `.\Setup.ps1 -verbose` command to run the script in verbose mode.

Postinstallation or upgrade configuration

This chapter describes component configurations that are performed after BlackBerry AtHoc is installed. There is no recommended order to the tasks described in this section.

Set antivirus file exclusions for database log and tempDB files

Real-time antivirus scanning at the file level can occasionally cause abnormal system behavior, like high CPU utilization.

You should exclude the following items from real-time scanning:

- The `ffmpeg.exe` file.
- The IIS Temporary Compressed Files folder located at: `%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files`.
- The SQL MDF database and the LDF log files.

Update certificate metadata for AuthServices

The appsettings configuration schema for AuthServices was changed in BlackBerry AtHoc release 7.11 to enable obtaining self-signed certificates from the Windows Certificate Store or invalid certificates from third-party vendors. Due to this change, the certificate metadata in the `appsettings.json` file must be modified after deployment.

Tip: You can still obtain the certificate from the Windows Certificate Store or from a disk. Set the ValidCertsOnly parameter to false to obtain self-signed and invalid certificates.

1. Obtain a valid certificate.
2. Import the valid certificate to the WINDOWS local store.
3. Open the certificate file and capture the Thumbprint and Passcode.
4. Open the `appsettings.json` file found at `AtHocENS\wwwroot\AuthServices\Auth \appsettings.json`.

   It is possible to add multiple certificate files, but you should add only one certificate file.
5. Update the `appsettings.json` file with one of the following:
   - To configure the certificate from a file system, use the following text:

```
             {"Logging": {
               "IncludeScopes": false,
               "LogLevel": {
                 "Default": "Error", // Trace, Debug, Information, Warning,
Error, Critical,
            None
                 "System": "Information",
                 "Microsoft": "Information"
               }
             },
             "Certificates": [
               {
                 "CertificateLocation": "FileSystem", // Location:
FileSystem,
            CertificateStore
```

```
                    "RelativeFilePath": ".\\wwwroot\\Certificates\
\TokenSigningCertificate.pfx",
                    "Passcode": "<passcode>"
                  },
                 ],
                 "AllowedHosts": "*"}
```

- To configure the certificate from the Windows Certificate Store, use the following text:

```
             {"Logging": {
               "IncludeScopes": false,
               "LogLevel": {
                 "Default": "Error", // Trace, Debug, Information, Warning,
Error, Critical,
            None
                 "System": "Information",
                 "Microsoft": "Information"
               }
             },
             "Certificates": [
               {
                  "CertificateLocation": "CertificateStore",
                  "StoreName": "Root", // My (Personal), Root (Trusted
Root), AddressBook,
             AuthRoot, CertificateAuthority, TrustedPeople,
TrustedPublisher, Disallowed
                   "StoreLocation": "LocalMachine", // CurrentUser,
LocalMachine
                   "Thumbprint": "<thumbprint>",
                   "Passcode": "<passcode>",
                   "ValidCertsOnly": true // for getting debug or
development certificates
                 }
               ],
               "AllowedHosts": "*"}
```

6. Update the values for Thumbprint and Passcode with the values you captured in Step 3.
7. Save and close the `appsettings.json` file.

IIS postinstallation checklist

After you install BlackBerry AtHoc, verify the following settings in IIS.

Note: In multiple application server environments, you must manually restart IIS on each application server after all application servers and the database have been upgraded.

Application pool configuration tables

The installation configures application pools using the settings described in the following sections. The configurations of the application pools are described in the following tables:

- Table 1: Application pool configuration
- Table 2: Application Pool - Web application associations for the AtHoc website - Enterprise configuration
- Table 3: AtHoc services application pool configuration
- Table 4: Application pools - web application association for AtHoc services web site

Table 1: Application pool configuration

Table 1a: General, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
General					
.NET framework version	No Managed code	v4.0	v4.0	v4.0	v4.0
Enable 32-bit applications	True	True	True	False	True
Managed pipeline mode	Integrated	Classic	Classic	Integrated	Clasic
Queue length	65535	1000	65535	65535	65535
Start automatically	AlwaysRunning	AlwaysRunning	AlwaysRunning	AlwaysRunning	AlwaysRunning

Table 1a: General, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
General			
.NET framework version	v4.0	v4.0	v4.0
Enable 32-bit applications	True	True	True
Managed pipeline mode	Integrated	Classic	Classic
Queue length	65535	65535	1000
Start automatically	AlwaysRunning	AlwaysRunning	AlwaysRunning

Table 1a: General, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
General			
.NET framework version	v4.0	v4.0	v4.0

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
General			
Enable 32-bit applications	True	True	True
Managed pipeline mode	Integrated	Integrated	Integrated
Queue length	65535	1000	65535
Start automatically	AlwaysRunning	AlwaysRunning	AlwaysRunning

Table 1b: CPU, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
CPU					
Limit	0	0	0	0	0
Limit action	NoAction	NoAction	NoAction	NoAction	NoAction
Limit interval (minutes)	5	5	5	5	5
Processor affinity enabled	False	False	False	False	False
Processor affinity mask	4294967295	4294967295	4294967295	4294967295	4294967295

Table 1b: CPU, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
CPU			
Limit	0	0	0
Limit action	NoAction	NoAction	NoAction
Limit interval (minutes)	5	5	5
Processor affinity enabled	False	False	False

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
CPU			
Processor affinity mask	4294967295	4294967295	4294967295

Table 1b: CPU, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
CPU			
Limit	30	0	0
Limit action	Throttle	NoAction	NoAction
Limit interval (minutes)	5	5	5
Processor affinity enabled	False	False	False
Processor affinity mask	4294967295	4294967295	4294967295

Table 1c: Process model, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Process model					
Identity (ApplicationPoolIdentity)	—	—	—	—	—
Idle time-out (minutes)	0	0	0	0	0
Load user profile	True	True	True	True	True
Maximum worker processes	1	1	1	2	2
Ping enabled	True	True	True	True	True

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Process model					
Ping maximum response time (seconds)	90	90	90	90	90
Ping period (seconds)	30	30	30	30	30
Shutdown time limit (seconds)	90	90	90	90	90
Startup time limit (seconds)	90	90	90	90	90

Table 1c: Process model, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Process model			
Identity (ApplicationPoolIdentity)	—	—	—
Idle time-out (minutes)	0	0	0
Load user profile	True	True	True
Maximum worker processes	1	1	1
Ping enabled	True	True	True
Ping maximum response time (seconds)	90	90	90
Ping period (seconds)	30	30	30
Shutdown time limit (seconds)	90	90	90
Startup time limit (seconds)	90	90	90

able 1c: Process model, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Process model			
Identity (ApplicationPoolIdentity)	—	—	—
Idle time-out (minutes)	0	0	0
Load user profile	True	True	True
Maximum worker processes	2	1	1
Ping enabled	True	True	True
Ping maximum response time (seconds)	90	90	90
Ping period (seconds)	30	30	30
Shutdown time limit (seconds)	90	90	90
Startup time limit (seconds)	90	90	90

Table 1d: Process Orphaning, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Process orphaning					
Enabled	False	False	False	False	False
Executable	—	—	—	—	—
Executable parameters	—	—	—	—	—

Table 1d: Process orphaning, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Process orphaning			
Enabled	False	False	False
Executable	—	—	—
Executable parameters	—	—	—

Table 1d: Process orphaning, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Process orphaning			
Enabled	False	False	False
Executable	—	—	—
Executable parameters	—	—	—

Table 1e: Rapid-fail protection, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Rapid-fail protection					
"Service Unavailable" response type	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False	False	False
Failure Interval (minutes)	5	5	5	5	5
Max Failures	5	5	5	5	5
Shutdown Executable	—	—	—	—	—
Shutdown Executable Parameters	—	—	—	—	—

Table 1e, Rapid-fail protection, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Rapid-fail protection			
"Service Unavailable" response type	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False
Failure interval (minutes)	5	5	5
Max failures	5	5	5
Shutdown executable	—	—	—
Shutdown executable parameters	—	—	—

Table 1e, Rapid-fail protection, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Rapid-fail protection			
"Service Unavailable" response type	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False
Failure interval (minutes)	5	5	5
Max failures	5	5	5
Shutdown executable	—	—	—
Shutdown executable parameters	—	—	

Table 1f: Recycling, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Recycling					
Disable overlapped recycle	False	False	False	False	False
Disable recycling for configuration change	False	False	False	False	False

Table 1f: Recycling, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Recycling			
Disable overlapped recycle	False	False	False
Disable recycling for configuration change	False	False	False

Table 1f: Recycling, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Recycling			
Disable overlapped recycle	False	False	False
Disable recycling for configuration change	False	False	False

Table 1g: Generate recycle event log entry, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Generate recycle event log entry					
Application pool configuration changed	False	False	False	False	False
Isapi reported unhealthy	False	False	False	False	False
Manual recycle	False	False	False	False	False
Private memory limit exceeded	True	True	True	True	True
Regular time interval	True	True	True	True	True
Request limit exceeded	False	False	False	False	False
Specific time	False	False	False	False	False
Virtual memory limit exceeded	True	True	True	True	True
Private memory limit (KB)	1800000	1800000	1800000	1800000	1800000
Regular time interval (minutes)	0	0	0	0	0
Request limit	0	0	0	0	0

Table 1g: Generate Recycle Event Log Entry, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Generate recycle event log entry			
Application pool configuration changed	False	False	False

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Generate recycle event log entry			
Isapi reported unhealthy	False	False	False
Manual recycle	False	False	False
Private memory limit exceeded	True	True	True
Regular time interval	True	True	True
Request limit exceeded	False	False	False
Specific time	False	False	False
Virtual memory limit exceeded	True	True	True
Private memory limit (KB)	1800000	1800000	1800000
Regular time interval (minutes)	0	0	0
Request limit	0	0	0

Table 1g: Generate Recycle Event Log Entry, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Generate recycle event log entry			
Application pool configuration changed	False	False	False
Isapi reported unhealthy	False	False	False
Manual recycle	False	False	False
Private memory limit exceeded	True	True	True
Regular time interval	True	True	True
Request limit exceeded	False	False	False
Specific time	False	False	False

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Generate recycle event log entry			
Virtual memory limit exceeded	True	True	True
Private memory limit (KB)	1800000	1800000	1800000
Regular time interval (minutes)	0	0	0
Request limit	0	0	0

Table 1h: Specific times, part 1

	AtHoc auth services .NET core pool	AtHoc D911 pool	AtHoc default pool	AtHoc desktop integrated pool	AtHoc desktop pool
Specific times					
[0]	01:38:00	01:33:00	01:34:00	01:34:00	01:36:00
Virtual memory limit (KB)	0	0	0	0	0

Table 1h: Specific times, part 2

	AtHoc IWS pool	AtHoc management system pool	AtHoc SDK pool
Specific times			
[0]	01:36:00	01:33:00	01:35:00
Virtual Memory Limit (KB)	0	0	0

Table 1h: Specific times, part 3

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Specific times			
[0]	01:33:00	01:35:00	01:38:00

	AtHoc Self Service pool	AtHoc web API pool	AtHoc web API v2 .NET core pool
Specific times			
Virtual Memory Limit (KB)	0	0	0

Table 2: Application Pool - Web application associations for the AtHoc website - Enterprise configuration

Web application	Associated application pool
api\ v1	AtHoc WebAPI pool
api\ v2	AtHoc WebAPI v2 .NET core pool
ast	AtHoc default pool
athoc-cdn	AtHoc IWS pool
athoc-iws	AtHoc IWS pool
AuthServices\ Auth	AtHoc auth services .NET core pool
CascadeAlertAgent	AtHoc default pool
client	AtHoc management system pool
config	AtHoc desktop integrated pool
csi	AtHoc desktop integrated pool
D911Server	AtHoc D911 pool
Data	AtHoc default pool
DataExport	AtHoc default pool
EasyConnect	AtHoc default pool
EmailResponse	AtHoc self service
Graphics	AtHoc default pool
Monitor	AtHoc default pool
Redirector	AtHoc default pool
SelfService	AtHoc Self Service pool
sdk	AtHoc SDK pool

Web application	Associated application pool
sps	AtHoc desktop integrated pool
sso	AtHoc default pool
Syndication	AtHoc Syndication pool
TwitterConfig	AtHoc default pool
wis	AtHoc desktop pool

Table 3: AtHoc services application pool configuration

Table 3: AtHoc services application pool configuration, part 1

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool
General					
.NET framework version	v4.6.1	v4.6.1	v4.6.1	v4.6.1	v4.6.1
Enable 32-bit applications	True	True	True	True	True
Managed pipeline mode	Integrated	Integrated	Integrated	Integrated	Integrated
Queue length	1000	1000	1000	1000	1000
Start automatically	AlwaysRunning	AlwaysRunning	AlwaysRunning	AlwaysRunning	AlwaysRunning
CPU					
Limit	0	0	0	0	0
Limit action	NoAction	NoAction	NoAction	NoAction	NoAction
Limit interval (minutes)	5	5	5	5	5
Processor affinity enabled	False	False	False	False	False
Processor affinity mask	4294967295	4294967295	4294967295	4294967295	4294967295

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool
Process model					
Identity[1]	—	—	—	—	—
Idle time-out (minutes)	0	0	0	0	0
Load user profile	True	True	True	True	True
Maximum worker processes	1	1	1	1	1
Ping enabled	True	True	True	True	True
Ping maximum response time (seconds)	90	90	90	90	90
Ping period (seconds)	30	30	30	30	30
Shutdown time limit (seconds)	90	90	90	90	90
Startup time limit (seconds)	90	90	90	90	90
Process orphaning					
Enabled	False	False	False	False	False
Executable	—	—	—	—	—
Executable parameters	—	—	—	—	—
Rapid-fail protection					
"Service Unavailable" response type	HttpLevel	HttpLevel	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False	False	False
Failure interval (minutes)	5	5	5	5	5

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool
Max failures	5	5	5	5	5
Shutdown executable	—	—	—	—	—
Shutdown executable parameters	—	—	—	—	—
Recycling					
Disable overlapped recycle	True	True	True	True	True
Disable recycling for configuration change	False	False	False	False	False
Generate recycle event log entry					
Application pool configuration changed	False	False	False	False	False
Isapi reported unhealthy	False	False	False	False	False
Manual recycle	False	False	False	False	False
Private memory limit exceeded	True	True	True	True	True
Regular time interval	True	True	True	True	True
Request limit exceeded	False	False	False	False	False
Specific time	False	False	False	False	False
Virtual memory limit exceeded	True	True	True	True	True
Private memory limit (KB)	800000	800000	800000	800000	800000

	AtHoc alert coordinator pool	AtHoc delivery coordinator pool	AtHoc tracking processor pool	AtHoc regular scheduler pool	AtHoc advanced scheduler pool
Regular time interval (minutes)	0	0	0	0	0
Request limit	0	0	0	0	0
Specific times					
[0]	04:30:00	04:30:00	04:30:00	04:30:00	04:30:00
Virtual memory limit (KB)	0	0	0	0	0

[1] ApplicationPoolIdentity

Table 3: AtHoc services application pool configuration, part 2

	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination coordinator pool
General				
.NET framework version	v4.6.1	v4.6.1	v4.6.1	v4.6.1
Enable 32-bit applications	True	True	True	True
Managed pipeline mode	Integrated	Integrated	Integrated	Integrated
Queue length	1000	1000	1000	1000
Start automatically	AlwaysRunning	AlwaysRunning	AlwaysRunning	AlwaysRunning
CPU				
Limit	0	0	0	0
Limit action	NoAction	NoAction	NoAction	NoAction
Limit interval (minutes)	5	5	5	5
Processor affinity Enabled	False	False	False	False

	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination coordinator pool
Processor affinity mask	4294967295	4294967295	4294967295	4294967295
Process model				
Identity[1]	—	—	—	—
Idle time-out (minutes)	0	0	0	0
Load user profile	True	True	True	True
Maximum worker processes	1	1	1	1
Ping enabled	True	True	True	True
Ping maximum response time (seconds)	90	90	90	90
Ping period (seconds)	30	30	30	30
Shutdown time limit (seconds)	90	90	90	90
Startup time limit (seconds)	90	90	90	90
Process orphaning				
Enabled	False	False	False	False
Executable	—	—	—	—
Executable parameters	—	—	—	—
Rapid-fail protection				
"Service Unavailable" response type	HttpLevel	HttpLevel	HttpLevel	HttpLevel
Enabled	False	False	False	False

	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination coordinator pool
Failure interval (minutes)	5	5	5	5
Max failures	5	5	5	5
Shutdown executable	—	—	—	—
Shutdown executable Parameters	—	—	—	—
Recycling				
Disable overlapped recycle	True	True	True	True
Disable recycling for configuration change	False	False	False	False
Generate recycle event log entry				
Application pool configuration changed	False	False	False	False
Isapi reported unhealthy	False	False	False	False
Manual recycle	False	False	False	False
Private memory limit Exceeded	True	True	True	True
Regular time interval	True	True	True	True
Request limit exceeded	False	False	False	False
Specific time	False	False	False	False
Virtual memory limit exceeded	True	True	True	True
Private memory limit (KB)	800000	800000	800000	800000

	AtHoc PSS polling agent pool	AtHoc tracking summary coordinator pool	AtHoc batch coordinator pool	AtHoc user termination coordinator pool
Regular time interval (minutes)	0	0	0	0
Request limit	0	0	0	0
Specific times				
[0]	04:30:00	04:30:00	04:30:00	04:30:00
Virtual memory limit (KB)	0	0	0	0

Table 4: Application pools - web application association for AtHoc services web site

Web application	Associated application pool
Advanced scheduler	AtHoc advanced scheduler pool
Alert coordinator	AtHoc alert coordinator pool
Batch coordinator	AtHoc batch coordinator pool
Delivery coordinator	AtHoc delivery coordinator pool
PSS polling agent	AtHoc PSS polling agent pool
Regular scheduler	AtHoc regular scheduler pool
Tracking processor	AtHoc tracking processor pool
Tracking summary coordinator	AtHoc tracking summary coordinator pool

IIS handler mappings

The following handler mappings are required:

Handler name	Path	Description
asp.net	*	AtHoc Wildcard Script Map
ASPClassic	*.asp	Handler for classic ASP
AXD-ISAPI-4.0_32bit	*.axd	web site administration requests handler
cshtml-ISAPI-4.0_32bit	*.cshtml	Required by MVC

Handler name	Path	Description
HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit	*.rem	Web service handler
HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit	*.soap	Web service handler
MvcScriptMap	*.mvc	Required by MVC
OPTIONSVerbHandler	*	URL-less page handler
PageHandlerFactory-ISAPI-2.0	*.aspx	ASP.NET v.2 page handler
PageHandlerFactory-ISAPI-4.0_32bit	*.aspx	ASP.NET v.4 page handler
SecurityCertificate	*.cer	processes SSL certificates
SimpleHandlerFactory-ISAPI-2.0	*.ashx	Generic Web handler
SimpleHandlerFactory-ISAPI-4.0_32bit	*.ashx	Generic Web handler
svc-ISAPI-4.0_32bit	*.svc	Web service handler
TRACEVerbHandler	*	URL-less page handler
WebServiceHandlerFactory-ISAPI-2.0	*.asmx	Web service handler
WebServiceHandlerFactory-ISAPI-4.0_32bit	*.asmx	Web service handler
StaticFile	*	URL-less page handler

Verification checklist

Use the following check list to ensure that all of the following items exist and are configured as described.

√	Item	Description
	ISAPI and CGI extensions	IIS 7: ISAPI and CGI Restrictions should have Active Server Pages and ASP.NET v4.0 (32-bit) in the Allowed category.
	Default web site	Ensure the default web site points to the <AtHocENS \wwwroot> folder.

√	Item	Description
	Virtual directories	The AtHoc website must contain the following virtual directories: • Data: Points to `<AtHocENS>\CommonSiteData\AtHocData` • Graphics: Points to `<AtHocENS>\CommonSiteData\Graphics`
	Web applications	The AtHoc website must contain the following Web applications: • api • v1 • v2 • ast • athoc-cdn • athoc-iws • AuthServices • Auth • CascadeAlertAgent • client • config • csi • D911Server • Data • DataExport • EasyConnect • EmailResponse • errorpages • Graphics • gw • help • icons • images • include • monitor • redirector • sdk • selfservice • sps • sso • syndication • temp • twitterconfig • user • wis

√	Item	Description
	ASP.NET version	All Web applications must point to the ASP.Net 4.0 version.IIS 7: this is set in the Basic or Advanced settings of each Application Pool.
	Application pools	The following application pools are created during the application server installation and must be present: • DefaultAppPool • AtHoc Advanced Scheduler Pool • AtHoc Alert Coordinator Pool • AtHoc Auth Services .Net Core pool • AtHoc Batch Coordinator Pool • AtHoc D911 Pool • AtHoc Default Pool • AtHoc Delivery Coordinator Pool • AtHoc Desktop Integrated Pool • AtHoc Desktop Pool • AtHoc IWS Pool • AtHoc Management System Pool • AtHoc PSS Polling Agent Pool • AtHoc Regular Scheduler Pool • AtHoc SDK Pool • AtHoc Self Service Pool • AtHoc Syndication Pool • AtHoc Tracking Processor Pool • AtHoc Tracking Summary Coordinator Pool • AtHoc User Termination Coordinator Pool • AtHoc WebAPI Pool • AtHoc WebAPI v2 .Net Core Pool
	Integrated Weather Alerts	Verify that the internal routing from the application server to the domain name (https://api.weather.gov/alerts/active) is functioning correctly over HTTP.
	MIME types	Verify that the following MIME types exist: • .mp4, video/mp4 • .webm, video/webm • .woff, application/x-wor

√	Item	Description
	AtHoc services	• Advanced Scheduler • Alert Coordinator • Batch Coordinator • Delivery Coordinator • PSS Polling Agent • Regular Scheduler • Tracking Processor • Tracking Summary Coordinator • User Termination Coordinator
	Response headers	There are six response headers for Default Web Site: • Content-Security-Policy, Value: default-src https: data: 'unsafe-inline' 'unsafe-eval' • Strict-Transport-Security, Value: max-age=31536000; includeSubDomains; Preload • X-Content-Type-Options, Value: nosniff • X-Xss-Protection, Value: 1;mode=block • X-Frame-Options, Value: SAMEORIGIN • X-Powered-By, Value: AtHoc Inc.

(Optional) Enable the TLS 1.2 protocol

BlackBerry AtHoc is fully TLS 1.2 compliant. If needed, TLS 1.2 can be enabled for inbound and outbound network connections on both the application and database servers.

Application server changes

After TLS 1.2 is enabled and enforced for inbound and outbound network connections on all AtHoc application servers, complete the following tasks on each application server:

1. Copy the registry script `AtHoc_AppServer_Win2016_TLS1.2.reg` (for Windows Server 2016) or `AtHoc_AppServer_Win2019_TLS1.2.reg` (for Windows Server 2019 with cumulative updates) available under the PostUpgrade\TLS1.2 folder to a local folder on the application server and double click to run it. It is important that the correct registry script based on AtHoc application server OS version (Microsoft Server 2016 or 2019) is run, to make necessary registry entries only after enabling and enforcing TLS 1.2 on the application server.
2. Reboot the application server.

Database server changes

Microsoft SQL Server 2016 and 2019 (with cumulative upates) support TLS 1.2 out-of-the-box and no further update is needed. If you have Microsoft SQL Server 2014 installed, go to the following URL to install and update your software to support TLS 1.2:

https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

Verify the database connection encryption state. Run the following SQL as a system administrator to view the SQL connections state. The encrypt_option column should display TRUE for all records:

```
select encrypt_option, count(*) FROM sys.dm_exec_connections group by
 encrypt_option
go
SELECT * FROM sys.dm_exec_connections order by connect_time desc
go
```

(Optional) Configure the application server for Windows authentication

1. Add a new Logon SQL Server for the domain account and make the new logon the owner of all AtHoc databases.
2. Modify all AtHoc application pools and the IUSR logon account to use the new logon.
3. Modify the anonymous user identity to use the new logon.
4. Change the OleDbConnectionString. Change “User Id=ngad;Password=@THOC123;” to “Integrated Security=SSPI;”.

For more information, see Configure AtHoc database operations to use Windows authentication in the "Advanced Server configuration" section.

(Optional) Configure client certificates on the application server

These steps are required if client certificates are intended to be used with the BlackBerry AtHoc system.

Configure client certificates on each application server so that they can make secure outbound requests to the database server.

To install and configure the client certificate, complete the following steps.

Note: These steps assume that you already have a certificate with a private key.

1. Log in to the application server.
2. Copy the client certificate to the file system.
3. Open Microsoft Management Console (MMC).
    a. From the Start menu, find MMC.
    b. Right click and select **Run as administrator**. The console opens.
4. Add the certificate snap-in.
    a. Click **File** and click **Add/Remove Snap-in...**.
    b. Click **Certificates** and click **Add**.

       The Certificate snap-ins dialog opens.
    c. Select **Computer account** and click **Next**.
    d. Select **Local Computer**.
    e. Click **Finish** and click **OK**.
5. Import the client certificate.
    a. Copy the certificate file to the application server.
    b. Open MMC and navigate to **Certificates** > **Personal**.
    c. Right-click **Personal** and select **Import**.

d. Complete the import wizard.

   Note: Wizard notes

   - The certificate that you import must be have a private key and be of the file type .PFX or .P12.
   - Store the certificate in the Personal store.

6. Verify that the client certificate has a private key by opening the certificate. On the **General** tab, look for the following note after the **Valid from** field: You have a private key that corresponds to this certificate.
7. Repeat this process for each application server.

When you configure the AtHoc Services application pool accounts, ensure that the account has access to the client certificate.

When you configure IIS, ensure that the web service has access to the client certificate.

(Optional) Set the SSL client certificate

In installations that require SSL client certificates on the application servers, such as smart card support, IIS folders must be set to **Require** client certificates instead of accepting client certificates.

Note: Indications that this setting has not been made include: desktop pop-ups display one or more security prompts, the Weather Alerting Module is not functional, and integration with external systems that use the AtHoc SDK APIs do not work.

To set the preference for client certificates, complete the following steps:

1. Open the **Internet Information Services Manager**.
2. Expand **Sites**, then expand **Default Web Site** or the named site. Select a Web application and open SSL Settings.
3. Select the **Ignore**, **Accept**, or **Require** option under client certificates. Use the recommendations for each folder, provided in the table below.
4. Click **Apply**.

The following table provides a reference for client certificate settings for customers that use smart cards or soft certificates for client authentication to web servers.

Application or virtual directory	SSL client certificates
Aspnet_client	Require
api	Ignore
ast	Require
athoc-cdn	Require
athoc-iws	Require
AuthConfig	Ignore
CascadeAlertAgent	Require
client[1]	Require

Application or virtual directory	SSL client certificates
config[2]	Ignore if you have desktop clients deployed. Require if not.
csi[2]	Ignore if you have desktop clients deployed. Require if not.
D911Server	Require
Data	Require
DataExport	Require
Default Web Site	Require
EasyConnect	Require
EmailResponse	Require
Help	Require
Graphics[2]	Ignore if you have desktop clients deployed. Require if not.
Gw	Require
Icons	Require
Images	Require
Include	Require
Integrated Weather Alerts[3]	Require
monitor	Ignore if your web server monitoring solution will not work with client certificates. Require if it does.
Redirector	Require
sdk	Ignore if your custom code integration does not support client certificates. Require if it does.
SelfService	Require
Self Service/AuthWin	Require
sps[2]	Ignore if you have desktop clients deployed. Require if not.
Sso	Require

Application or virtual directory	SSL client certificates
Syndication	Require if your IIM devices have client certificates installed, or If no IIM devices are deployed. Ignore if not.
TwitterConfig	Require
User	Require
wis	Require

1. BlackBerry AtHoc health monitors do not currently support client certificate authentication. Setting the `client` Web directory to “Require Client Certificates” might cause the BlackBerry AtHoc management system health monitor to falsely show that the system is down. You should disable this monitor in this configuration.
2. If `config`, `csi`, `Graphics`, and `sps` are set to “Require Client Certificates” and you have desktop clients deployed, one of two things can happen:
   - Users experience periodic prompts for client certificate pin authentication.
   - The SSL stack on the IIS web server becomes overwhelmed with SSL renegotiation issues. This condition looks like your web server is under a denial of service attack, with page loads becoming slower and eventually timing out with errors.
3. Make sure the Symantec/Verisign certificate chain for the target system is properly represented in the Windows Certificate Manager.

(Optional) Install certificates for cloud delivery services

Certificates to access cloud delivery services such as TAS, email, and SMS are automatically installed as part of the BlackBerry AtHoc installation.

If you need to reinstall these certificates, complete the following steps for each BlackBerry AtHoc application server:

1. Go to the following URL: https://www.digicert.com/digicert-root-certificates.htm.
2. Locate and download the following certificate files to the application server and rename the extension to `.CER`:
   - DigiCert
   - DigiCert SHA2 Secure Server CA
3. Open the Windows **Start** menu and in the search field, type `mmc.exe`. The Microsoft Management Center (MMC) opens.
4. Click **File** > **Add/Remove Snap-in**.
5. Click **Certificates**, click **Add**. The Certificate snap-ins dialog opens.
6. Select **Computer account** and click **Next**.
7. Select **Local computer**.
8. Click **Finish** and click **OK**.
9. To import the certificate, copy the certificate file to the application server.
10. Open **MMC** and navigate to **Trusted Root Certificate Authorities** > **Certificates**.
11. Right-click **Certificates** and click **All Tasks** > **Import**. The Certificate Import Wizard opens.
12. Click **Next** and click **Browse**.
13. Navigate to where you saved the certificates.

14. Before the **File name** field, in the **File type** drop-down list, select **All Files (*.*)**.
15. Select a certificate and click **Open**.
16. Click **Next** twice, and click **Finish**.
17. Restart IIS.

(Optional) Configure new access card formats for operator auto-login

BlackBerry AtHoc supports several types of log in configurations. Operators can manually log in using a username and password, a personal identification verification (PIV) card, or a Common Access Card (CAC) card.

1. Gather information from the customer to determine what type of PIV or CAC card will be used by operators. If the card type is not supported, contact BlackBerry AtHoc customer support.
2. Configure BlackBerry AtHoc security settings.
3. Restart IIS.

Gather information from the customer

If the organization using an access card requires a format not supported by BlackBerry AtHoc, you must request support. Gather 5 to 10 samples of the customer client certificate strings and the variable name in the HTTP header from the organization that stores the certificate string. Provide BlackBerry AtHoc with the examples.

For example:

```
Subject: DC=edu, DC=athoc, O=internal, OU=people,
 OID.0.9.2342.19200300.100.1.1=jsmith@athoc.com, CN=Jane Smith <mapping
 identifier>
Subject: DC=edu, DC=athoc, O=internal, OU=people,
 OID.0.9.2342.19200300.100.1.1=jdoe@athoc.com, CN=John Doe <mapping identifier>
 (affiliate)
```

BlackBerry AtHoc creates a primary and an alternate regular expression (regex) that allows users to log in with their PIV or CAC cards. The expression extracts the MID from the certificate string. It then compares the MID with values in the database to determine the user identity and logs the user in automatically.

BlackBerry AtHoc provides an SQL UPDATE script that updates the GLB_CONFIG_TAB so that operators can log in with their access cards.

Update BlackBerry AtHoc management system security policy

To change the automatic login for the BlackBerry AtHoc management system, update the Security Policy settings.

Note: You must be in the system setup organization (3) to update this setting.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **System Setup** section, click **Security Policy**.
4. On the **Security Policy** window, in the **Smart Card Authentication** section, select the Smart Card Login **Enabled** option.
5. Save your changes.
6. Log out and attempt to log back in using a smart card.

(Optional) Update the application server registry for smart card login

For smart card login, update the registry on the application server to enable users to select a CAC certificate.

To add a value to the SCHANNEL registry key, complete the following steps:

1. From the Windows Start menu, type **regedit**.
2. Navigate to the following node: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`.
3. Right-click the **SCHANNEL** node and click **New**.
4. Click **DWORD (32-bit) Value**. The new value is created.
5. Enter the name of the new value: **ClientAuthTrustMode**.
6. You must enter the value when the name field becomes available for editing because you cannot change the name later.
7. Double-click on the new value and enter the following value in the field. Data: **2**.
8. Click **OK**.

(Optional) Enable FIPS on each application server

Federal Information Processing Standards (FIPS) requires an HTTPS environment.

1. Set the following key to **1**: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy`

   Note: If the key is set to 0, then FIPS is disabled.
2. Restart the server.

(Optional) System Archive account requirement

Note: This task is required only for new installations that use System Archive.

In order for the System Archive function to work, the AtHoc services application pool identities need a domain service account with **sysadmin** access on the SQL Server. A viable alternative is the built-in Local System account. However, additional configuration on SQL is required.

Add all application servers' *domain\computer$* account as a new login to SQL Server and grant it the sysadmin server role.

The backup folder path must also exist on the Microsoft SQL Server and the application pool identities must have write access to that folder. The backup folder path is defined in the System Setup (3) organization in System Settings.

If you use a client certificate for this server, ensure that the account has permission to access that client certificate. For more information, see (Optional) Configure client certificates on the application server.

1. As a sysadmin, log in to the database server instance.
2. Give sysadmin permissions to the following user: *domain*\"<*app-server-name*>$".
3. Map the DEFAULT DATABASE to "ngaddata".
4. As a sysadmin, log in to the **SQL Server Management Studio**.
5. Open **Object Explorer**.
6. Click *server_instance_name* > **Security** > **Logins**.
7. Right-click **Logins** and then select **New Login**.
8. On the folder defined in GLB_CONFIG_TAB for [key_name]"DB_ARCHIVE_LOCATION", give full permissions to the [NTAUTHORITY\SYTEM] login and sysadmin permissions to the database server instance.
9. On the application server, open the registry.
10. Edit the OleDbConnectionString value to add the following string at the end: **Trusted_Connection=True**.
11. As an administrator, at the command prompt, run the **IISRESET** command to restart IIS.

Configure .NET framework to use a web proxy

1. Open Notepad as administrator and open the following file:

   ```
   C:\Windows\Microsoft.NET\framework\v4.0.30319\config\machine.config
   ```

2. Search for `<system.net>`. If `<system.net>` is not found, add the following text as the second line from the end (</configuration>) and substitute the proxy address as appropriate for the environment:

   ```
   <system.net>
        <defaultProxy>
                <proxy autoDetect="false" bypassonlocal="true"
    proxyaddress="http://proxy_host:8080" />
        </defaultProxy>
   </system.net>
   ```

3. Save and close the file.
4. Open Notepad as an administrator and open the following file:

   ```
   C:\Windows\Microsoft.NET\framework\v4.0.30319\config\web.config
   ```

5. Search for `<system.net>`. If `<system.net>` is not found, add the following text as the second line from the end (</configuration>) and substitute the proxy address as appropriate for the environment:

   ```
   <system.net>
        <defaultProxy>
                <proxy autoDetect="false" bypassonlocal="true"
    proxyaddress="http://proxy_host:8080" />
        </defaultProxy>
   </system.net>
   ```

6. Save and close the file.
7. Open up a command prompt as an administrator and run the following command, substituting the proxy address as appropriate for the environment:

   ```
   C:\Windows\syswow64\netsh.exe winhttp set proxy http://proxy_host:8080 bypass-
   list="*.customernetwork.com"
   ```

   Note: The bypass-list argument is optional, but it can be used to allow BlackBerry AtHoc to poll itself (health monitors) without going through the proxy.

8. Execute the following command to verify the proxy setting:

   ```
   C:\Windows\syswow64\netsh.exe winhttp show proxy
   ```

9. Issue the following commands to restart the BlackBerry AtHoc application:

   ```
   iisreset /stop
   iisreset /start
   ```

(Optional) Restore the XML files for duplicated devices

If you backed up duplicated device XML files, restore the XML files to the following directories from the temporary directory:

```
\AtHocENS\ServerObjects\utils\AddOnModules\Packages
```

```
\AtHocENS\ServerObjects\utils\AddOnModules\IIM\Enable
```

(Optional) Set up error pages for Self Service throttling

Self Service is implemented as a separate application which runs in its own application pool. In a production environment, the Self Service application shares CPU resources with other applications like the operator management system. To ensure that alerting is not negatively affected by the Self Service application during heavy loads to the Self Service application, the AtHoc Self Service application pool that Self Service runs under will be throttled so that it uses only 30% of the available CPU at any time. This ensures that BlackBerry AtHoc alerts can always be published, even during heavy loads to Self Service. One impact of this change is that during heavy loads in Self Service, you might encounter some slowness in the Self Service application.

Starting with release 6.1.8.90, the throttling changes are applied automatically by the installer during new installation and upgrade.

External error pages for Self Service throttling

When the AtHoc Self Service application is throttled to use only 30% of CPU, it is likely that IIS will display errors with a status code of "503" or "500" when the system is under heavy load and unable to handle requests. If these errors occur, IIS displays a default error page that does not contain a lot of useful information for users.

These errors are usually not customizable at the IIS level on the same server, as documented by Microsoft. BlackBerry AtHoc provides friendly messages in static pages that can be used in place of the default error pages, provided that the BlackBerry AtHoc system is deployed behind a proxy server or load balancer that supports error message customization. You can configure these load balancers or proxy servers to trap these errors and redirect to the friendlier messages instead. The error pages are available on the application server at the following path: `AtHocENS\wwwroot\errorpages`.

You can take the **errorpages** folder and host it on any web server that is capable of serving HTML, CSS, and Javascript pages.

Note: The server where you host your error pages should be different than the AtHoc server where you are running the AtHoc applications.

To host the folder, administrators copy the folder and make it publicly available from their web server. For example, if you hosted these pages directly under the root folder of the web server, the error pages can then be accessed using the following URLs, where <domainnameofserver> refers to the actual domain name of the server:

Error page	Error page URL	Message
500 – Internal Server Error	https://<domainnameofserver>/errorpages/index.html?code=500	The server encountered an unexpected condition which prevented it from fulfilling the request. Try to access the page again. If this doesn't work, wait a few minutes, restart your browser, and then try again.

Error page	Error page URL	Message
503 – Service Unavailable	https://<domainnameofserver>/ errorpages/index.html?code=503	The server is unable to load the page you are requesting. This could be because increased traffic is overwhelming the server. Wait a few minutes and then try again.

After these pages are hosted on a different server than the AtHoc server, you can configure the individual proxy server or load balancers to redirect to the static hosted pages based on the error that IIS returns to the client.

Note: Because the configuration process varies depending on the type of load balancer or proxy server being used, the configuration process is not documented here.

Advanced server configuration

The following topics describe advanced server configuration tasks.

Migrate a preinstalled server

In some cases, BlackBerry AtHoc provides a customer with a preinstalled server. In other cases, there is a need to move an installed server to another domain.

Stop services

Stop IIS.

Application server changes

1. Uninstall and reinstall MSMQ.
2. Update the connection string in the registry of all application servers.
3. Update the `<Server=Server Name>` parameter in the following keys:

   ```
   HKEY_LOCAL_MACHINE\Software\AtHocServer\OleDbConnectionString
   ```

Start IIS

To perform management system changes, under the **Administration** > **Parameters** > **Configuration Options** tab, update Time Zone and Homepage URL.

Migrate to an enterprise hierarchy

After you upgrade to this release, you can migrate to a BlackBerry AtHoc enterprise. The enterprise provides system-wide alerting and content management for all organizations on your system.

During the upgrade, standard out-of-the-box attributes and alert folders are migrated to System Setup (3) from all other organizations and are now inherited by all other organizations from System Setup. Following the upgrade, run the Enterprise Migrator tool to organize the hierarchy structure and promote user attributes and alert folders.

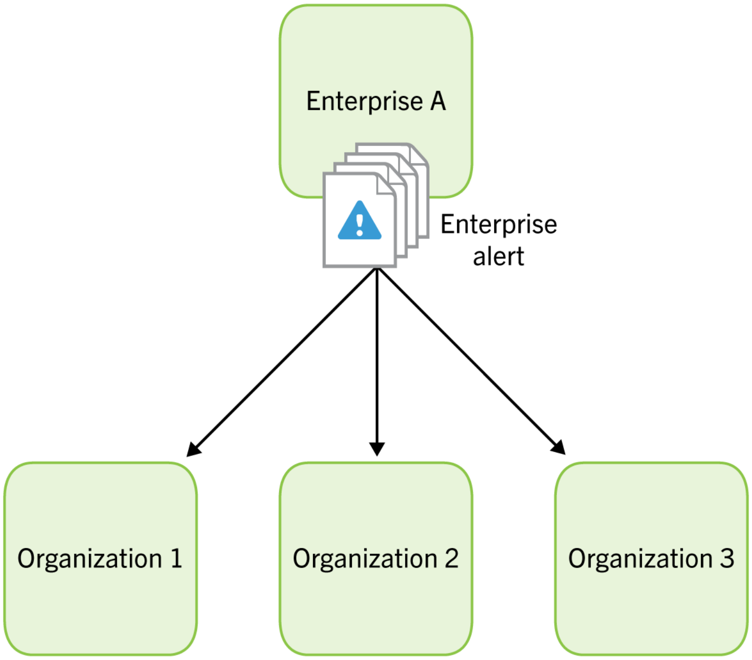
Plan the enterprise hierarchy

Important: Plan your hierarchy before you use the Enterprise Migrator tool. After you save your changes, you cannot change the hierarchy.

The Enterprise Migrator tool displays the organizations currently in your BlackBerry AtHoc system. By default, new organizations that are created in the system are listed under the System Setup node. These are standalone enterprise organizations. They can be used as either an enterprise organization or moved under an enterprise to become a suborganization.

In BlackBerry AtHoc enterprise organization, there are three levels:

- The top level is System Setup. The system administrator role manages the system by logging into the System Setup (3) organization. User attributes and alert folders can be created here, which all organizations in the system inherit.
- The next level is Enterprise. There can be multiple enterprise organizations associated with System Setup. The enterprise administrator manages the enterprise organization and suborganizations. The administrator can create enterprise-level attributes and folders for the enterprise organization that is inherited by its children.



- The third level is suborganization (or member organization). Each enterprise organization can have an unlimited number of suborganizations. The organization administrator manages the local organization only. The organization administrator can create organization-level attributes and folders for the local organization. A suborganization has peers, but no children.

Using the Enterprise Migrator tool, you will choose one organization that acts as the enterprise organization, and the rest that are members (suborganizations.) System Setup is the default and top-level organization. An enterprise organization inherits from System Setup and a suborganization inherits from the enterprise organization.

- Typically, content is managed at the enterprise level because it provides one place to control the content and send alerts to all users in suborganizations. The suborganization level contains content specific to a subset of the enterprise, customized for a particular organization.
- The Enterprise Migrator tool migrates existing operators that have an enterprise administrator role in a suborganization to organization administrator. Other operator permissions remain unchanged.
- When you move an organization into the enterprise, the Connect relationships and user accounts remain unchanged for the organization.

Important: Enterprise hierarchy uses inheritance for user attributes and alert folders. Content created at the system level can be seen by enterprise and suborganizations, but not edited. Content created at the suborganization level cannot be seen at the enterprise or system levels.

Best practices

- Rename user attributes with the name “Organization”. BlackBerry AtHoc provides an enterprise user attribute with this name.
- Plan the promotion of attributes and alert folders:
  - Use enterprise attributes and alert folders is to enforce consistency.
  - If more than one organization uses the same user attribute, the attribute should be promoted to the enterprise level.
  - If organizations use different values for the same user attribute, all values are promoted to the enterprise level.

    - Think about situations in which you need to alert the entire enterprise. What attributes do you need to target all users in an alert? These attributes should be promoted to the enterprise level.
    - Attributes that are for only one suborganizations should stay at the suborganization level.
- Create end users and operators for suborganizations at the suborganization level, not the enterprise level.
- You can see all users from suborganizations from the enterprise organization so there is no reason to create any users at this level aside from enterprise operators (operators that need to send alerts more than one suborganization.)
- Create a new enterprise organization rather than reuse a headquarters organization if there are existing users. Move the headquarters organization under the enterprise level.

Run the Enterprise Migrator tool

The Enterprise Migrator tool is provided with the installation package. You can use this tool to specify the relationship between parent and child organizations.

1. Log in to the BlackBerry AtHoc server and change to the following directory: `..\AtHocENS\ServerObjects\Tools`.
2. Locate the following executable file: `EAMigrator`.
3. Right-click the file and select **Run as Administrator**.

The Enterprise Migrator opens.

Migrate organizations to the enterprise

Run the Enterprise Migrator tool to create or modify an enterprise hierarchy, and to promote attributes and alert folders from suborganizations to the enterprise or system level.

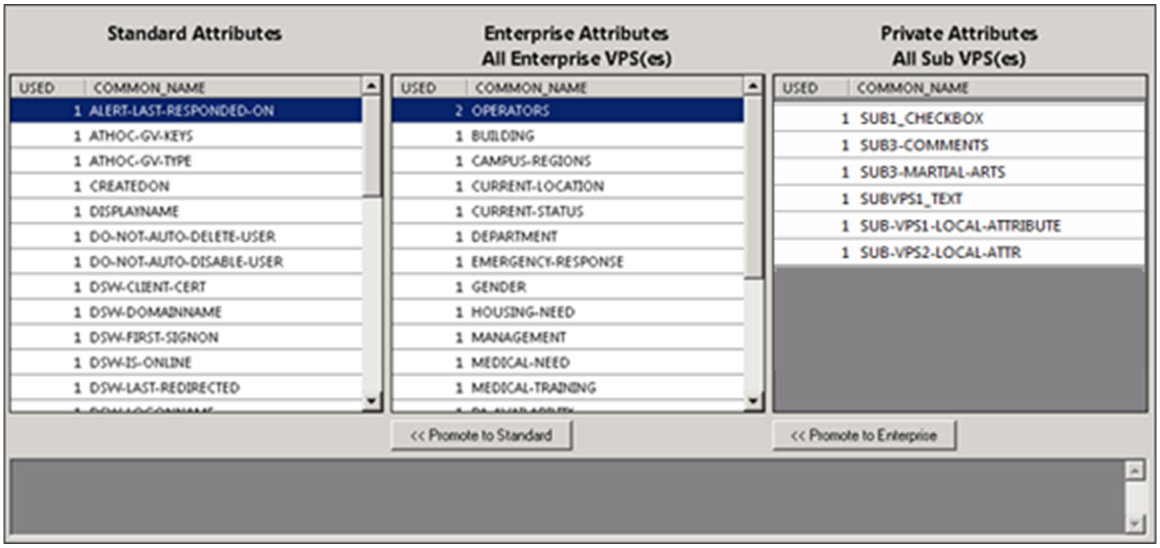
1. Plan your hierarchy before you use the tool. After you save your changes, you cannot change them.
2. The list of organizations shows all standalone organizations, except for basic organizations. If an organization is missing, it likely has an incorrect database type.
3. In the first column of the Enterprise Migrator, drag and drop any organization under another organization to specify the enterprise and suborganization levels.
4. Verify your structure before you save your changes. After your changes are saved, they cannot be undone.
5. Click **Save Structure**.

Promote user attributes and alert folders

During migration, you specify at which level the custom attributes and alert folders are defined: at the system, enterprise, or suborganization level. If only a small group of users in a suborganization needs access to an attribute, it should be handled locally. However, for most user attributes or alert folders, the system or enterprise level is the typical location.

To promote custom attributes, complete the following steps:

1. Open the Enterprise Migrator tool and click **User Attributes**.
2. Determine how many instances there are of an attribute at the suborganization and enterprise organization level and promote if it seems efficient. If you promote an attribute to the enterprise level, it is promoted from all the suborganizations within that enterprise.
3. Select the attribute name.
4. Verify that you want to promote the attribute. You cannot undo this step.



Standard Attributes

USED	COMMON_NAME
1	ALERT-LAST-RESPONDED-ON
1	ATHOC-GV-KEYS
1	ATHOC-GV-TYPE
1	CREATEDON
1	DISPLAYNAME
1	DO-NOT-AUTO-DELETE-USER
1	DO-NOT-AUTO-DISABLE-USER
1	DSW-CLIENT-CERT
1	DSW-DOMAINNAME
1	DSW-FIRST-SIGNON
1	DSW-IS-ONLINE
1	DSW-LAST-REDIRECTED

Enterprise Attributes
All Enterprise VPS(es)

USED	COMMON_NAME
2	OPERATORS
1	BUILDING
1	CAMPUS-REGIONS
1	CURRENT-LOCATION
1	CURRENT-STATUS
1	DEPARTMENT
1	EMERGENCY-RESPONSE
1	GENDER
1	HOUSING-NEED
1	MANAGEMENT
1	MEDICAL-NEED
1	MEDICAL-TRAINING

Private Attributes
All Sub VPS(es)

USED	COMMON_NAME
1	SUB1_CHECKBOX
1	SUB3-COMMENTS
1	SUB3-MARTIAL-ARTS
1	SUBVPS1_TEXT
1	SUB-VPS1-LOCAL-ATTRIBUTE
1	SUB-VPS2-LOCAL-ATTR

5. Click **Promote to Enterprise** or **Promote to System** to move them up to a higher level.

   Promote an attribute from suborganization to Enterprise if the entire enterprise needs to use the attribute. Keep the attribute in a suborganization if you want to restrict access to a single organization. For example, promote a general attribute like `DepartmentName` to enterprise because each employee needs to be grouped in a department. Alternatively, keep an attribute like `SoftballTeam` at the suborganization level because its members have joined a lunchtime league.
6. Click **Alert Folders**.
7. Select an alert folder type to promote, and click **Promote to Enterprise** or **Promote to System** based on what types of alerts certain personnel should see.

   For example, promote an alert folder like `FireDrills` from suborganization to enterprise if the entire enterprise needs to receive alerts from that alert folder. Keep the alert folder like `ExecutiveSafety` at suborganization if you want to restrict access to operators and users that have a need to know.
8. Save your changes.

You have completed the reorganization.

What's next?

Grant permissions to the enterprise administrator for access to the suborganizations.

1. Restart IIS after you have made the structure or content changes.
2. Log in to the enterprise organization as an administrator.
3. Create a user and grant this user the enterprise administrator role.
4. Change to each suborganization and grant the same user the organization administrator role.

Duplicate organizations across systems

Use the Organization Duplicator to make a copy of an organization on another server to set up a failover system, or to migrate to a new server. This tool is located on the application server.

Prerequisites:

- Two configured organizations on different database servers:
  - **Source server**: The server location of the organization to be duplicated.
  - **Target server**: The server location where the organization is to be duplicated.

- The source server should have configured users, alert templates, map layers, and other objects.

Objects that are not duplicated:

- Global health monitors
- AtHoc Connect organizations
- Incoming alerts
- Sent alerts
- User accounts
- Distribution lists (static only)

For detailed information about what is duplicated, see Appendix B: Organization duplicator object management.

1. Log in to the application server for the source system and navigate to the following directory: `AtHocENS/ServerObjects/Tools/VPSDuplicator`.
2. Run the Organization Duplicator tool as an administrator.
3. Provide the source and target server information:
   - Source:
     - Database server: The source application server name. For example: `DBSourceServer.mynetwork.com`.
     - Username and Password of the ngad database.
   - Target:
     - Database server: The target application server name. For example: `DBTargetServer.mynetwork.com`.
     - Username and Password of the ngad database.
4. Click **Connect** to establish a connection and view the organizations that can be duplicated.
5. Select the organizations to be duplicated. The Status column indicates whether the organization is ready to copy.
6. Do one of the following:
   - Click **Copy to Target** to copy the organizations to a new system.
   - Click **New on Source** to create a new organization on the source system.
   - Click **Duplicate on Source** to copy an organization on the same system.

The message log indicates whether the duplication was successful.

Create organizations on the source server

You can use the Organization Duplicator to create organizations on the source server.

1. Click **New on Source**.
2. Enter the organization name and organization code (around 5 characters.)
3. Select the type of organization.
4. Click **OK**.

You cannot select an organization administrator using the tool. The message log shows whether the new organization has been created.

Duplicate organizations on the source server

You can use the Organization Duplicator to duplicate organizations on the source server.

1. Click **Duplicate on Source**.
2. Enter the organization name and the number of copies of the organization that you want to create.

3. If you select a value higher than 1, organizations are created with the following string appended to the name: “Copy 0001”.
4. Click **OK**. The message log shows whether the duplicated organizations have been created.

Note: After duplicating the organization, verify operator permissions to the new organization.

- Use the system administrator role to do the initial set up. To access the Users menu, use the advanced operator manager role to assign your user account the organization administrator role.
- **Distribution List permissions**: Ensure that users with accounts in a different organization have distribution list permission in the new organization. Use the advanced operator manager role to provide access distribution lists.
- **Basic Organization roles:** If operators from other organizations need permission for a Basic organization, use the advanced operator manager role to configure permissions. Grant either the basic administrator or basic operator roles. If you choose other roles, you might get unexpected results.

Configure AtHoc database operations to use Windows authentication

Run the configuration script on each application server so that AtHoc database operations use Windows authentication. This script ensures a trusted connection from the application server to connect to database server. All AtHoc applications need to run under a Windows domain account.

1. From the application server, open a command prompt and run as administrator.
2. Navigate to the following directory: `<%AtHocENS%>\ServerObjects\Tools\`.
3. Run the following script, using 32-bit version of cscript: `setWindowsAuth.vbs <%DomainName%> <%Domain AccountName%> <%DomainAccountPassword%>`.

   Where:

   - DomainName is the Windows domain name of the application server.
   - Domain Account Name is the name of the Windows domain account.
   - DomainAccountPassword is the password of the Windows domain account.

The script makes the following updates:

- Creates a Windows domain account as a login and a new "AtHoc" database server role in the SQL server. The Windows domain account is created as a member of AtHoc server role.

  Database access is granted to the AtHoc server role instead of giving direct access to the Windows domain account. This login is given ownership to all AtHoc databases.

  If for any reason a database restore is performed manually and the Windows domain account user account is missing, it can be created by running the ATH_CREATE_USERS SQL stored procedure in the msdb database. To return to SQL authentication by using ngad login, use the ATH_CREATE_USERS stored procedure.

  Contact BlackBerry AtHoc customer support for information about using this stored procedure.
- Updates the connection string for BlackBerry AtHoc to use a trusted connection.
- Modifies all AtHoc application pool identities in IIS to use the new domain account.
- Modifies the Anonymous account in IIS from IUSR to the new domain account.

Configure IIS processor affinity

On multi-CPU servers, application pools can be configured to establish affinity between worker processes and an individual processor to more efficiently use CPU caches. This configuration also isolates applications such that if one application causes a CPU to stop responding, other CPUs continue to function normally. Processor affinity is used in conjunction with the processor affinity mask setting to specify CPUs.

1. Create a .vbs file named `affinity.vbs`. Copy the following data, and save it in your temp folder:

```
set appPoolObj=GetObject("IIS://localhost/W3svc/AppPools/DefaultAppPool")
    ' Set the properties. Enable processor affinity for processors 0,1,2,3:
    appPoolObj.Put "SMPAffinitized", TRUE
    appPoolObj.Put "SMPProcessorAffinityMask", &HFF
    ' Save the property changes in the metabase:
    appPoolObj.SetInfo
    WScript.Echo "After: " & appPoolObj.SMPAffinitized & ", " &
 appPoolObj.SMPProcessorAffinityMask
```

2. Change the value of **SMPProcessorAffinityMask** in the `affinity.vbs` file to reflect the number of cores available.

   The value for SMPProcessorAffinityMask must be entered as hexadecimal.
3. Complete any of the following tasks:
   a. Specify specific cores to use: Create the value as binary (each core is represented by 1 bit) and then transformed into a hexadecimal. The easiest way to do this is to use a Windows scientific calculator. For example, eight cores in binary would be represented as 11111111.
   b. Specify to use only the first four cores. For example, all cores in the same chip for a quad-core): Select 00001111 or 11110000 (if dual-quad.)
   c. Specify to use every other core:
      1. Enter **10101010** (or **01010101**) in a Windows scientific calculator in binary data (Bin) and click **Hex** to see the equivalent value in hexadecimal (&AA or &55.)
      2. Stop IIS and run the `affinity.vbs` file in a command prompt. (`cscript affinity.vbs`)

         You should see the mask change to the correct decimal value for the hexadecimal value that was used. If you are not sure what the decimal value should be, check the Windows calculator.
      3. Reset the IIS.
      4. Open the Performance Monitor (`perfmon`) performance tab to verify that the correct core combination is used.

Increase the IIS file size upload limit

When uploading files, IIS may return an HTTP 500 error because the maximum file size limit has been exceeded. For example, this can occur when uploading very large .csv or audio files.

1. In **IIS Manager**, click the **client** web application.
2. Double-click the ASP feature icon.
3. Expand the Limits Properties.
4. Change the value of the Maximum Requesting Entity Body Limit.

This entry specifies the maximum number of bytes allowed in the entity body of an ASP request.

Note: The Setup Kit sets this to 20480000 (20 Mb). If audio files larger than that will need to be uploaded, this value must be increased.

Database recovery setting

If the recovery model for the SQL databases is set to Full, the transaction log files must be backed up before they become full. Otherwise, all operations on the database will stop and the system will freeze. It is very important to understand the backup strategy for the site and configure these settings carefully. Consult with your database administrator before you make any changes to the recovery model.

Note: The default setting for recovery is **Simple**.

IIS 10.0 Security Technology Implementation Guide

The following sections describe the server and application tasks that you can complete to achieve IIS 10.0 STIG compliance in your BlackBerry AtHoc system.

Server STIG

This section describes the tasks you need to complete to ensure your servers comply with the IIS 10.0 STIG.

IIST-SV-000102: Enable enhanced logging

Enhanced logging for the IIS 10.0 web server must be enabled and must capture all user and web server events.

To check compliance with IIST-SV-000102, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields** and verify that at least one of the following fields are selected:
   - Date
   - Time
   - Client IP Address
   - User Name
   - Method
   - URI Query
   - Protocol Status
   - Referrer

If no options are selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the following fields: **Date**, **Time**, **Client IP Address**, **User Name**, **Method**, **URI Query**, **Protocol Status**, and **Referrer**.
6. In the **Actions** pane, click **Apply**.

IIST-SV-000103: Enable log file and Event Tracing for windows

Both the log file and Event Tracing for Windows (ETW) for the IIS 10.0 web server must be enabled.ts.

To check compliance with IIST-SV-000103, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the **Actions** pane, click **Apply**.

IIST-SV-000110: Produce log records

The IIS 10.0 web server must produce log records that contain sufficient information to establish the outcome (success or failure) of IIS 10.0 web server events.

To check compliance with IIST-SV-000110, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, verify that **Request Header >> Connection** and **Request Header >> Warning** are selected.

If any custom fields are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, select the following fields:
    - **Source Type** > **Request Header**
    - **Source** > **Connection**
7. Click **OK**.
8. Click **Source Type** > **Response Header**.
9. Click **Source** > **Warning**.
10. Click **OK**.
11. In the **Actions** pane, click **Apply**.

IIST-SV-000111: Produce log records

The IIS 10.0 web server must produce log records that contain sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IIST-SV-000111, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, verify that **User Agent**, **User Name**, and **Referrer** are selected.

7. Under **Custom Fields**, verify that **Request Header >> Authorization** and **Response Header >> Content-Type** are selected.

If any of the standard or custom fields are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is configured to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, select **User Agent**, **User Name**, and **Referrer**.
7. Under **Custom Fields**, select the following fields:
    - **Source Type** > **Request Header**
    - **Source** > **Authorization**
8. Click **OK**.
9. Click **Source** > **Content-Type**
10. Click **Source Type** > **Response Header**.
11. Click **OK**.
12. In the **Actions** pane, click **Apply**.

IIST-SV-000115: Protect log information

The log information from the IIS 10.0 web server must be protected from unauthorized modification or deletion.

To check compliance with IIST-SV-000115, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Click **Browse** and then navigate to the directory where the log files are stored.
5. Right-click the log file directory and select **Properties**.
6. Click the **Security** tab.
7. Verify the log file access is restricted to **System - Full Control** and **Administrators - Full Control**.

If the log file restrictions are not set to **System - Full Control** and **Administrators - Full Control**, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. Click **Browse** and then navigate to the directory where the log files are stored.
5. Right-click the log file directory and select **Properties**.
6. Click the **Security** tab.
7. Set the log file permissions to **System - Full Control** and **Administrators - Full Control**.
8. Click **OK**.
9. In the **Actions** pane, click **Apply**.

IIST-SV-000117: Do not perform user management

The IIS 10.0 web server must not perform user management for hosted applications.

To check compliance with IIST-SV-000117, complete the following steps:

1. Verify with the System Administrator (SA) if the IIS 10.0 web server is hosting an application.
2. If the IIS 10.0 web server is hosting an application, verify with the SA that they can provide supporting documentation about how the application's user management is accomplished outside of the IIS 10.0 web server.

If the web server is hosting an application and the SA cannot provide the supporting documentation, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Reconfigure any hosted applications on the IIS 10.0 web server to perform user management outside the IIS 10.0 web server.
2. Document how the hosted application user management is accomplished.

IIST-SV-000118: Contain only necessary functions

The IIS 10.0 web server must contain only functions that are necessary for operation.

To check compliance with IIST-SV-000118, complete the following steps:

1. Click **Start**.
2. Open the **Control Panel**.
3. Click **Programs**.
4. Click **Programs and Features**.
5. Review the installed programs.

If any programs are installed that are not required for the IIS 10.0 web services, your server is not compliant. If additional software is needed, supporting documentation must be signed by the Information Systems Security Officer (ISSO.)

If your server is not compliant, remove all unapproved programs and roles from the production IIS 10.0 web server.

IIST-SV-000119: Must not be both a website server and a proxy server

The IIS 10.0 web server must not be both a website server and a proxy server.

To check compliance with IIST-SV-000119, complete the following steps:

1. Open the IIS 10.0 Manager.
2. In the **Connections** pane, select the IIS 10.0 web server.
3. Under **IIS installed features**, verify if **Application Request Routing Cache** is present. If this setting is not present, your server is compliant.
4. If the **Application Request Routing Cache** is present, double-click the icon.
5. In the **Actions** pane, under **Proxy**, click **Server Proxy Settings...**.
6. In the **Application Request Routing** window, verify if the **Enable proxy** option is selected.

If the **Enable proxy** option is selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. In the **Connections** pane, select the IIS 10.0 web server.
3. Under **IIS installed features** double-click the **Application Request Routing Cache** icon.
4. In the **Actions** pane, under **Proxy**, click **Server Proxy Settings...**.
5. In the **Application Request Routing** window, deselect the **Enable proxy** option.
6. In the **Actions** pane, click **Apply**.

IIST-SV-000120: Remove code samples, example applications, and tutorials

All IIS 10.0 web server sample code, example applications, and tutorials must be removed from a production IIS 10.0 server.

To check compliance with IIST-SV-000120, complete the following steps:

1. Navigate to the following folders:
   - intepub\
   - Program Files\Common Files\System\msadc
   - Program Files (x86)\Common Files\System\msadc
2. Check if the folder or sub-folders contain any executable sample code, example applications, or tutorials which are not explicitly used by a production website.

If the folder or sub-folders contain any executable sample code, example applications, or tutorials which are not explicitly used by a production website, your server is not compliant.

If your server is not compliant, remove any executable sample code, example applications, or tutorials which are not explicitly used by a production website.

IIST-SV-000121: Delete accounts created by uninstalled features

Accounts created by uninstalled features such as tools and utilities must be deleted from the IIS 10.0 server.

To check compliance with IIST-SV-000121, complete the following steps:

1. Open the IIS 10.0 Manager.
2. On the **Apps** menu, under **Administrative Tools**, click **Computer Management**.
3. In the left pane, expand **Local Users and Groups**.
4. Click **Users**.
5. Review the local users listed in the middle pane.

If any local accounts are present that were created by uninstalled features or are not used, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. On the **Apps** menu, under **Administrative Tools**, click **Computer Management**.
3. In the left pane, expand **Local Users and Groups**.
4. Click **Users**.
5. Delete any local accounts that were created by uninstalled features or are not used.

IIST-SV-000123: Remove unnecessary features, utilities, plug-ins, and modules

The IIS 10.0 web server must be reviewed on a regular basis to remove any Operating System features, utility programs, plug-ins, and modules not necessary for operation.

To check compliance with IIST-SV-000123, complete the following steps:

1. Consult with the System Administrator and review all installed IIS 10.0 and Operating System features.
2. Determine if any features installed are no longer necessary for operation.

If any Operating System features are installed, your server is not compliant.

If your server is not compliant, remove all utility programs, Operating System features, or modules that are not necessary for web server operation.

IIST-SV-000124: Disable MIMEs that invoke OS shell programs

The IIS 10.0 web server must have Multipurpose Internet Mail Extensions (MIME) that invoke OS shell programs disabled.

To check compliance with IIST-SV-000124, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. Under **Application**, verify that the list of MIME types for OS shell program extensions that have been removed includes, at a minimum, the following extensions:
    - .exe
    - .dll
    - .com
    - .bat
    - .csh

If any OS shell MIME types are configured, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under "Application", remove MIME types for OS shell program extensions, to include at a minimum, the following extensions:
    - .exe
    - .dll
    - .com
    - .bat
    - .csh
6. In the **Actions** pane, click **Apply**.

IIST-SV-000125: Disable WebDAV

The IIS 10.0 web server must have Web Distributed Authoring and Versioning (WebDAV) disabled.

To check compliance with IIST-SV-000125, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Click the **Logging** icon.
4. In the **Cells** section, review the list of features.

If the **WebDAV Authoring Rules** icon exists, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Access Server Manager on the IIS 10.0 web server.
2. Click the IIS 10.0 web server name.
3. Click **Manage**.
4. Click **Add Roles and Features**.

5. On the **Before you begin** dialog, click **Next**.
6. On the **Installation Type** dialog, click **Role-based or feature-based installation**.
7. Click **Next**.
8. On the **Server Selection** dialog, click the IIS 10.0 web server.
9. From the **Windows Features** dialog, navigate to **World Wide Web Services** > **Common HTTP Features**.
10. Deselect **WebDAV Publishing**.
11. Click **Next** to remove the WebDAV Publishing feature from the IIS 10.0 web server.

IIST-SV-000130: Limit installed Java software

Java software installed on a production IIS 10.0 web server must be limited to .class files and the Java Virtual Machine.

To check compliance with IIST-SV-000130, search the system for files with either .java or .jpp extensions.

If files with .java or .jpp extensions are found, your server is not compliant.

If your server is not compliant, remove all files from the web server with both .java or .jpp extensions.

IIST-SV-000131: Limit access to only administrative accounts

IIS 10.0 web server accounts that access the directory tree, the shell, or other operating system functions and utilities must only be administrative accounts.

To check compliance with IIST-SV-000131, complete the following steps:

1. Obtain a list of the user accounts with access to the system, including all local and domain accounts.
2. Review the privileges to the web server for each account.
3. Verify with the System Administrator or the ISSO that all privileged accounts are mission essential and documented.
4. Verify with the System Administrator or the ISSO that all non-administrator access to shell scripts and operating system functions are mission essential and documented.

If undocumented privileged accounts are found, your server is not compliant.

If undocumented non-administrator access to shell scripts and operating system functions are found, your server is not compliant.

Note: If your IIS 10 installation supports Microsoft Exchange and is not otherwise hosting any content, this requirement is not applicable.

If your server is not compliant, complete the following steps:

1. Ensure that non-administrators are not allowed access to the directory tree, the shell, or other operating system functions and utilities.
2. Ensure that all non-administrator access to shell scripts and operating system functions is mission essential and documented.

IIST-SV-000134: Use cookies to track session state

The IIS 10.0 web server must use cookies to track session state.

To check compliance with IIST-SV-000134, do one of the following:

- 1. Open the IIS 10.0 Manager.
  2. Click the IIS 10.0 web server name.
  3. Under **ASP.Net**, double-click the **Session State** icon.
  4. Under **Cookie Settings**, verify that the **Use Cookies** option is selected in the **Mode** drop-down list.

If the **Use Cookies** option is not selected, your server is not compliant.

- 1. Click the site name.
  2. In the **Management** section, click **Configuration Editor**.
  3. On the configuration editor, from the **Section:** drop-down list, locate **system.web/sessionState**.
  4. Verify that **cookieless** is set to **UseCookies**.

  If the **cookieless** option is not set to **UseCookies**, your server is not compliant.

Note: If your IIS 10.0 server/site is used only for system-to-system maintenance, does not allow users to connect to an interface, and is restricted to specific system IPs, this is not applicable.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **ASP.Net**, double-click the **Session State** icon.
4. Under **Cookie Settings**, select **Use Cookies** from the **Mode** drop-down list.
5. In the **Actions** pane, click **Apply**.

IIST-SV-000135: Accept only system-generated session identifiers

The IIS 10.0 web server must accept only system-generated session identifiers.

To check compliance with IIST-SV-000135, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **ASP.NET** section, select **Session State**.
4. Under **Cookie Settings**, verify that the **Use Cookies** option is selected from the **Mode:** drop-down list.
5. Under **Time-out (in minutes)**, verify that **20 minutes or less** is selected.

If the **Use Cookies** option is selected, and **Time-out (in minutes)** is not set to **20 minutes or less**, you server is not compliant.

Note: If your IIS 10.0 server/site is used only for system-to-system maintenance, does not allow users to connect to the interface, and is restricted to specific system IPs, this is not applicable.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **ASP.NET** section, click **Session State**.
4. In the **Actions** pane, click **Apply**.
5. Under **Cookie Settings**, select the **Use Cookies** option from the **Mode:** drop-down list.
6. Under **Time-out (in minutes)**, click **20 minutes or less**.

IIST-SV-000138: Disable directory browsing

Directory Browsing on the IIS 10.0 web server must be disabled.

To check compliance with IIST-SV-000138, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Directory Browsing** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.
5. In the **Actions** panel, verify that **Directory Browsing** is disabled.

If **Directory Browsing** is enabled, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Directory Browsing** icon.
4. In the **Actions** pane, click **Disabled**.

IIST-SV-000139: Index only web content

The IIS 10.0 web server Indexing must only index web content.

To check compliance with IIST-SV-000139, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex\Catalogs\. If this key exists, then indexing is enabled. If the key does not exist, this check is not applicable.
4. Review the catalog keys to determine if directories other than web document directories are being indexed.

If directories other than web document directories are being indexed, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Run MMC.
2. Add the **Indexing Service** snap-in.
3. Edit the indexed directories to include only web document directories.

IIST-SV-000140: Modify warning and error messages

Warning and error messages displayed to clients must be modified to minimize the identity of the IIS 10.0 web server, patches, loaded modules, and directory paths.

To check compliance with IIST-SV-000140, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Error Pages** icon.
4. Click any error message.
5. In the **Actions** pane, click **Edit Feature Setting**.

If the feature setting is not set to **Detailed errors for local requests and custom error pages for remote requests**, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Error Pages** icon.
4. Click any error message.
5. In the **Actions** pane, set **Feature Setting** to **Detailed errors for local requests and custom error pages for remote requests**.

IIST-SV-000141: Follow access policy

Remote access to the IIS 10.0 web server must follow access policy or work with enterprise tools designed to enforce policy requirements.

If web administration is performed at the console, this check is not applicable.

If web administration is performed remotely, to check compliance with IIST-SV-000141, verify that the following conditions are met:

- If administration of the server is performed remotely, it is only performed securely by System Administrators.
- If website administration or web application administration has been delegated, those users are documented and approved by the ISSO.
- Remote administration is in compliance with any requirements contained within the Windows Server STIGs and any applicable Network STIGs.
- Remote administration of any kind is restricted to documented and authorized personnel.
- All users performing remote administration are authenticated.
- All remote sessions are encrypted and use FIPS 140-2-approved protocols. FIPS 140-2-approved TLS versions include TLS V1.2 or greater.

Review with site management how remote administration is configured on the website, if applicable. If remote management meets the criteria listed above, your server is compliant. If remote management is used and does not meet the criteria listed above, your server is not compliant.

If your server is not compliant, ensure that the web server administration is only performed over a secure path.

IIST-SV-000142: Restrict inbound connections

The IIS 10.0 web server must restrict inbound connections from non-secure zones.

Note: This requirement applies to the Web Management Service. If the Web Management Service is not installed, this requirement is not applicable.

To check compliance with IIST-SV-000142, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **Management**, double-click **Management Service**.
4. If **Enable remote connections** is not selected, this requirement is not applicable. If **Enable remote connections** is selected, review the entries under **IP Address Restrictions**.
5. Verify that only known, secure IP ranges are configured as **Allow**.

If **IP Address Restrictions** are not configured, or IP ranges that are configured as **Allow** are not restrictive enough to prevent connections from non-secure zones, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.5 web server name.
3. Under **Management**, double-click **Management Service**.
4. In the **Actions** pane, stop the Web Management Service.
5. Configure only known, secure IP ranges as **Allow**.
6. In the **Actions** pane, click **Apply**.
7. In the **Actions** pane, restart the Web Management Service.

IIST-SV-000144: Conform to minimum file permission requirements

IIS 10.0 web server system files must conform to minimum file permission requirements.

To check compliance with IIST-SV-000144, complete the following steps:

1. Open Explorer and navigate to the **inetpub** directory.
2. Right-click **inetpub** and select **Properties**.

3. Click the **Logging** icon.
4. Click the **Security** tab.
5. Verify the permissions for the following users:
    - System: Full control
    - Administrators: Full control
    - TrustedInstaller: Full control
    - ALL APPLICATION PACKAGES (built-in security group): Read and execute
    - ALL RESTRICTED APPLICATION PACKAGES (built-in security group): Read and execute
    - Users: Read and execute, list folder contents
    - CREATOR OWNER: Full Control, Subfolders and files only

If the permissions for the users listed above are less restrictive, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open Explorer and navigate to the **inetpub** directory.
2. Right-click **inetpub** and select **Properties**.
3. Click the **Security** tab.
4. Set the following permissions:
    - System: Full control
    - Administrators: Full control
    - TrustedInstaller: Full control
    - ALL APPLICATION PACKAGES (built-in security group): Read and execute
    - ALL RESTRICTED APPLICATION PACKAGES (built-in security group): Read and execute
    - Users: Read and execute, list folder contents
    - CREATOR OWNER: Special permissions to subkeys

IIST-SV-000145: Allocate sufficient log record storage capacity

The IIS 10.0 web server must use a logging mechanism configured to allocate log record storage capacity large enough to accommodate the logging requirements of the IIS 10.0 web server.

To check compliance with IIST-SV-000145, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. In the **Logging** dialog, verify the **Directory:** that W3C logging is written to.
5. Confirm with the System Administrator that the designated log path is of sufficient size to maintain the logging.
6. Under **Log File Rollover**, verify that **Do not create new log files** is not selected.
7. Verify that a schedule is configured to roll over log files on a regular basis.
8. Verify with the System Administrator that there is a documented process for moving the log files off of the IIS 10.0 web server to another logging device.

If the designated logging path device is not large enough to maintain all log files, and there is not a schedule to roll over files on a regular basis, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Under **IIS**, double-click the **Logging** icon.

4. In the **Logging** dialog, designate a log path to a location able to house the logs.
5. Under **Log File Rollover**, deselect the **Do not create new log files** option.
6. Configure a schedule to roll over log files on a regular basis.

IIST-SV-000147: Restrict access to web administration tools

Access to web administration tools must be restricted to the web manager and the web manager's designees.

To check compliance with IIST-SV-000147, complete the following steps:

1. Right-click **InetMgr.exe**, and then click **Context** > **Properties**.
2. Click the **Security** tab.
3. Review the groups and user names.
4. Compare the local documentation authorizing specific users against the users observed when reviewing the groups and users.

The following accounts may have full control privileges:

- TrustedInstaller
- Web Managers
- Web Manager designees
- CREATOR OWNER: Full Control, Subfolders and files only

The following accounts may have read and execute or read permissions:

- Non Web Manager Administrators
- ALL APPLICATION PACKAGES (built-in security group)
- ALL RESTRICTED APPLICATION PACKAGES (built-in security group)
- SYSTEM
- Users

Specific users may have read and execute and read permissions.

If any other access is observed, your server is not compliant.

If your server is not compliant, restrict access to the web administration tool to only the web manager and the web manager's designees.

IIST-SV-000149: Disable IPP

The Internet Printing Protocol (IPP) must be disabled on the IIS 10.0 web server.

If the Print Services role and the Internet Printing role are not installed, this check is not applicable.

To check compliance with IIST-SV-000149, complete the following steps:

1. Navigate to the following directory: %windir%\web\printers. Take note if the directory exists.
2. Click **Start** > **Administrative Tools**, and then click **Server Manager**.
3. Expand the **roles** node.
4. Right-click **Print Services**, and then click **Remove Roles Services**.

If the %windir%\web\printers folder exists, your server is not compliant. If the Internet Printing option is enabled, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Click **Start** > **Administrative Tools**, and then click **Server Manager**.
2. Expand the **roles** node.
3. Right-click **Print Services**, and then click **Remove Roles Services**.

4. Deselect the the **Internet Printing** option.
5. Click **Next**.
6. Click **Remove**.

IIST-SV-000152: Use TLS to send session IDs

IIS 10.0 web server session IDs must be sent to the client using TLS.

To check compliance with IIST-SV-000152, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **session** section.
6. Verify that **keepSessionIdSecure** is set to **True**.

If **keepSessionIdSecure** is not set to True, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **session** section.
6. Select **True** for **keepSessionIdSecure**.
7. In the **Actions** pane, click **Apply**.

IIST-SV-000153: Use TLS to maintain confidentiality

An IIS 10.0 web server must maintain the confidentiality of controlled information during transmission through the use of an approved Transport Layer Security (TLS) version.

To check compliance with IIST-SV-000153, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server.
4. Verify that **DisabledByDefault** has a REG_DWORD value of **0**.
5. Navigate to the following paths and verify that **DisabledByDefault** has a REG_DWORD value of **1** and **Enabled** has a REG_DWORD value **0**:
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server

If any of the registry paths do not exist or are configured with the wrong value, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access an administrator command prompt and type **regedit <enter>** to access the server's registry.
3. Navigate to: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server.

4. Configure **DisabledByDefault** to have a REG_DWORD value of **0**.
5. Navigate to the following paths and configure **DisabledByDefault** to have a REG_DWORD value of **1** and **Enabled** to have a REG_DWORD value **0**:
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server
    - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server

IIST-SV-000154: Use approved TLS version

The IIS 10.0 web server must maintain the confidentiality of controlled information during transmission through the use of an approved Transport Layer Security (TLS) version.

To check compliance with IIST-SV-000154, review the web server documentation and deployed configuration to determine which version of TLS is being used.

If the TLS version is not TLS 1.2 or higher, according to NIST SP 800-52, or if non-FIPS-approved algorithms are enabled, your server is not compliant.

If your server is not compliant, configure the web server to use an approved TLS version according to NIST SP 800-52 and disable all non-approved versions.

IIST-SV-000156: Assign passwords

All accounts installed with the IIS 10.0 web server software and tools must have passwords assigned and default passwords changed.

To check compliance with IIST-SV-000156, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access the **Apps** menu.
3. Under **Administrative Tools**, click **Computer Management**.
4. In the left pane, expand **Local Users and Groups**.
5. Click **Users**.
6. Review the local users displayed in the middle pane.
7. If any local accounts are present and used by IIS 10.0, verify with your System Administrator that the default passwords have been changed.

If passwords have not been changed from the default, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Access the IIS 10.0 web server.
2. Access the **Apps** menu.
3. Under **Administrative Tools**, click **Computer Management**.
4. In the left pane, expand **Local Users and Groups**.
5. Click **Users**.
6. Change the password for any local accounts displayed that are used by IIS 10.0.
7. Verify with your System Administrator that the default passwords have been changed.

IIST-SV-000158: Remove unspecified file extensions

Unspecified file extensions on a production IIS 10.0 web server must be removed.

To check compliance with IIST-SV-000158, complete the following steps:

1. Open the IIS 10.0 Manager.

2. Click the IIS 10.0 web server name.
3. Double-click the **ISAPI and CGI restrictions** icon.
4. Click **Edit Feature Settings**.
5. Verify that **Allow unspecified CGI modules** and **Allow unspecified ISAPI modules** are not selected.

If **Allow unspecified CGI modules** or **Allow unspecified ISAPI modules** is selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **ISAPI and CGI restrictions** icon.
4. Click **Edit Feature Settings**.
5. Deselect **Allow unspecified CGI modules** and **Allow unspecified ISAPI modules**.
6. Click **OK**.

IIST-SV-000159: Configure a global authorization rule

The IIS 10.0 web server must have a global authorization rule configured to restrict access.

To check compliance with IIST-SV-000159, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **.NET Authorization Rules** icon.

If any groups other than **Administrators** are listed, your server is not compliant.

If ASP.NET is not installed, this is not applicable. If the server is hosting Microsoft SharePoint, this is not applicable. If the server is hosting WSUS, this is not applicable.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. Double-click the **Authorization Rules** icon.
4. Remove all groups other than **Administrators**.

IIST-SV-000200: Configure the Max Connections setting

The IIS 10.0 website's MaxConnections setting must be configured to limit the number of allowed simultaneous session requests.

To check compliance with IIST-SV-000200, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.
3. In the **Management** section, click **Configuration Editor**.
4. From the **Section:** drop-down list at the top of the configuration editor, locate **system.applicationHost/sites**.
5. Expand **siteDefaults**.
6. Expand **limits**.
7. Review the results and verify that the value of the **maxconnections** parameter is greater than zero.

If the **maxconnections** parameter value is zero, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server name.

3. In the **Management** section, click **Configuration Editor**.
4. From the **Section:** drop-down list at the top of the configuration editor, locate **system.applicationHost/sites**.
5. Expand **siteDefaults**.
6. Expand **limits**.
7. Set the **maxconnections** parameter to a value greater than zero.

IIST-SV-000205: Enable HSTS

The IIS 10.0 web server must enable HTTP Strict Transport Security (HSTS.)

To check compliance with IIST-SV-000205, complete the following steps:

1. Access the IIS 10.0 web server.
2. Open IIS Manager.
3. Click the IIS 10.0 web server name.
4. Under **Management**, open **Configuration Editor**.
5. For the **Section**, navigate to **system.applicationHost/sites**.
6. Expand **siteDefaults** and **HSTS**.

Your server is not compliant if:

- enabled is not set to True.
- includeSubDomains is not set to True.
- max-age is not set to a value greater than 0.
- redirectHttpToHttps is not set to True.

If your server is not compliant, complete the following steps:

1. Log in to the Configuration Editor in the IIS Manager or Powershell.
2. Enable **HSTS**.
3. Set **includeSubDomains** to **True**.
4. Set **max-age** to a value greater than 0.
5. Set **redirectHttpToHttps** to **True**.

IIST-SV-000160: Require authentication for an SMTP relay

An IIS server configured to be an SMTP relay must require authentication.

To check compliance with IIST-SV-000160, interview your System Administrator about the role of the IIS 10.0 web server.

If the IIS 10.0 web server is running SMTP relay services, have the SA provide supporting documentation about how the server is hardened. A DoD-issued certificate, and specific allowed IP address should be configured.

If the IIS web server is not running SMTP relay services, this is not applicable.

If the IIS web server running SMTP relay services without TLS enabled, your server is not compliant.

If your server is not compliant, configure the relay server with a specific allowed IP address from the same network as the relay and implement TLS.

Application STIG

This section describes the tasks you need to complete to ensure your application complies with the IIS 10.0 STIG.

IIST-SI-000201: Enable session state

The IIS 10.0 website session state must be enabled.

To check compliance with IIST-SI-000201, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State Mode Settings**, verify that the **In Process** mode is selected.

If the **Session State Mode Settings** mode is not set to **In Process** selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, select **Session State**.
4. Under **Session State Mode Settings**, select **In Process** mode.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000202: Configure session state cookie settings

The IIS 10.0 website session state cookie settings must be configured to Use Cookies mode.

To check compliance with IIST-SI-000202, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Cookie Settings**, verify that the **Use Cookies** mode is selected from the **Mode:** drop-down list.

If the **Use Cookies** mode is selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, select **Session State**.
4. Under **Cookie Settings**, select **Use Cookies** from the **Mode:** drop-down list.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000206: Enable the log file and ETW

Both the log file and Event Tracing for Windows (ETW) for each IIS 10.0 website must be enabled.

To check compliance with IIST-SI-000206, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your application is not compliant.

Note: "Microsoft-IIS-Logging/logs" must be enabled before configuring this setting.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000210: Produce log records containing sufficient information

The IIS 10.0 website must produce log records containing sufficient information to establish the identity of any user/subject or process associated with an event.

To check compliance with IIST-SI-000210, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 web server.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the **Format:** option is configured to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, verify that the following fields are configured:
   - Request Header >> Authorization
   - Response Header >> Content-Type

If either **Request Header >> Authorization** or **Response Header >> Content-Type** is not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, configure **Format:** under **Log File** to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, select **Request Header >> Authorization**and **Response Header >> Content-Type**.
7. Click **OK**.
8. In the **Actions** pane, click **Apply**.

IIST-SI-000214: Disable MIMEs that invoke OS shell programs

The IIS 10.0 website must have Multipurpose Internet Mail Extensions (MIME) that invoke OS shell programs disabled.

To check compliance with IIST-SI-000214, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under **Application**, verify that MIME types for OS shell program extensions have been removed, to include at a minimum, the following extensions:
   - .exe

- .dll
- .com
- .bat
- .csh

If any OS shell MIME types are configured, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 site.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by:** drop-down list, select **Content Type**.
5. From the list of extensions under **Application**, remove MIME types for OS shell program extensions to include, at a minimum, the following extensions:
   - .exe
   - .dll
   - .com
   - .bat
   - .csh
6. In the **Actions** pane, click **Apply**.

IIST-SI-000216: Set resource mappings

The IIS 10.0 website must have resource mappings set to disable the serving of certain file types. For request filtering, the ISSO must document and approve all scripts the website allows (white list) and denies (black list.) The white list and black list are compared to the request filtering in IIS 10.0. Request filtering at the site level takes precedence over request filtering at the server level.

To check compliance with IIST-SI-000216, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **Request Filtering** > **File Name Extensions Tab**.

If any script file extensions from the black list are not denied, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **Request Filtering** > **File Name Extensions Tab** > **Deny File Name Extension**.
4. Add any script file extensions listed on the black list that are not listed.
5. In the **Actions** pane, click **Apply**.

IIST-SI-000217: Disable WebDAV

The IIS 10.0 website must have Web Distributed Authoring and Versioning (WebDAV) disabled.

To check compliance with IIST-SI-000217, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the IIS 10.0 website.
3. Review the features listed under the **IIS** section.

If the **WebDAV Authoring Rules** icon is present, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Access **Server Manager** on the IIS 10.0 website.
2. Click **Local Server**.
3. Click **Manage**.
4. Click **Add Roles and Features**.
5. In the **Before you begin** dialog, click **Next**.
6. In the **Installation Type** dialog, click **Role-based or feature-based installation**.
7. Click **Next**.
8. On the **Server Selection** dialog, select the IIS 10.0 web server.
9. On the **Windows Features** dialog, navigate to **World Wide Web Services** > **Common HTTP Features**.
10. Deselect **WebDAV Publishing**.
11. Click **Next**.
12. In the **Actions** pane, click **Apply**.

IIST-SI-000221: Restrict anonymous access accounts

Anonymous IIS 10.0 website access accounts must be restricted.

To check compliance with IIST-SI-000221, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click **Authentication**.
4. If Anonymous Access is disabled, this is not applicable. If Anonymous Access is enabled, click **Anonymous Authentication**.
5. In the **Actions** pane, click **Edit**.
6. If the **Specific user** option is selected and an ID is specified in the adjacent control box, this is the ID being used for anonymous access. Take note of the account name.
7. Check privileged groups that may allow the anonymous account inappropriate membership:
    a. On the computer, open **Server Manager**.
    b. Expand **Configuration**.
    c. Expand **Local Users and Groups**.
    d. Click **Groups**.
    e. Review members of the following privileged groups:
        - Administrators
        - Backup Operators
        - Certificate Services (of any designation)
        - Distributed COM Users
        - Event Log Readers
        - Network Configuration Operators
        - Performance Log Users
        - Performance Monitor Users
        - Power Users
        - Print Operators
        - Remote Desktop Users
        - Replicator
    f. Double-click each group and review its members.

If the IUSR account or any account noted above used for anonymous access is a member of any group with privileged access, your application is not compliant.

If your application is not compliant, remove the Anonymous Access account from all privileged accounts and all privileged groups.

IIST-SI-000223: Generate unique session identifiers

The IIS 10.0 website must generate unique session identifiers that cannot be reliably reproduced.

To check compliance with IIST-SI-000223, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State** mode settings, verify that the **In Process** mode is selected.

If the **In Process** mode is not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **ASP.NET**, click **Session State**.
4. Under **Session State** mode settings, select the **In Process** mode.

IIST-SI-000224: Separate document directory and system files

The IIS 10.0 website document directory must be in a separate partition from the IIS 10.0 websites system files.

To check compliance with IIST-SI-000224, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. In the **Actions** pane, click **Advanced Settings**.
4. Review the Physical Path.

If the **Path** is on the same partition as the OS, your application is not compliant.

Note: If this IIS 10.0 installation supports Microsoft Exchange, and is not otherwise hosting any content, this requirement is not applicable.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. In the **Actions** pane, click **Advanced Settings**.
4. Change the Physical Path to the new partition and directory location.

IIST-SI-000225: Limit the maxURL

The IIS 10.0 website must be configured to limit the maxURL.

To check compliance with IIST-SI-000225, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.

3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **maxUrl** value is not set to 4096 or less, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **maxUrl** value to 4096 or less.

IIST-SI-000226: Limit the size of web requests

The IIS 10.0 website must be configured to limit the size of web requests.

To check compliance with IIST-SI-000226, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **maxAllowedContentLength** value is not explicitly set to "30000000" or less, or a length documented and approved by the ISSO, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **maxAllowedContentLength** value to "30000000" or less.

IIST-SI-000227: Configure the Maximum Query String limit

The IIS 10.0 website's Maximum Query String limit must be configured.

To check compliance with IIST-SI-000227, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **Maximum Query String** value is not set to "2048" or less, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Set the **Maximum Query String** value to 2048 or less.

IIST-SI-000228: Prohibit non-ASCII characters in URLs

Non-ASCII characters in URLs must be prohibited by any IIS 10.0 website.

To check compliance with IIST-SI-000228, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **Allow high-bit characters** option is selected, your application is not compliant.

Note: If this IIS 10.0 installation supports Microsoft Exchange, and is not otherwise hosting any content, this requirement is not applicable.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

Deselect the **Allow high-bit characters** option.

IIST-SI-000229: Prohibit double encoded URL requests

Double encoded URL requests must be prohibited by any IIS 10.0 website.

To check compliance with IIST-SI-000229, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.

If the **Allow double escaping** option is selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Deselect the **Allow double escaping** option.

IIST-SI-000231: Disable directory browsing

Directory Browsing on the IIS 10.0 website must be disabled.

To check compliance with IIST-SI-000231, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Double-click the **Directory Browsing** icon. If Directory Browsing is not installed, this is not applicable.
4. In the **Actions** pane, verify that **Directory Browsing** is **Disabled**.

If the **Directory Browsing** option is not Disabled, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Directory Browsing** icon.
4. In the **Actions** pane, click **Disabled**.

IIST-SI-000233: Modify warning and error messages

Warning and error messages displayed to clients must be modified to minimize the identity of the IIS 10.0 website, patches, loaded modules, and directory paths.

To check compliance with IIST-SI-000233, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Error Pages** icon.
4. Click each error message and then click **Edit Feature** in the **Actions** pane.

If any error message is not set to **Detailed errors for local requests and custom error pages for remote requests**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click the **Error Pages** icon.
4. Click each error message and then click **Edit Feature** in the **Actions** pane.
5. Set each error message to **Detailed errors for local requests and custom error pages for remote requests**.

IIST-SI-000234: Disable debugging and trace information

Debugging and trace information used to diagnose the IIS 10.0 website must be disabled.

Note: If the ".NET feature" is not installed, this check is not applicable.

To check compliance with IIST-SI-000234, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **.NET Compilation**.
4. Scroll down to the **Behavior** section and verify that the value for **Debug** is set to **False**.

If the **Debug** option is not set to **False**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Double-click **.NET Compilation**.
4. Scroll down to the **Behavior** section and set the value for **Debug** to **False**.

IIST-SI-000238: Use a logging mechanism

The IIS 10.0 website must use a logging mechanism configured to allocate log record storage capacity large enough to accommodate the logging requirements of the IIS 10.0 website.

To check compliance with IIST-SI-000238, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. In the **Logging** dialog, determine the **Directory:** that **W3C** logging is being written to.
5. Confirm with your System Administrator that the designated log path is of sufficient size to maintain the logging.
6. Under **Log File Rollover**, verify that **Do not create new log files** is not selected.
7. Verify that a schedule is configured to roll over log files on a regular basis.
8. Consult with your System Administrator to determine if there is a documented process for moving the log files off of the IIS 10.0 web server to another logging device.

If the designated logging path device is not of sufficient space to maintain all log files and there is not a schedule to rollover files on a regular basis, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **IIS**, double-click the **Logging** icon.
4. If necessary, in the **Logging** configuration box, designate a log path to a location able to house the logs.
5. Under **Log File Rollover**, deselect the **Do not create new log files** setting.

IIST-SI-000244: Use TLS to send session IDs

IIS 10.0 website session IDs must be sent to the client using TLS.

To check compliance with IIST-SI-000244, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click the site name.
3. Under **Management**, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **Session** section.
6. Verify if **keepSessionIdSecure** is set to **True**.

If **keepSessionIdSecure** option is not set to **True**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click the website name.
3. Under **Management**, double-click the **Configuration Editor** icon.
4. From the **Section:** drop-down list, select **system.webServer/asp**.
5. Expand the **Session** section.
6. Select **True** for the **keepSessionIdSecure** setting.
7. In the **Actions** pane, click **Apply**.

IIST-SI-000255: Set an application pool recycle time

The application pool for each IIS 10.0 website must have a recycle time explicitly set.

To check compliance with IIST-SI-000255, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Recycling** section.
   e. Expand the **Generate Recycle Event Log Entry** section.
   f. Verify that **Regular time interval** and **Specific time** are set to **True**.

If both the **Regular time interval** and **Specific time** options are not set to **True**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Recycling** section.
   e. Expand the **Generate Recycle Event Log Entry** section.
   f. Set the **Regular time interval** and **Specific time** options to **True**.

IIST-SI-000257: Enable application pool pinging monitor

The application pools pinging monitor for each IIS 10.0 website must be enabled.

To check compliance with IIST-SI-000257, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Process Model** section.
   e. Verify that the value for **Ping Enabled** is set to **True**.

If the value for **Ping Enabled** option is not set to **True**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Process Model** section.

   e. Set the value for **Ping Enabled** to **True**.
   f. Click **OK**.

IIST-SI-000259: Enable application pool rapid fail protection settings

The application pool rapid fail protection settings for each IIS 10.0 website must be managed.

Note: If the IIS Application Pool hosts Microsoft SharePoint, this is not applicable.

To check compliance with IIST-SI-000259, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Open the IIS 10.0 Manager.
2. Click **Application Pools**.
3. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Rapid Fail Protection** section.
   e. Verify that the value for **Failure Interval** is set to **5**.

If the **Failure Interval** option is not set to **5**, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Click **Application Pools**.
3. Complete the following steps for each Application Pool:
   a. Click **Application Pools**.
   b. Highlight an Application Pool.
   c. In the **Action** pane, click **Advanced Settings**.
   d. Scroll down to the **Rapid Fail Protection** section.
   e. Set the value for **Failure Interval** to **5**.
   f. Click **OK**.

IIST-SI-000261: Keep interactive scripts in unique and designated folders

Interactive scripts on the IIS 10.0 web server must be located in unique and designated folders.

To check compliance with IIST-SI-000261, complete the following steps for each site hosted on the IIS 10.0 web server:

1. Determine whether scripts are used on the web server for the target website. Common file extensions include, but are not limited to: .cgi, .pl, .vbs, .class, .c, .php, and .asp.
2. All interactive programs must be placed in unique designated folders based on CGI or ASP script type. For modular and third-party applications, it is permissible to have script files in multiple folders.
3. Open the IIS 10.0 Manager.
4. Click the website name.
5. Click **Explore**.
6. Search for the listed script extensions. Each script type must be in a unique designated folder.

If scripts are not segregated from web content and in their own unique folders, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.

2. Click the website name.
3. Click **Explore**.
4. Search for the listed script extensions.
5. Move each script type to a unique designated folder.
6. Set the following permissions for the script folders:
    - Administrators: FULL
    - TrustedInstaller: FULL
    - SYSTEM: FULL
    - ApplicationPoolId: READ
    - Custom Service Account: READ
    - Users: READ
    - ALL APPLICATION PACKAGES: READ

IIST-SI-000262: Add restrictive access controls for interactive scripts

Interactive scripts on the IIS 10.0 web server must have restrictive access controls.

To check compliance with IIST-SI-000262, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Determine whether scripts are used on the web server for the subject website. Common file extensions include, but are not limited to: .cgi, .pl, .vb, .class, .c, .php, and .asp. If the website does not utilize CGI, this finding is not applicable. All interactive programs must have restrictive permissions.
2. Open the IIS 10.0 Manager.
3. Right-click the website name and click **Explore**.
4. Search for the listed script extensions.
5. Review the permissions of the CGI scripts.
6. Verify that only the following permissions, or more restrictive permissions, are assigned:
    - Administrators: FULL
    - Web Administrators: FULL
    - TrustedInstaller: FULL
    - ALL APPLICATION PACKAGES: Read
    - ALL RESTRICTED APPLICATION PACKAGES: Read
    - SYSTEM: FULL
    - ApplicationPoolId: READ
    - Custom Service Account: READ
    - Users: READ

If the permissions are less, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 10.0 Manager.
2. Right-click the website name and click **Explore**.
3. Search for the listed script extensions.
4. Set the following permissions, or more restrictive permissions, for the CGI scripts:
    - Administrators: FULL
    - Web Administrators: FULL
    - TrustedInstaller: FULL
    - ALL APPLICATION PACKAGES: Read
    - ALL RESTRICTED APPLICATION PACKAGES: Read

- SYSTEM: FULL
- ApplicationPoolId: READ
- Custom Service Account: READ
- Users: READ

IIST-SI-000263: Remove backup interactive scripts

Backup interactive scripts on the IIS 10.0 server must be removed.

To check compliance with IIST-SI-000263 complete the following steps for each site hosted on the IIS 10.0 web server:

1. Determine whether scripts are used on the web server for the subject website. Common file extensions include, but are not limited to: .cgi, .pl, .vb, .class, .c, .php, .asp, and .aspx. The scope of this requirement is to analyze only within the web server content directories, not the entire underlying operating system. If the website does not utilize CGI, this finding is not applicable.
2. Open the IIS 10.0 Manager.
3. Right-click the website name and click **Explore**.
4. Search for the listed script extensions.
5. Search for the following files: *.bak, *.old, *.temp, *.tmp, *.backup, or "copy of...".

If files with these extensions are found, your application is not compliant.

If your application is not compliant, remove the backup files from the production web server.

IIST-SI-000264: Display the required DoD banner page

The required DoD banner page must be displayed to authenticated users accessing a DoD private website.

Note: This requirement is only applicable for private DoD websites.

If a banner is required, the following banner page must be in place:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests, not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

OR

If your system cannot meet the character limits to store this amount of text in the banner, the following is another option for the warning banner: "I've read & consent to terms in IS user agreem't."

Note: While DoDI 8500.01 does not contain a copy of the banner to be used, it does point to the RMF Knowledge Service for a copy of the required text. It is also noted that the banner is to be displayed only once when the individual enters the site and not for each page.

If the access-controlled website does not display this banner page before entry, your application is not compliant.

If your application is not compliant, configure a DoD private website to display the required DoD banner page when authentication is required for user access.

IIS 8.5 Security Technology Implementation Guide

The following sections describe the server and application tasks that you can complete to achieve IIS 8.5 STIG compliance in your BlackBerry AtHoc system.

Server STIG

This section describes the tasks you need to complete to ensure your servers comply with the IIS 8.5 STIG.

IISW-SV-000103: Enable log file and Event Tracing windows

Both the log file and Event Tracing for Windows (ETW) for the IIS 8.5 web server must be enabled.

To check compliance with IISW-SV-000103, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Log file only** option is selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 server name.
3. Click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the **Actions** pane, click **Apply**.

IISW-SV-000107: Sufficient web server log records for location of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish where IIS 8.5 web server events occurred.

To check compliance with IISW-SV-000107, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields**.
6. Verify that the **Service Name** and **Protocol Version** fields are selected.

If the **Service Name** and **Protocol Version** fields are not checked, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the **Service Name** and **Protocol Version** fields.
6. Click **OK**.

7. In the **Actions** pane, click **Apply**.

IISW-SV-000108: Sufficient web server log records for source of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish the source of IIS 8.5 web server events.

To check compliance with IISW-SV-000108, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Click **Select Fields**.
6. Verify that **Server Name** and **Host** are checked.

If the **Server Name** and **Host** fields are not checked, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Format**, select **W3C**.
5. Select the **Server Name** and **Host** fields.
6. Click **OK**.
7. In the **Actions** pane, click **Apply**.

IISW-SV-000110: Sufficient web server log records to establish the outcome of web server events

The IIS 8.5 web server must produce log records that contain sufficient information to establish the outcome (success or failure) of IIS 8.5 web server events.

To check compliance with IISW-SV-000110, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that **Format:** is set to **W3C**.
5. Click **Fields**.
6. Under **Custom Fields**, verify that the following fields are configured:
   - Request Header >> Connection
   - Request Header >> Warning

If any of these fields are not configured, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Verify that **Format:** under **Log File** is set to **W3C**.
5. Click **Fields**.
6. Select the following custom fields:
   - Request Header >> Connection

- Request Header >> Warning

7. Click **OK**.
8. In the **Actions** pane, click **Apply**.

IISW-SV-000111: Sufficient web server log records to establish identity

The IIS 8.5 web server must produce log records that contain sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SV-000111, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the format is set to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, verify that **User Agent**, **User Name**, and **Referrer** are selected.
7. Under **Custom Fields**, verify that the following fields are selected:

   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type

If any of these fields are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 web server IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log File**, verify that the format is set to **W3C**.
5. Select **Fields**.
6. Under **Standard Fields**, select **User Agent**, **User Name**, and **Referrer**.
7. Under **Custom Fields**, select the following fields:

   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type

8. Click **OK**.
9. In the **Actions** pane, click **Apply**.

IISW-SV-000112: Web server must use Event Tracing for Windows logging option

The IIS 8.5 web server must use the Event Tracing for Windows (ETW) logging option.

To check compliance with IISW-SV-000112, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Verify that the **W3C** format is selected for **Log File**.
5. Verify that the **Both log file and ETW event** log event destination option is selected.

If the **W3C** or the **Both log file and ETW event** options are not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. For the **Log File**, select **W3C** from the **Format** list.
5. For **Log Event Destination**, select the **Both log file and ETW event** option.
6. In the **Actions** pane, click **Apply**.

IISW-SV-000120: Samples, examples, and tutorials must be removed from production server

All IIS 8.5 web server sample code, example applications, and tutorials must be removed from a production IIS 8.5 server.

To check compliance with IISW-SV-000120, complete the following steps:

1. Navigate to the **inetpub\** folder.
2. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.
3. Navigate to the `Program Files\Common Files\System\msadc` folder.
4. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.
5. Navigate to the `Program Files (x86)\Common Files\System\msadc` folder.
6. Check for any executable sample code, example applications, or tutorials that are not explicitly used by a production website.

If any of the folders or sub folders above contain any executable sample code, example applications, or tutorials that are not explicitly used by a production website, your server is not compliant.

If your server is not compliant, remove any executable sample code, example applications, or tutorials that are not explicitly used by a production website.

IISW-SV-000124: Web server must have MIMEs that invoke OS shell programs disabled

The IIS 8.5 web server must have Multipurpose Internet Mail Extensions (MIMEs) that invoke OS shell programs disabled.

To check compliance with IISW-SV-000124, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by** list, select **Content Type**.
5. Click **Select Fields**.
6. Under **Application**, verify that the following MIME types for OS shell program extensions have been removed from the list of extensions:
   - .exe
   - .dll
   - .com
   - .bat
   - .csh

If any of these OS shell MIME types are configured, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.

3. Under **IIS**, double-click the **MIME Types** icon.
4. Select **Content Type** from the **Group by:** list.
5. Under **Application**, remove the following MIME types for OS shell program extensions from the list of extensions:
   - .exe
   - .dll
   - .com
   - .bat
   - .csh
6. In the **Actions** pane, click **Apply**.

IISW-SV-000146: Web server must not impede ability to write log record content to an audit log

The IIS 8.5 web server must not impede the ability to write specified log record content to an audit log server.

To check compliance with IISW-SV-000146, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Under **IIS**, double-click the **Logging** icon.
4. Select the **Both log file and ETW event** option.
5. In the **Actions** pane, click **Apply**.

IISW-SV-000153: Web server must maintain the confidentiality of controlled information during transmission

An IIS 8.5 web server must maintain the confidentiality of controlled information during transmission through the use of an approved TLS version.

To check compliance with IISW-SV-000153, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Access an administrator command prompt.
4. Type **regedit<enter>** to access the registry of the server.
5. Navigate to the following registry paths:
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server`
6. Verify that **DisabledByDefault** has a REG_DWORD value of **0**.
7. Navigate to the following registry paths:
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server`

   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server`
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server`
8. Verify that **DisabledByDefault** has a REG_DWORD value of **1**.

If any of the listed registry paths do not exist or are configured with the incorrect value, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 web server name.
3. Access an administrator command prompt.
4. Type **regedit<enter>** to access the registry of the server.
5. Navigate to the following registry paths:
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server`
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server`
6. Set the **DisabledByDefault** REG_DWORD value to **0**.
7. Navigate to the following registry paths:
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server`
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server`
   - `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server`
8. Set the **DisabledByDefault** REG_DWORD value to **1**.

IISW-SV-000154: Web server must maintain the confidentiality of controlled information during transmission

The IIS 8.5 web server must maintain the confidentiality of controlled information during transmission through the use of an approved TLS version.

To check compliance with IISW-SV-000154, complete the following steps:

1. Review the web server documentation.
2. Review the web server deployed configuration.
3. Determine which version of TLS is being used.

If the TLS version is not an approved version according to NIST SP 800-52 or to the non-FIPS-approved enabled algorithms, your server is not compliant.

If your server is not compliant, complete the following steps:

1. Configure the web server to use an approved TLS version according to NIST SP 800-52.
2. Disable any non-approved TLS versions.

Application STIG

This section describes the tasks you need to complete to ensure your application complies with the IIS 8.5 STIG.

IISW-SI-000206: Enable log file and Event Tracing windows

Both the log file and Event Tracing for Windows (ETW) for each IIS 8.5 website must be enabled.

To check compliance with IISW-SI-000206, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, verify that the **Both log file and ETW event** option is selected.

If the **Both log file and ETW event** option is not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Under **IIS**, double-click the **Logging** icon.
4. Under **Log Event Destination**, select the **Both log file and ETW event** option.
5. In the **Actions** pane, click **Apply**.

IISW-SI-000209: Sufficient website log records to establish identity

The IIS 8.5 website must produce log records containing sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SI-000209, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under **Log File**, verify that the **Format:** field is configured to **W3C**.
4. Click **Fields**.
5. Under **Standard Fields**, verify that the **User Agent**, **User Name**, and **Referrer** fields are selected.
6. Under **Custom Fields**, verify that the following fields are selected:
    - Server Variable >> HTTP_USER_AGENT
    - Request Header >> User-Agent
    - Request Header >> Authorization
    - Response Header >> Content-Type

If any of the above fields are not selected, your application is not compliant.

If your application is not compliant, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under **Log File**, set the **Format:** field to **W3C**.
4. Click **Fields**.
5. Under **Standard Fields**, select the **User Agent**, **User Name**, and **Referrer** fields.
6. Under **Custom Fields**, select the following fields:
    - Server Variable >> HTTP_USER_AGENT
    - Request Header >> User-Agent
    - Request Header >> Authorization
    - Response Header >> Content-Type

7. Click **OK**.
8. In the **Actions** pane, click **Apply**.

IISW-SI-000210: Sufficient website log records to establish identity

The IIS 8.5 website must produce log records containing sufficient information to establish the identity of any user, subject, or process associated with an event.

To check compliance with IISW-SI-000210, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Under **Log File**, verify that the **Format:** field is configured to **W3C**.
4. Click **Fields**.
5. Under **Standard Fields**, verify that the **User Agent**, **User Name**, and **Referrer** fields are selected.
6. Under **Custom Fields**, verify that the following fields are selected:
   - Server Variable >> HTTP_USER_AGENT
   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type

If any of the above fields are not selected, your application is not compliant.

If your application is not compliant, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 web server IIS 8.5 Manager.
2. Under **IIS**, double-click the **Logging** icon.
3. Click the **Logging** icon.
4. Under **Log File**, set the **Format:** field to **W3C**.
5. Click **Fields**.
6. Under **Standard Fields**, select the **User Agent**, **User Name**, and **Referrer** fields.
7. Under **Custom Fields**, select the following fields:
   - Server Variable >> HTTP_USER_AGENT
   - Request Header >> User-Agent
   - Request Header >> Authorization
   - Response Header >> Content-Type
8. Click **OK**.
9. In the **Actions** pane, click **Apply**.

IISW-SI-000211: Website must use Event Tracing for Windows logging option

The IIS 8.5 web server must use the Event Tracing for Windows (ETW) option.

To check compliance with IISW-SI-000211, complete the following steps for each website hosted on the IIS 8.5 web server.

1. Open the IIS 8.5 IIS Manager.
2. Select the website to review.
3. In the **IIS** section, double-click the **Logging** icon.
4. Verify that the **W3C** format is selected for **Log File**.
5. Verify that the **Both log file and ETW event** log event destination option is selected.

If the **W3C** or the **Both log file and ETW event** options are not selected, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Select the website to update.
3. In the **IIS** section, double-click the **Logging** icon.
4. For the **Log File**, select **W3C** from the **Format** list.
5. For **Log Event Destination**, select the **Both log file and ETW event** option.
6. In the **Actions** pane, click **Apply**.

IISW-SI-000214: Website must have MIMEs that invoke OS shell programs disabled

The IIS 8.5 website must have Multipurpose Internet Mail Extensions (MIMEs) that invoke OS shell programs disabled.

To check compliance with IISW-SI-000214, complete the following steps on each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 website.
3. Under **IIS**, double-click the **MIME Types** icon.
4. From the **Group by** list, select **Content Type**.
5. Click **Select Fields**.
6. Under **Application**, verify that the following MIME types for OS shell program extensions have been removed from the list of extensions:

    - .exe
    - .dll
    - .com
    - .bat
    - .csh

If any of these OS shell MIME types are configured, your application is not compliant.

If your application is not compliant, complete the following steps:

1. Open the IIS 8.5 IIS Manager.
2. Click the IIS 8.5 website.
3. Under **IIS**, double-click the **MIME Types** icon.
4. Select **Content Type** from the **Group by:** list.
5. Under **Application**, remove the following MIME types for OS shell program extensions from the list of extensions:

    - .exe
    - .dll
    - .com
    - .bat
    - .csh
6. In the **Actions** pane, click **Apply**.

IISW-SI-000228: Non-ASCII characters in URLs must be prohibited

Non-ASCII characters in URLs must be prohibited by any IIS 8.5 website.

To check compliance with IISW-SI-000228, complete the following steps:

1. Open the IIS 8.5 Manager.

2. Click website name.
3. Double-click the **Request Filtering** icon.
4. In the**Actions** pane, click **Edit Feature Settings**.
5. Verify that the **Allow high-bit characters** check box is not selected.

If the **Allow high-bit characters** check box is selected, your application is not compliant.

Note: If the website has operational reasons to set **Allow high-bit characters**, this vulnerability can be documented locally by the ISSM/ISSO.

If your application is not compliant, complete the following steps for each site hosted on the IIS 8.5 web server:

1. Open the IIS 8.5 Manager.
2. Click the website name.
3. Double-click the **Request Filtering** icon.
4. In the **Actions** pane, click **Edit Feature Settings**.
5. Deselect the **Allow high-bit characters** check box.

Verifying BlackBerry AtHoc is operational

After you complete a new installation or upgrade of BlackBerry AtHoc, a thorough test of functionality should be performed to ensure that the system operates properly. This chapter presents a set of test procedures that cover the most important system functions.

Basic BlackBerry AtHoc test procedures

The following tables provides detailed instructions on the basic BlackBerry AtHoc test procedures.

Log in

√	Description	Expected result
	Open a browser, and navigate to the Management System application. To do this, navigate to the `<AtHoc-ENS-URL>`. For example, `https://alerts.company.com` (if SSL is used).	The login page displays.
	Log in as an administrator.	The BlackBerry AtHoc management system home page displays.
	In the navigation bar, click ⚙.	—

Connect a client

√	Description	Expected result
	Install a desktop software client, as described in the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.	The desktop software is installed on the user's computer and the user appears in the User manager.

Custom attributes

√	Description	Expected result
	Open the BlackBerry AtHoc management system. In the navigation bar, click ⚙.	—
	Click **Users** > **User Attributes**. On the **User Attributes** page, click **New**.	—
	Create a multi-select picklist attribute whose Attribute Name is **Test**.	—
	Assign two pick-list values to the Test attribute: **T1** and **T2**.	—

√	Description	Expected result
	Click **Save** to create the pick list attribute.	A pick list attribute named **Test** is created.
	Create a number attribute named **ID**.	A number attribute named **ID** is created.
	Create a text attribute named **Comments**.	A text attribute named **Comments** is created.
	Select the pick list attribute named **Test** and click **Delete**.	The **Test** attribute is deleted.

Hierarchy editing

√	Description	Expected result
	In the navigation bar, click ⚙.	The Settings page opens.
	From the **Settings** page, in the **Users** section, click **User Attributes**.	The User Attributes screen opens.
	On the **User Attributes** screen, select the attribute that is of the Type **Path**.	The Organizational Hierarchy settings page opens.
	In the **Values** section, add or delete a node.	—
	Click **Save**.	A Success message is displayed.
	In the navigation bar, click ⚙.	The Settings page opens.
	From the **Settings** page, in the **Users** section, click **Distribution List Folders**.	The Distribution List Folders screen opens.
	On the **Distribution List Folders** screen, add or delete a node.	—
	Click **Save**.	A success message is displayed.

Distribution lists

√	Description	Expected result
	In the navigation bar, click **Users**. Click **Distribution Lists**.	—
	Create a static list named **Stat1** and add your user ID as a member.	The **Members** field displays **1**.
	Create a dynamic list named **Dyn1** and add a criteria that includes your user ID in the results.	—

Import or export users

√	Description	Expected result
	In the navigation bar, click the **Users** > **Users**.	The **Users** page opens.
	Click **More Actions** > **Import** > **Users**.	—
	Download a template .csv file. An Excel spreadsheet opens and must (if new install) contain only the selected User ID.	**Note:** Excel must be installed on your computer. If you do not have Excel, use Notepad to view the .csv file content. The file must contain all static lists, custom attributes, and devices.
	Fill in all required fields.	—
	Save the file with the name `test.csv`.	—
	Return to the management system and continue from the **Import User File** page.	—
	Select the import .csv file: **1.** Click **Browse**. **2.** In the file selection dialog, navigate to and select the `test.csv` file. **3.** Right-click and select **Open with** to confirm the selection of the file. **4.** Click **Open**. **5.** Click **Import**.	The Import User Progress window opens and all users are successfully processed. The **Last import** field displays the correct date and time of the import.
	Click **Download Log** and in the **File Download** dialog, select **Open**.	An Excel spreadsheet opens and displays all the users from the .csv file. The AtHoc Import Result column contains the value *OK* and each user has a unique user ID.
	Compare the Users list with the import .csv file. To open the .csv file: **1.** From the **Users** page, click **More** > **Actions** > **Import** > **Users**. **2.** Click **Browse** and open the import .csv file.	An Excel spreadsheet opens and contains the current user and the users that were imported.
	In the navigation bar, click **Users** > **Users**.	All qualified users display in the table.
	Spot check users to verify that the correct details have been imported.	The details pane at the bottom of the screen displays the correct information for the selected end user.

Alert templates

√	Description	Expected result
	In the navigation bar, click **Alert** > **Alert Templates**.	The Alert Templates page opens.
	Click **New**.	The New Alert Template screen opens.
	Create an alert template named **SC1**.	—
	For the new template: **1.** Select **Available for Quick Publish**. **2.** Add the title and body. **3.** Add a response option. **4.** Target one or more users. **5.** Select delivery to the following device: Desktop popup. **6.** Check spelling.	—
	Save the alert template.	An alert template named **SC1** is created.

Alert publishing

√	Description	Expected result
	In the navigation bar, click **Alerts** > **New Alert**.	The Select from Alert Templates page opens.
	Publish an alert template: **1.** Select the **SC1** alert template and click **Edit**. **2.** In the **Target Users** section, click review the users in the Targeting Summary. **3.** Click **Review and Publish**. **4.** Click **Publish**.	All qualified users are targeted. The Sent Alerts list displays the published alert with a Live status. If the status is still Scheduled, wait 15 seconds and re-select **Sent Alerts** to refresh the display. The status must be live in no more than 15 seconds from template activation.
	Wait up to two minutes for the alert to arrive on the users desktop. After you receive the pop-up, click **Acknowledge and Close**.	The desktop pop-up displays and an audio alert plays (if speakers are connected and audio is enabled). Upon acknowledgment, the pop-up must disappear.

Self Service

√	Description	Expected result
	From the user's computer, right-click the AtHoc desktop software system tray icon (🪐) and select **Access Self Service**. For Mac users, left-click to open the status item menu.	A new browser window displays the Self Service Inbox which contains the newly published alert (but only if the user authentication is set to Auto\Windows authentication.) (Mac) The Safari browser is launched for any service selected from the status item menu.
	Navigate through the other Self Service tabs and verify that the displayed information is correct.	The published alert appears in the list with a Live status.

Alert tracking reports

√	Description	Expected result
	In the navigation bar, click **Alert** > **Sent Alerts**.	The published alert appears in the list with a Live status.
	Hover the pointer over the published alert. The tool tip displays the title body and responses. Click the alert to open the details.	You can see the Delivery Summary, which lists the number of targeted users, the number of Sent to users, and the number of users who acknowledged the alert. You can also see a drop–down list of detail reports.
	Click **Export** > **Export Full Report**. Note that you must have Excel 2003 or higher installed on your computer to open the report.	You are asked to open the .csv file. The Detailed Alert tracking report must open and display the alert details and track information. You can see the users who received and acknowledged the alert.

Audio files

√	Description	Expected result
	In the navigation bar, click ⚙.	—
	In the **Basic** section, click **Audio Files**.	The Audio Files page opens.
	Click **New**.	The New Audio File dialog opens.
	Enter an audio name and upload a .wav file that is larger than 1 MB but not more than 2 MB.	**Note:** You can record a .wav file using the Windows Sound Recorder (Start / Programs / Accessories / Entertainment / Sound Recorder.) A voice recording of 30 seconds must be 1 MB. After you record a voice, save it using **File** > **Save As**.

√	Description	Expected result
	After selecting the file to be uploaded, click **Save**.	# Return to Audio Files.

Error logs

√	Description	Expected result
	Check the Windows application event log and the AtHocEventViewer on the application server.	You must not see any unexplained errors in the log.

Extended BlackBerry AtHoc test procedures

√	Description	Expected result
	Perform detailed end user search.	
	Publish an alert targeted to a static list.	
	Publish an alert targeted to a dynamic list.	
	Publish an alert with different device preference options.	
	Create an operator with a user base.	
	Create, enable, disable, and delete an alert folder.	
	Manually create a new user and assign a custom attribute.	
	End a published alert.	
	Check navigation.	

Appendix A: Troubleshooting

Error code: None
Message: The installation stops because the following prerequisites are missing on the server. Install these components first: *<List of Missing Prerequisites>*
Cause: The listed prerequisites are not installed.
Resolution: Install the missing prerequisites.

Error code: 2147217900
Message: No additional message
Cause: During a new installation, the `ngad` user password does not meet Microsoft SQL Server password requirements.
Resolution: Do not use the default password for `ngad` Enter a custom password that meets the strong password requirement of Microsoft SQL Server.

Error code: 2147217900
Message: The operating system returned the error "5(Access is denied." while attempting to "restoreContaininer::ValidateTargetForCreation" on <path>."
Cause: Microsoft SQL Server service account does not have permission to create files.
Resolution: Change the service account to “Local System account.”

Error code: 2147217900
Message: No additional message
Cause: The transaction log for database NGADDATA is full.
Resolution: Shrink the NGADDATA database and back up the transaction log.

Error code: 2147217900
Message: No additional message
Cause: The Application server logon account did not have a logon on the Database server, or did not have a Microsoft SQL Server logon with system administrator rights.
Resolution: Grant the correct permissions or switch to an account that has the correct permissions.

Error code: 2147217900
Message: 3a CreateUsers Error running ATH_CREATE_USERS sp: error -2147217900, exec dbo.ATH_DROP_USERS @dropLogin = 1
Cause: Microsoft SQL Server is configured to require strong passwords, and the user chose to use the default password for the ngad database user, which does not meet strong password requirements.
Resolution: Do not use the default password for ngad. Enter a custom password that meets the strong password requirement of Microsoft SQL Server.

Error code: 2147319779
Message: Library not registered
Cause: `Scrrun.dll` is not registered. This error occurs when one of the custom actions executes a `CreateObject` on `Scripting.FileSystemObject`. This error occurs on some locked down systems.
Resolution: Register the 32-bit version of `scrrun.dll`.

Error code: 2147467259
Message: Unspecified error
Cause: A connection to the database server could not be made and returns the COM error code: E_FAIL "Unspecified error", which is a generic return code when a COM method call fails.
Resolution: Make sure that the Microsoft SQL Server service is running or call BlackBerry AtHoc customer support.

Appendix B: Organization duplicator object management

This section describes the objects that are copied during a single or cross-system duplication. Some objects are not duplicated depending on the type of the source organization or the account type.

The following tables describe objects that are duplicated to the organization on the target server.

Feature: Server configuration
Objects: • Cascading systems • Images • Gateways and devices • Health monitors (Actions only, not Global Health Monitors.)
Duplicates across servers: • Enterprise/sub (from SRC/SRC) • Basic (from SRC)

Feature: System Setup (Organization 3)
Objects: • Attributes • Channels
Duplicates across servers: • Enterprise/sub (from SRC/SRC) • Basic (from SRC)

Feature: Standard Organization Configuration
Objects: • Provider configuration • Page layouts • Buttons • Gateways and devices • Standard hierarchy (Org hierarchy, DL hierarchy, Emergency Community) • Standard DLs (Auto delete users, auto disable users) • Alert templates • Maps and layers
Duplicates across servers: • Enterprise/sub (from SRC/SRC) • Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Attributes
- Channels
- Audio
- Templates
- Mass devices
- Custom DLs (Except static list user membership [see Users].)
- Alert templates (Except targeting of individual users [see Users].)
- Reports
- Schedules

Duplicates across servers:

- Enterprise/sub (from SRC/SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Operator permissions
- Users, their DL memberships, and targeting (Organization users, Static DL user membership, alert templates individual user targeting)

Not duplicated across servers:

- Enterprise/sub (from SRC/SRC)
- Basic (from SRC)

The following tables describe objects that are created on the source server for a new organization, or duplicated to a new organization on the same server.

Feature: Server configuration

Objects:

- Cascading systems
- Images
- Gateways and devices
- Health monitors (Actions only, not Global Health Monitors.)

Feature: Server configuration

Not created on the same server:

- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Not duplicated on the same server:

- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: System setup (Organization 3)

Objects:

- Attributes
- Channels

Not created on the same server:

- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Not duplicated on the same server:

- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Standard organization configuration

Objects:

- Provider configuration
- Page layouts
- Buttons
- Gateways and devices
- Standard hierarchy (Org hierarchy, DL hierarchy, Emergency Community)
- Standard DLs (Auto delete users, auto disable users)
- Alert templates
- Maps and layers

Feature: Standard organization configuration

Created on the same server:

- Enterprise (from 5)
- Sub (from ENT)
- Basic (from 6)

Duplicated on the same server:

- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Attributes
- Channels
- Audio
- Templates
- Mass devices
- Custom DLs (Except static list user membership [see Users].)
- Alert templates
- Reports

Created on the same server:

- Enterprise (from 5)
- Basic (from 6)

Not created on the same server:

- Sub (from ENT)

Duplicated on the same server:

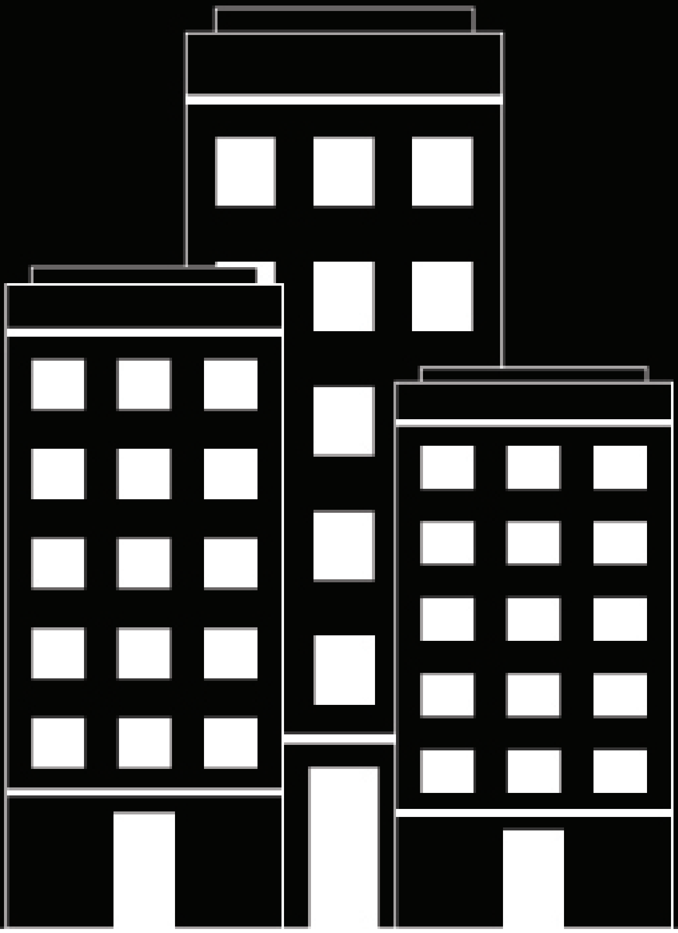
- Enterprise (from SRC)
- Sub (from SRC)
- Basic (from SRC)

Feature: Custom organization configuration

Objects:

- Users, their DL memberships and targeting (Organization users, static DL user membership, alert templates, individual user targeting)

Feature: Custom organization configuration
Not created on the same server: • Enterprise (from 5) • Sub (from ENT) • Basic (from 6) **Not duplicated on the same server:** • Enterprise (from SRC) • Sub (from SRC) • Basic (from SRC)



BlackBerry AtHoc

Plan and Manage Enterprise Organizations

7.16

Contents

Getting Started

This document contains information about enterprise concepts, uses, planning, and implementation. It assumes you have detailed knowledge of the BlackBerry® AtHoc® management system, including implementation, user management, and alert management for stand-alone organization configurations.

To learn about the BlackBerry AtHoc management system, see the BlackBerry AtHoc documentation available at: https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc.

Enterprise management overview

You can use the enterprise configuration in BlackBerry AtHoc to manage alerts for a large, complex group of users. Using the enterprise configuration, you can delegate alerting to the organizations, while you maintain critical, unified alerting policies and processes for the enterprise and its members.

This document discusses the basics of BlackBerry AtHoc enterprise configuration and explains how to plan and implement one.

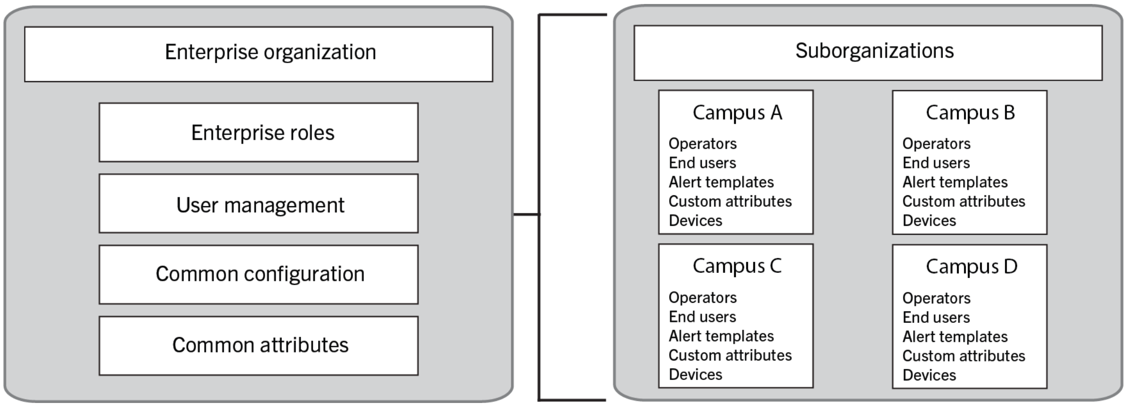
The following topics are covered:

- Enterprise concepts and benefits
- The differences between using an enterprise or stand-alone configuration
- Integration of AtHoc Connect to improve communication between organizations inside or outside the enterprise
- Tips for migrating your existing organizations to an enterprise configuration or creating an enterprise from scratch
- Enterprise role and permissions management
- User management for enterprise configurations
- Alert publishing in the enterprise

What is an enterprise configuration?

An enterprise configuration is a set of BlackBerry AtHoc organizations in one system that are managed by a single parent organization called the enterprise organization.

The enterprise organization centralizes the user, content, and policy management of its suborganizations.



User accounts are created in suborganizations, but the enterprise provides a higher-level view. The enterprise also manages common content such as user attributes, audio files, and delivery templates.

The enterprise configuration uses a hierarchy to control the flow of information and centralize management tasks for organizations in the same system. The enterprise organization has one or more suborganizations that are defined by location or purpose. The suborganizations inherit certain configuration settings from the enterprise organization, while the enterprise manages users and provides a way to send alerts to multiple organizations across the enterprise.

Single organization configuration

Many BlackBerry AtHoc customers have found that their configurations are becoming too complex.

A single organization configuration can become unwieldy, with distribution lists and user accounts that are difficult to manage and synchronize as users come and go or business units change. Users suffer from too many alerts or fail to get any at all. Additionally, operators can find it difficult to use the Connect network effectively, especially if they are separated geographically. While each location would like to connect with certain neighboring agencies or companies, local alerts from these neighbors show up in everyone's inbox, at times creating an information overload.

Example A

A federal agency has developed one very large organization. Thousands of end users are targeted for various alerts ranging from daily status, emergency drills, or live emergencies. Despite having a flexible system, complex configurations make it difficult to ensure that operators have the correct permission to target only the people they should.

This agency can use the enterprise configuration to better organize personnel into smaller organizations with local administrators to manage user permissions and contact information.

Multiple organizations are great for many sites or regions, can have unique configurations for a location, delegate user management to organization administrators, and can separate distinct functions. However, using multiple organizations loses the benefit of a consolidated view of your operations. It is more difficult to have consistent and centralized communication across all organizations. Independent organizations are harder to maintain, require duplicate configuration effort, and do not have a good way to communicate with each other. Additionally, maintaining consistent user attributes, templates, and distribution lists is impossible because too much customization is occurring in each organization. Finally, individual organizations can communicate using Connect, but there is no easy way to communicate across all organizations, or with subsets of an organization.

Example B

A military organization has many bases around the world. The organization has created one organization for each base, which has thousands of personnel with rotating assignments and changing permissions (best managed by local administrators). However, with over 50 bases and hundreds of thousands of personnel, the senior leadership cannot effectively alert all bases in a consistent way or alert just the required subset of each base (such as by function). They can not determine, from a single view, who is available and where they are located.

During a major emergency, this military branch cannot account for personnel, send alerts to multiple bases at once, or effectively manage distribution lists that need to span organizations. They need a consistent way to target personnel across all organizations in the system and for those personnel to provide their location and status.

Enterprise configuration

To help large organizations, BlackBerry AtHoc provides the enterprise configuration. Enterprise configuration centralizes communication for multiple organizations, while using inheritance to provide consistent policies and procedures. Alerts can be sent from the enterprise organization to all organizations or subsets of suborganizations.

The enterprise configuration works with AtHoc Connect, allowing suborganizations to communicate with each other and outside organizations, such as vendors or community agencies.

Customers that have a standalone organization with too many users and distribution lists can create multiple suborganizations based on common alerting needs. The enterprise configuration allows you to delegate user management to local organizations, while maintaining the centralized control and communication that the single organization provided.

Example A

A federal agency with an unwieldy single organization can migrate to an enterprise configuration by breaking the large organization into small organizations that represent each geographical location. With multiple locations, the federal agency creates an organization for each alerting region, while retaining the ability to alert all users.

The federal agency also has manageable user bases that operators can maintain locally. The smaller suborganizations makes it easier to manage user contact information and distributions lists. Each suborganization can use AtHoc Connect to communicate with each other or to invite local vendors and community agencies to join AtHoc Connect without impacting the larger enterprise with connect requests and incoming alerts.

With an enterprise configuration, customers that have multiple organizations can have a virtual view of all personnel and consolidate and centralize communication and alert consistency. Enterprises can keep the benefit of multiple organizations, such as user management at the local suborganization.

Example B

A military branch has over 50 organizations, one for each base. To migrate to an enterprise configuration, they implement the following changes:

- They migrate to a configuration that uses three enterprise organizations, one for each continent on which they have bases. They use three enterprises because the emergency alerting for each continent is managed by a different team of people and each continent has different configuration needs.
- All enterprises are in the same system, so that any common content in System Setup can be inherited by the enterprise organizations.
- For each enterprise, they have about five enterprise administrators (EA) and 10 enterprise operators (EO) who can publish alerts to all or parts of the enterprise. At least one EO can access each of the three enterprises.
- Each enterprise organization has suborganizations for each base on that continent.
- Operators can create customized common content for bases on each continent (such as content in additional languages) at the enterprise level. Suborganizations inherit the common content.

Alerts can be sent from the enterprise organization, while personnel in the system can be accounted for by tracking responses to alerts.

The consolidated view provides the leadership with useful personnel accountability information for each continent from their respective enterprise.

Each suborganization can use AtHoc Connect to communicate with their peer suborganizations and affiliates of the organization such as vendors and local governments.

If there is a hurricane on the East coast of the U.S., they can publish alerts to only the appropriate North American alerting regions and ask for responses to check on personnel location, safety status, and availability to assist with recovery. Each base can then alert their Connect affiliates and assess their status.

Does enterprise solve my problems?

The hierarchy enables the enterprise to delegate user management, while maintaining critical unified alerting policies and processes. The enterprise configuration answers the following questions for many customers:

Question	Answer
Can I have a single user interface for managing all of my users?	Yes you can perform the following types of management from the enterprise organization: • Manage user accounts • Filter and search • Create enterprise distribution lists • Create reports

Question	Answer
Can I manage operators across my entire system efficiently?	Yes, you can create enterprise operators that have permission to publish alerts to all or parts of the enterprise. You can also limit the ability of operators to publish to only their local organization.
Can I overcome cumbersome cascading configurations for communicating with other organization or outside affiliates?	Yes, you can use AtHoc Connect at the suborganization level for peer-to-peer alerting or for connecting with outside affiliates.
Can my users in one suborganization move to another organization efficiently?	Yes, you can set the "Enterprise Features" flag in the General Settings of the enterprise organization to enforce uniqueness of users in the enterprise and suborganizations. This enables users to move between suborganizations using the same Self Service URL, login credentials, and the same organization code in the BlackBerry AtHoc Desktop App.

When should I use an enterprise configuration?

Planning your configuration is essential whether you are a small or large organization. You must consider which user roles, security policies, user base size, and content are common to all organizations and whether they need to be centralized by using enterprise alerting, user, and content management.

Enterprise configurations are generally for large, complex implementations with multiple locations that need to segment end users. Small groups find it easier to manage user bases with one or more standalone organizations. The following table compares the use of a standalone organization, multiple standalone organizations, and enterprises with suborganizations.

Setup	Standalone organization	Multiple standalone organizations	Enterprise with suborganizations
Advantages	• Best for one geographic site • Lowest up-front cost • One-time configuration of common content and settings • Import users once	• Best for multiple sites or regions • Delegate user management to administrators • Unique configurations by location • Distinct operations per site • Works with AtHoc Connect	• Shared configuration between organizations • Centralized user views • Alerting of enterprise users • All the benefits of multiple organizations • Works with AtHoc Connect • Alert folder restrictions are not inherited from one organization to another

Setup	Standalone organization	Multiple standalone organizations	Enterprise with suborganizations
Disadvantages	• Difficult to manage operator permissions • Hard to separate team operations • Harder to implement AtHoc Connect effectively	• Hard to maintain multiple configurations and consistency • Requires duplicate effort for entity configuration and security policies • No central user management or alerting between peer organizations • Users that move between sites have to re-enter profile information • Hard to manage personnel accountability	• Migration can be complex • Device configuration is not inherited • Some stand-alone features not available on the enterprise

What can I do in the enterprise?

Now that you've seen the primary pros and cons for standalone and enterprise organizations, let's delve more deeply into how things work in the enterprise organization.

Enterprise user management

The enterprise organization provides a central view of all users in the organization. The enterprise administrator manages users at the enterprise level, and is able to grant or revoke operator permissions to the enterprise, as well as create or modify any user account.

You can view all users on the Users screen when you are logged in to the enterprise organization. To identify which organization the user account was created in, you can add the Organization column. This column is based on the Enterprise attribute of the same name and exists only in the enterprise organization. To learn more about enterprise user management, see Manage users in the enterprise and Manage roles and permissions.

Enterprise publishing

To help with consistency across organizations, users with any alert publishing roles for the enterprise organization can create and publish enterprise alert templates. When they are logged in to the enterprise organization, users with alert publishing roles create the templates. Enterprise alert templates are most effective for targeting users in multiple suborganizations. Alert templates are not inherited by suborganizations.

Using enterprise attributes, the operator can create common dynamic distribution lists, custom alert responses, and reports. Creating user attributes from the enterprise organization makes them available for publishing enterprise-wide alerts and ensures that operators in each suborganizations can also use them.

While logged into the enterprise organization, operators can publish alerts that target users from multiple suborganizations. Targeting works very similarly to stand-alone organizations, except that operators can see users in all suborganizations to which they have access. When filling out the user targeting section of the alert, the operator can select any user or group to which they have access through their user base. Use the "Organization" attribute to target users in suborganizations.

AtHoc Connect for peer-to-peer organization alerts

Enterprise is great for targeting users within the enterprise. However, AtHoc Connect is best for communication between suborganizations or outside entities, without targeting individuals. For example, if a site in a federal agency has an IT outage, they can alert other organizations and ask if they have been affected.

You might already be using AtHoc Connect to communicate with outside agencies. You can also enable alerting between organizations in the enterprise with AtHoc Connect. Each suborganization registers for AtHoc Connect and then invites the other organizations in the enterprise to join their network. Operators can then send alerts to their peer organizations, just like they would for outside agencies.

Note: You do not target individuals in another organization through AtHoc Connect. The other organization would need to set up incoming alert rules that publish an alert targeting an individual.

Manage common content with inheritance

One of the main advantages of an enterprise configuration is the ability to create common content or configuration settings in one place and push them down to subordinate organizations. This is known as "inheritance".

There are three levels of inheritance.

- **System**: This is the top level that is used for the entire BlackBerry AtHoc system. A a system is defined as a single installation of BlackBerry AtHoc accessed by a single URL. An example of a system user attribute is First Name. All users have the First Name attribute, no matter what organization or enterprise they belong to. System configuration is set in the System Setup (3) organization.
- **Enterprise**: This is the second level of inheritance, primarily used for content and settings that need to be the same across all suborganizations. An example is a user attribute called employeeID. By setting this attribute at the enterprise level, the content is part of all user profiles that are in the organization managed by the enterprise.
- For Cloud configurations, content and settings are set in the enterprise, which allows the cloud to use multitenancy.
- **Suborganization**: This is the third level, primarily used for content that is specific to a single base or location. An example is the user attribute OptIn4Birthdays, which is used by only one organization.

Security policies are also frequently handled as common content, allowing them to be inherited so that consistent policies, procedures, and communication methods can be established across a system.

Example

The following example focuses on attributes, but it also applies to any type of common content.

A federal agency has three organizations managed by a single enterprise. There are three tiers, including one called System Setup at the system level. The enterprise organization is named Fed_Agency_Enterprise and it has three suborganizations: East Coast, Mid-West, and West Coast.

The organizations have the following user attributes:

- *System Setup* has three user attributes that are available for the system, which includes all enterprise and suborganizations: `UserName`, `ID`, and `LastName`.
- *Fed_Agency_Enterprise* has three user attributes that are available for the enterprise and its suborganizations: `Department`, `Location`, and `CPR-Trained`.
- The *East Coast* organization has a team that wants to track birthdays, so they have added an attribute called `OptIn4Birthdays`.

An operator in the suborganization can edit the value of an attribute for a user if the operator has access to the organization in which the user attribute was created.

- The system administrators on System Setup can access and edit user attributes created at the System level. In this example, they can target users through the `UserName`, `ID`, and `LastName` attributes. However, they cannot see any attributes defined at lower levels.
- Enterprise operators have more options. They can view and use all of the attributes inherited from the System level, plus publish, search, create reports, and edit the attributes created in that enterprise organization (`Department`, `Location`, and `CPR-Trained`).
- Operators in the suborganizations can use but not edit user attributes inherited from system and enterprise levels. These operators can also create, use, and edit user attributes for publishing to the local organization. However, operators do not have access to attributes from peer organizations. As a result, operators in the *East Coast* organization can access and edit the `OptIn4Birthdays` user attribute, while none of the other suborganization operators or enterprise or system administrators can use the attribute.

For a list of entities that are inherited, Inherited content and settings in the enterprise.

Create an enterprise hierarchy

Before starting to plan and implement your organization, make sure you read the following section on Best Practices.

Important: For cloud configurations, BlackBerry AtHoc operations must create the enterprise hierarchy.

Best practices for creating an enterprise hierarchy

Consider the following recommendations when planning your implementation:

- Plan the number of suborganizations and how they will be organized.
    - Think about which operators need to send alerts to a group of users. An organization is a group of people that need to be alerted by a specific team of operators and is not always a reflection of the corporate organization structure.
    - Create an organization for each alerting region, such as military base, a campus, or a hospital. The alerting regions are often organized by geography, but can also be organized by purpose such as Weather, Security, or Disaster Relief alerts.
    - Do not make the suborganizations too granular. For example, in a large corporation, create organizations by site, region, or division. Do not create an organization for each department or team.
- Create end users and operators at the suborganization level, not at the enterprise level. No user accounts should exist in the enterprise organization because it prevents sending alerts to user accounts in the enterprise unless they are enterprise alerts. If users are in a suborganization, they can get alerts from their location as well as any enterprise alerts. You can see all users in suborganizations from the enterprise organization so there is no reason to create any users at this level.
- Plan the user attributes and alert folders that should be created in the enterprise organization.
    - Use enterprise attributes and alert folders to enforce consistency for all suborganizations.
    - Think about situations in which you need to alert the entire enterprise. What attributes do you need to target all users in an alert? These attributes should be created at the enterprise level.
    - Attributes that are for only one suborganization should be created at the suborganization level.
    - Do not name a user attribute with the string “Organization.” BlackBerry AtHoc provides an enterprise user attribute with this name that is used to identify the suborganization in which a user account is created.
- If you plan to create an organization for “headquarters”, make it a suborganization. The enterprise organization should only be used for managing the suborganizations and should not have user accounts for headquarters personnel.
- Maintain unique email addresses for users across your suborganizations to provide end users with a single enterprise-wide organization code.
- Enable user uniqueness in the General Settings of the enterprise organization to enforce uniqueness in usernames and mapping IDs across the enterprise organization and all suborganizations. Having unique users allows you to:
    - Deploy a single desktop app for the enterprise that determines a user's suborganization based on their unique mapping ID.
    - Provide end users with a single Self Service URL that can be used at the suborganization or enterprise level.
    - Provide end users with a single enterprise-wide organization code that they can use to sign in to their suborganization client.

Create and configure the enterprise

1. Plan your configuration. See Enterprise management overview and Best practices for creating an enterprise.
2. Log in to the System Setup (3) organization using the login values provided by BlackBerry AtHoc customer support.
3. Create an enterprise organization and suborganizations.

Important: For cloud configurations, BlackBerry AtHoc operations must perform this step.

Create an enterprise organization

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click **New**.
4. Enter the name of the new enterprise organization.
5. Add your name as the first account and click **Save**.
6. In the navigation bar, click your username > **Change Organization**.
7. Select the new enterprise organization.
8. Optionally, configure the organization. For detailed instructions, see "Manage organizations" in the *BlackBerry AtHoc System Settings and Configuration* guide.
9. To create an additional enterprise organization, you can duplicate a peer-level organization. To duplicate the organization, go to the Organizations Manager, select the enterprise organization you created, and click **Duplicate**.

Create a suborganization

Prerequisite

Verify that you are logged in to the enterprise organization.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click **New**.
4. Enter the name of the new organization and click **Save**.
5. In the navigation bar, click your username > **Change Organization**.
6. Select the new organization.
7. (Optional or save for later) Configure the organization. For detailed instructions, see "Manage organizations" in the *BlackBerry AtHoc System Settings and Configuration* guide.
8. After you configure the new organization, you can duplicate a peer-level organization. To duplicate the organization, open the Organizations Manager, select an organization, and click **Duplicate**.

Migrate existing organizations to an enterprise

After you upgrade to the latest release of BlackBerry AtHoc, you can migrate to an enterprise configuration.

Best practices for migrating to an enterprise organization

Consider the following recommendations when you plan your migration.

- Rename any existing user attribute with the name “Organization” to avoid conflicts. BlackBerry AtHoc provides an enterprise user attribute with this name for targeting users by organization.
- Plan the number of suborganizations and how they are organized.
  - Create a new enterprise organization rather than reuse a headquarters organization if there are existing users. Move the headquarters organization under the enterprise level.
  - Do not make the suborganizations too granular. For example, in a large corporation, create organizations by site, region, or division. Do not create an organization for each department or team.
- Plan the promotion of attributes and alert folders. Content that is common among the existing organizations should be promoted.
  - Use enterprise attributes and alert folders to enforce consistency.
  - If more than one organization uses the same user attribute, the attribute should be promoted to the enterprise level.
  - If organizations use different values for the same user attribute being promoted, all values are promoted to the enterprise level.
  - Think about situations in which you need to alert the entire enterprise. What attributes do you need to target all users in an alert? These attributes should be promoted to the enterprise level.
  - Attributes that are for only one suborganization should stay at the suborganization level.
  - The “Emergency Community” and “Organization Hierarchy” attributes are not available for targeting in the enterprise organization.
- Create all user accounts at the suborganization level, not at the enterprise level.
- Authorized administrators can manage suborganization accounts from the enterprise organization.

Prepare to migrate

Important: For Cloud configurations, BlackBerry AtHoc operations must perform the following steps.

Use the Enterprise Migrator tool to move your existing organizations to an enterprise configuration.

Important: Plan your hierarchy before you use the tool. After you save your changes, you cannot change the hierarchy.

Prerequisite: Before you run the migrator tool, create an organization that will be the enterprise organization. Existing organizations likely have users and have been used for local alerting. Instead of re-purposing an organization for the enterprise, create an empty organization. This method allows current organizations to continue operations without interruption and enables you to start with a clean enterprise organization.

Using the migration tool, you will specify the new organization to be the enterprise organization. You then move other organizations under the enterprise. These organizations become subordinate to the enterprise.

The Enterprise Migrator tool migrates existing operators that have an enterprise administrator role in a suborganization to organization administrator. Other operator permissions remain unchanged.

When you move an organization into the enterprise organization, the AtHoc Connect relationships and user accounts remain unchanged for the organization.

Run the Enterprise Migrator tool

Run the Enterprise Migrator tool to move standalone organizations under an enterprise organization. You can also promote attributes and alert folders from suborganizations to the enterprise or system level.

1. Log in to the BlackBerry AtHoc server and change to the following directory:

```
..\AtHocENS\ServerObjects\Tools
```

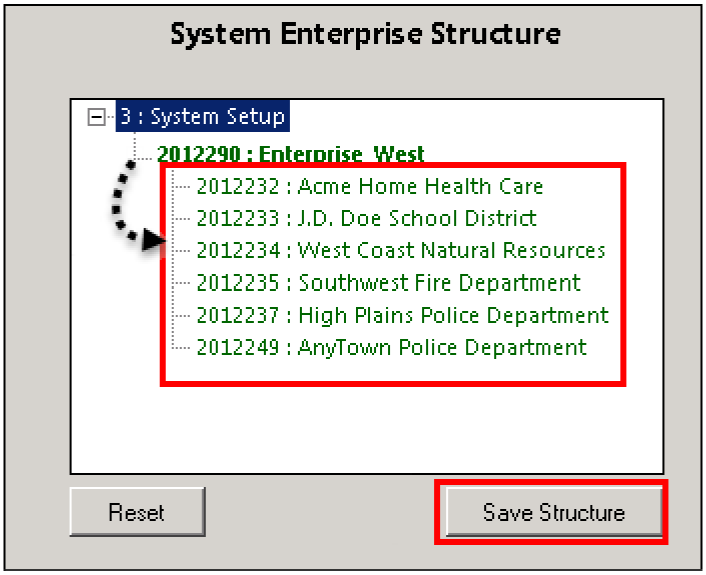
2. Locate the following file: `EAMigrator.exe`.
3. Right-click the file and select **Run as Administrator**.

Migrate organizations to the enterprise

The Enterprise Migrator tool displays the organizations currently in your BlackBerry AtHoc system. By default, new organizations that are created in the system are listed under the System Setup node. These are standalone organizations. You can move them under an enterprise organization to become a suborganization. If an organization is missing, it likely has an incorrect organization type, such as "draft."

Prerequisite: Plan your hierarchy before you use the tool. After you save your changes you cannot change them.

1. In the first column of the Enterprise Migrator tool, drag and drop any organization under another organization to specify the enterprise and suborganization levels. For example, the following image shows seven organizations. When the tool opens, all are considered standalone organizations. Six organizations have been dragged under Enterprise West, migrating them to suborganizations.
2. Verify your structure carefully. You cannot undo the next step.
3. Click **Save Structure**.



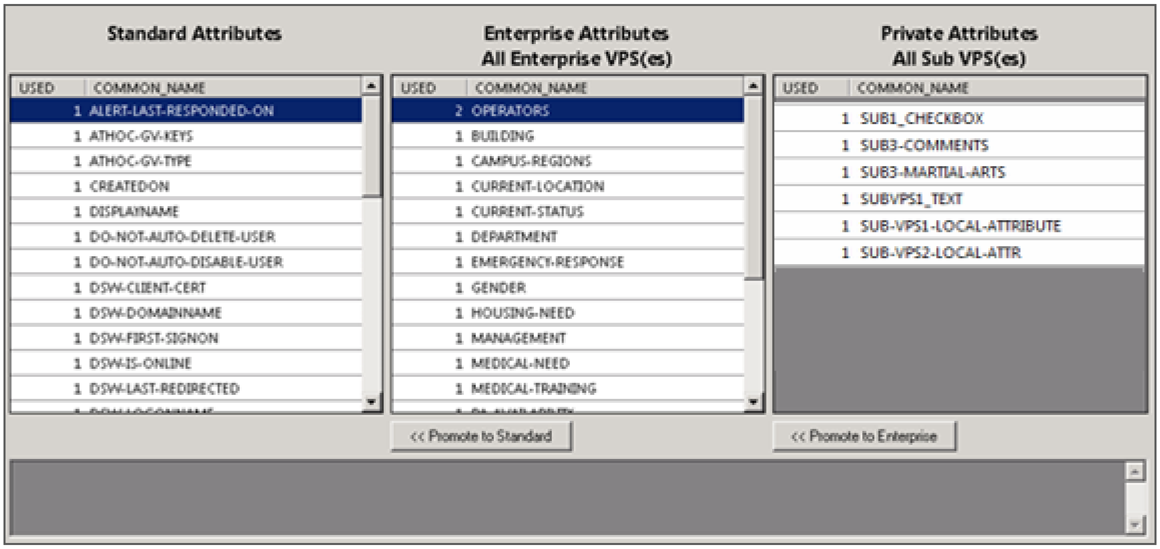
System Enterprise Structure

3 : System Setup
2012290 : Enterprise West
2012232 : Acme Home Health Care
2012233 : J.D. Doe School District
2012234 : West Coast Natural Resources
2012235 : Southwest Fire Department
2012237 : High Plains Police Department
2012249 : AnyTown Police Department

Promote user attributes and alert folders

During migration, you specify at which level the user attributes and alert folders are defined: system, enterprise, or suborganization level. If only a small group of users in a suborganization needs access to an attribute, it should be handled locally. However, for commonly used attributes or alert folders, the system or enterprise level is the typical location.

1. Open the Enterprise Migrator tool and click **User Attributes**.
2. Determine how many instances there are of an attribute at the suborganization and enterprise organization level and promote if it seems efficient. If you promote an attribute to the enterprise level, it is promoted from the suborganizations within the enterprise.



Standard Attributes

USED	COMMON_NAME
1	ALERT-LAST-RESPONDED-ON
1	ATHOC-GV-KEYS
1	ATHOC-GV-TYPE
1	CREATEDON
1	DISPLAYNAME
1	DO-NOT-AUTO-DELETE-USER
1	DO-NOT-AUTO-DISABLE-USER
1	DSW-CLIENT-CERT
1	DSW-DOMAINNAME
1	DSW-FIRST-SIGNON
1	DSW-IS-ONLINE
1	DSW-LAST-REDIRECTED

Enterprise Attributes
All Enterprise VPS(es)

USED	COMMON_NAME
2	OPERATORS
1	BUILDING
1	CAMPUS-REGIONS
1	CURRENT-LOCATION
1	CURRENT-STATUS
1	DEPARTMENT
1	EMERGENCY-RESPONSE
1	GENDER
1	HOUSING-NEED
1	MANAGEMENT
1	MEDICAL-NEED
1	MEDICAL-TRAINING

Private Attributes
All Sub VPS(es)

USED	COMMON_NAME
1	SUB1_CHECKBOX
1	SUB3-COMMENTS
1	SUB3-MARTIAL-ARTS
1	SUBVPS1_TEXT
1	SUB-VPS1-LOCAL-ATTRIBUTE
1	SUB-VPS2-LOCAL-ATTR

3. Select the attribute name.
4. Verify that you want to promote the attribute. You cannot undo the next step.
5. Click **Promote to Enterprise** to move the attribute up to a higher level.

   Promote an attribute from suborganization to enterprise if the entire enterprise needs to use the attribute. Keep the attribute in a suborganization if you want to restrict access to a single organization. For example, promote a general attribute like `DepartmentName` to enterprise because each employee needs to be grouped in a department. Alternatively, keep an attribute like `SoftballTeam` at the suborganization because its members have joined a lunch-time league.
6. Click **Alert Folders**.
7. Select an alert folder type to promote, and click **Promote to Enterprise** based on what types of alerts certain personnel should see.

   For example, promote an alert folder such as `FireDrills` from suborganization to enterprise if the entire enterprise needs to receive alerts from that alert folder. Keep an alert folder such as `ExecutiveSafety` at suborganization if you want to restrict access to operators and users that have a need to know.
8. Save your changes.
9. Restart IIS after you have made structure or content changes.

You have completed the migration to the enterprise.

Postrequisite

Grant permissions to the enterprise for the enterprise administrator for access to the suborganizations. Next, grant enterprise access to operators that need to publish alerts across the enterprise.

Manage users in the enterprise

The enterprise configuration provides centralized user management for all suborganizations under the enterprise organization. The enterprise organization shows a virtual view of users in all suborganizations. Using the virtual view, you can perform most of the operations as if the user accounts were created in the enterprise.

Enable enterprise features

You can manage user accounts from the enterprise organization or from a suborganization if user uniqueness is enforced in your enterprise. When uniqueness is enforced, the system checks for uniqueness of usernames and mapping IDs in the enterprise organization and suborganizations when a new user is created from the BlackBerry AtHoc desktop app, Self Service, API, or through the BlackBerry AtHoc management console. When user uniqueness is enforced, the following items are enabled:

- A single enterprise desktop app: Set up the desktop app to connect to the enterprise. The desktop app then searches for users across the enterprise and connect to the correct suborganization. If the user is not found, a new user is created in the enterprise.
- A single enterprise Self Service URL: Users in any suborganization can log in using the same Self Service URL for the enterprise organization or suborganization.
- Mobile registration from an enterprise organization code: Users can register from their mobile device using the organization code for the enterprise or for any suborganization.
- Enterprise user import and export: Users can be imported into any suborganization directly from the enterprise organization. Users from suborganizations can be exported from the enterprise.
- User move: Users can be moved from one suborganization to another. You can move users between suborganizations through the Users page in the management console, or through the import process.
- Subscribed organizations: Users can subscribe to multiple suborganizations in an enterprise organization. Once subscribed, users can receive alerts and events targeted to them in both their home and subscribed organizations.

For more information, see the *BlackBerry AtHoc Enterprise Features* guide.

Note: Unique email addresses are not enforced in the BlackBerry AtHoc management system when user uniqueness is enabled. However, it is a best practice to have a unique email address for each user in your enterprise and suborganizations.

Enable user uniqueness

1. In the navigation bar, click ⚙.
2. In the **Basic** section , click **General Settings**.
3. In the **Enterprise Features** section, click **Check Readiness** beside Enterprise Features. The system checks for user uniqueness (no users have the same username or mapping ID.)

   If the system finds duplicate users, the Duplicate Users Found window opens and provides a list of duplicate users, their usernames, mapping IDs, and organizations. You must modify any duplicate usernames or mapping IDs to proceed with enabling user uniqueness.

   Click **Export to Excel** to download and save the list of duplicate users. After you update the duplicate users, run the duplicate user check again. If no duplicate users are found, a Check Passed message displays. Click **Close** to return to the General Settings page. The Check Readiness button is replaced by an Enable check box.
4. Select **Enable**.
5. Click **Save**.

Move users in an enterprise organization

The Enterprise User Move feature enables operators in an enterprise organization to easily move users between the different organizations in their enterprise. An enterprise operator with Enterprise User Manager permissions can move users from the enterprise organization to any suborganization, from one suborganization to another, or from a suborganization to the enterprise organization. Enterprise operators can import users at the enterprise level, and then move them into the appropriate suborganization.

Users must be unique across the enterprise and all suborganizations to use the enterprise user move feature. See Enable enterprise features for more information.

When a user is moved from an organization, any roles they had in their original organization are revoked. If a user is later moved back to their original organization, the user's roles are not reinstated. The one exception is for users in the enterprise organization with the enterprise administrator role.

When a user is moved, any subscriptions they have to other suborganizations are cancelled automatically.

When a user is moved, their dependents are also moved.

The history of moved users is preserved. Sent alert reports still display all targeted users that were in the organization at the time the alert was sent.

The status of a user in their original organization (enabled or disabled) is preserved after being moved.

The attribute values for users (for example, personal device addresses) are preserved after being moved, even if those devices or attributes are not enabled in the new organization.

Once a user is moved out of an organization, they can no longer be targeted in any alerts, including draft or scheduled alerts, from that organization.

When a user is moved by an operator or moves themselves, information about the move is recorded in the User Activity section in the user's profile and in the operator audit trail.

If you want to prevent users from being moved between organizations after you have manually moved them either through the management console or by using the .csv import process, set the Prevent User Move attribute for those users. This is useful if you want to prevent users from being moved by an external synchronization source such as LDAP or ADSync.

Move users from the management system

Enterprise operators with enterprise administrator permissions can move users between their enterprise and suborganizations using the BlackBerry AtHoc management system. You can move up to 1000 users at a time.

User uniqueness must be enabled before you can move users between organizations. For more information, see Enable enterprise features.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check box next to the users that you want to move.
4. Click **More Actions** > **Move**. The Move Users window opens.
5. Select an organization from the **Organization** list.

   If any users you are moving have the Prevent User Move attribute enabled, the **Move locked users** option appears and is selected by default. When selected, the Move locked users option allows users to be moved regardless of whether the Prevent User Move attribute has been set.

   The **Lock all users after move** option is selected by default. When selected, the Lock all users after move option adds the Prevent User Move attribute to all moved users. This is useful to prevent any external synchronization sources from moving the users.

6. Click **Move**.

The selected users are moved to the selected organization. Any roles that the users had in their original organizations are revoked. Users in an enterprise organization with the enterprise administrator role retain this role.

Move users with a .csv file

Operators with enterprise administrator permissions can use the import and export process to move large groups of users between their enterprise and suborganizations.

User uniqueness must be enabled before you can move users between organizations. For more information, see Enable enterprise features.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check boxes next to the users that you want to move.
4. Click **More Actions** > **Export**.
5. On the **Export Users** window, use the **Add >** button to select the Organization and Prevent User Move columns.
6. Use the **Add >** button to select any additional columns that you want to include in the export file.
7. Click **Export CSV**.
8. Save the .csv file to your local system.
9. Open the .csv file on your local system.
10. Update the Organization column for any users you want to move. You can also add rows to include new users and specify the organization you want to add them to.
11. Update the **Prevent User Move** column. Enter **Yes** for all users to block them from being moved to another organization. Enter **No** to unblock users if they already have the Prevent User Move attribute set.

    Note: When creating users, the Prevent User Move check box is set when the user is created. If a user is already in an organization, the Prevent User Move attribute is respected upon import. You cannot move and then prevent a future move in the same import action when moving users with the .csv import process.
12. Save the updated .csv file.
13. In the BlackBerry AtHoc management system, click **Back** to return to the user management screen.
14. Click **More Actions** > **Import**.
15. Click **Browse** and navigate to the updated .csv file on your local system.
16. Verify that the Organization and Prevent User Moves columns are selected in the **Select the columns to import** window.
17. Click **Import**.

When the import process completes, you can select the **Download Log** link to view the results.

View and manage user accounts

You can manage user accounts from the enterprise organization or from a suborganization.

From the enterprise organization users list

An enterprise administrator can perform many of the user management tasks that they can from a standalone or suborganization, including:

- View and update user accounts from any suborganization
- Use search and filter to find user accounts from any suborganization
- Add or change roles for any user, such as adding enterprise operator roles
- Restrict the user base of an operator at the enterprise or suborganization

- Create static and dynamic distribution lists across multiple organizations
- Delete or disable user accounts in the enterprise

From the sub organization users list

The following user management tasks must be performed in the suborganization:

- Create user accounts
- Add an operator role for a specific suborganization
- Import users when creating a new organization

Create enterprise distribution lists

When you plan your alerting strategies, you need to identify groups of users to alert across the enterprise and create distribution lists that target the right groups. Distribution lists help the operator send an alert quickly under stressful conditions, reducing the risk of targeting the wrong recipients.

You can populate a distribution list with a static list of users or create a dynamic list based on attributes or queries that are flexible enough to handle changes within the enterprise.

Distribution Lists are not inherited by suborganizations.

- Use static distribution lists when the group is small or very stable, or when certain people (instead of roles) must receive alerts.
- Use dynamic distribution lists when there are large groups that need to be targeted, or when personnel frequently change roles.

Tip: Use the `Organization` attribute to search for users across multiple organizations when creating static distribution lists. You can also use this attribute in an advanced query when creating a dynamic list.

Create an enterprise static distribution list

1. Log in to the BlackBerry AtHoc management system on the enterprise organization as an enterprise operator.
2. Create a static distribution and provide a name that signals that it is enterprise-wide, such as `Ent-SeniorStaff`.
3. Build the list of users in the **Distribution List Members** section.
   a. Click **Modify** to add users to the list.

      Note: If your user base has been restricted, the user list shows only the users in your user base.
   b. Select users from the list. Use the Organizations column to determine which organizations users belong to.
   c. Click **Add Selected** to save the users you selected to the distribution list.
4. Click **Save**.

Create an enterprise dynamic distribution list

Create a dynamic distribution list to target users in multiple organizations. Personnel changes can impact a list, so use a condition to target users that meet the criteria instead of selecting individual users that might move out of the organization.

You can use the enterprise `Organization` attribute, to select users based on the organization that they belong to.

1. Create a dynamic distribution list from the enterprise organization and provide a name that signals that the list is enterprise-wide, such as `Ent-SeniorStaff`.
2. In the **Distribution List Members** section, click **Edit**.
3. In the **Select Attribute** list, select an enterprise attribute to use as targeting criteria for the distribution list.

An enterprise attribute is defined at the enterprise organization level and inherited by suborganizations.

4. In the **Select Operator** list, select the query operator needed for the condition, such as `equals`.

   Note: The list of operators varies depending on the type of attribute selected.
5. In the third field, enter a value, or select one or more available values for the attribute.
6. When you have finished adding conditions, click **Add** to add the criteria to the dynamic list.
7. Click **Save**.

Manage roles and permissions

BlackBerry AtHoc roles are the same in the enterprise, with a few exceptions.

Define user accounts in suborganizations, and then grant them access from the enterprise organization.

The **enterprise administrator** is an operator role that creates and manages the member organizations and common content. Typically, there are 2–5 operators with this role in the enterprise, depending on the size of your organization. The enterprise administrator also grants operator access to the enterprise and specifies the user base for each enterprise operator.

Note: The operator account for the enterprise administrator exists in a suborganization, but the system administrator (or another enterprise administrator) grants the appropriate roles from the users manager in the enterprise organization.

The enterprise administrator role provides full permissions for the enterprise organization and for all suborganizations. The enterprise administrator role is granted to an operator account from one of the suborganizations. The enterprise administrator cannot grant system administrator roles and permissions.

An **enterprise operator** is an operator with any BlackBerry AtHoc role except administrator roles. For example, when assigned the advanced alert publisher role at the enterprise level, an operator can send alerts to users and distribution lists across the enterprise, based on their user base definition.

The enterprise operator can target users in multiple member organizations, based on a system or custom user attribute. They can also use a static distribution list with members from across multiple suborganizations. Or, the operator can use a dynamic distribution list (with a common attribute such as dept='IT') to target members in multiple organizations.

Some or all suborganizations might have enterprise operators, depending on which operators need to alert the enterprise.

Note: The operator account exists in a suborganization, but the enterprise administrator grants the appropriate roles from the users manager in the enterprise organization.

BlackBerry AtHoc roles

Enterprise Administrators, Organization Administrators, and System Administrators can grant operator permissions to any user who needs access to the BlackBerry AtHoc management system. Granting operator permissions includes selecting which roles the user has when they are logged in, as well as setting any restrictions. Roles are additive: you can assign multiple roles and they build on one another, such as End Users Manager and Advanced Alert Publisher.

Administrators cannot assign or revoke higher level operator permissions than their own permissions. For example, an Organization Administrator can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

The role that a user is assigned to determines what BlackBerry AtHoc features they can access. Roles that are associated with specific features in BlackBerry AtHoc can only be assigned to users when that feature is enabled for that user's organization. The features in the following table are restricted to specific roles.

Feature	Roles
Account	• Accountability Manager • Accountability Officer

Feature	Roles
Activity Log	• Activity Log Manager • Activity Log Viewer
Connect **Note:** Connect is enabled and the Connect Agreement Manager role becomes available when organizations are connected.	• Connect Agreement Manager
Situation Response	• Plan Manager • Plan Incident Manager
Collaborate	• Collaboration Manager

The following sections describe the roles that are available in BlackBerry AtHoc.

For more information, see the *BlackBerry AtHoc Roles and Permissions Matrix*.

Create the enterprise administrator

Best Practice: Do not create any user accounts in the enterprise organization.

1. Log in to the BlackBerry AtHoc management system as a system or enterprise administrator.
2. Optionally, change to the appropriate suborganization and then create a new user, if needed.
3. Change to the enterprise organization and open an existing user account from the Users list.
4. Grant the enterprise administration role for the user.
    a. From the user details screen, click **Modify Operator Permissions**.
    b. On the **Operator Permissions** screen, click **Operator Roles**.
    c. Select the **Enterprise Administrator** role.

    Note: Granting the enterprise administrator role gives the user full administrator permissions to all member organizations.
5. When needed, enter a password for the operator.
6. Click **Save**.

Assign operator permissions for the enterprise

Grant enterprise publishing roles for any operator that needs to send alerts to users in more than one organization. The role is granted to an operator account that exists in one of the suborganizations.

1. Log in to the BlackBerry AtHoc management system as a system or enterprise administrator.
2. Optionally, change to the appropriate suborganization and create a new user, if needed.
3. Change to the enterprise organization and open an existing user account from the Users list.
4. Grant roles for the user to specify their permissions within the enterprise.
    a. From the user details screen, click **Modify Operator Permissions**.
    b. On the **Operator Permissions** screen, click **Operator Roles**.
    c. Click to select each of the roles you want to assign to the enterprise operator.

You can grant any available role, such as advanced alert manager or alert publisher. These roles provide the same access to the enterprise, as they do on a standalone or suborganization.

d. To remove an operator permission, click **X** beside the role name.

Tip: Specify a user base for the operator to limit their access to specific groups of users.

Restrict the operator user base

Your security policies might require that you limit enterprise operator access by the type of distribution lists, organization, or seniority of an end user. Use user base definitions to define these restrictions for the operator.

Note: You cannot modify the user base of an operator to give them a less restricted user base than you have.

1. From the operator profile, under **User Base**, select **Restricted** and click **Modify**.

   The Create Conditions screen opens. You can create conditions (queries) that target users in more than one member organization of the enterprise. The conditions use enterprise attributes that are inherited at the member organization level.

   a. In the **Select Attribute** field, click the down arrow to select an attribute.
   b. Select an operator such as `equals`, `not equals`, or `is empty`.
   c. Specify the values that either include or exclude users based on the chosen attribute.

      Note: The `Organization` attribute targets users in specific member organizations.

      For example, if the manager of the IT engineers across the enterprise should only be able to send alerts to their personnel, restrict their user base with the condition `Department equals IT`.

      Or, if an enterprise operator should only be able to publish alerts to organizations in the United States, specify the `EastCoast`, `MidWest`, and `WestCoast` values for the Organization attribute.
2. When needed, enter a password for the operator.
3. Click **Save**.

Manage alerts

Enterprise operators can publish alerts across the enterprise, either to the entire group or to subsets based on attributes or user base restrictions. To publish an enterprise alert, you must be logged into the enterprise organization and have enterprise operator permissions. You must use an alert template created at the enterprise level.

You can use enterprise user attributes and alert folders to target users. You can create enterprise user attributes for each user segment that must be targeted. For example, if you need to publish alerts to the IT departments across the organization, create a Department attribute with a pick list that includes the value `IT`.

Role Permissions: You must have enterprise administrator or operator permissions on the enterprise organization to publish an alert to the entire enterprise organization or to a subset of organizations in the enterprise organization.

Publish an alert to the entire enterprise

Targeting the enterprise assumes that you want to contact all users in all suborganizations of the enterprise. This type of alert should be a rare event, especially if you have multiple organizations that are separated by geography or function.

Best Practice: Target the smallest group of users necessary. Done too frequently, publishing an alert to the full user base will be considered spamming and users will ignore the alerts that are urgent.

Prerequisites

- Verify that devices and gateways are enabled for all targeted devices and gateways in the enterprise organization.
- Verify that you have alerting operator permissions on the enterprise with an unlimited user base.

1. Log in to the BlackBerry AtHoc management system and switch to the enterprise organization.
2. Create or open an enterprise alert template or blank alert.
3. Enter the alert title and content.
4. In the **Targeting** section, select the **By Groups** tab and select **All User Base**.
5. Select the devices that reach as many users as possible. Include mass devices to extend coverage to users that are out of range of other targeted devices.

   You can use the devices, gateways, and delivery templates that are enabled for the enterprise.
6. Review the alert:
   - Ensure that the content provides critical and relevant information to the majority of recipients.
   - Check the spelling and the accuracy of the content.
   - Verify that the device coverage reaches enough users.
7. Publish the alert.

Publish alerts to a subset of the enterprise

Typically, when you send an enterprise-level alert, you want to limit it to those sub groups for whom the alert is relevant. For example, if you have an enterprise with multiple locations in the United States, and you need to send an alert only to users on the East Coast, you would not include those in the West Coast or the Mid West organizations

Tip: When users frequently receive irrelevant alerts, they begin viewing all alerts as spam and ignore or block them. Over-targeting on a regular basis becomes a serious issue when essential alerts are ignored.

You can target a subset of users by using user attributes that are defined in the enterprise organization, or by distributions lists.

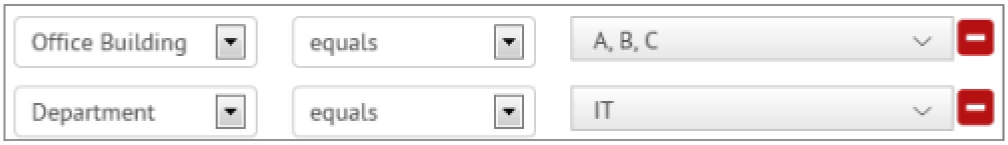
For example, an enterprise operator sends out an alert to a subset of users in three member organizations. The operator can either use enterprise attributes, such as Office Building= "A, B, C" and Department = "IT", or a dynamic distribution list to target the IT staff in the three buildings on different campus locations in the region.

Target by advanced query

You can use user attributes in advanced queries to target users by department, location, skills, or status.

For example, enterprise operators in a federal agency can use the Department and OfficeBuilding enterprise attributes to target users by office building and department to alert IT personnel that there is an outage affecting three buildings.

1. Log in to the BlackBerry AtHoc management system and switch to the enterprise organization.
2. Create or open an alert template, or create a blank alert.
3. Create the content.
4. To target by user attribute, click the **Advanced Query** tab.
5. Click **Add Condition**.
6. Create a condition (attribute, operator, and value) to target users that exist in the organizations that you must reach. The following image shows the conditions for our IT outage example.



Office Building equals A, B, C

Department equals IT

7. Select the devices and any organizations that you need to include.
8. Review and publish the alert.

Target by distribution list

Enterprise distribution lists can include users in multiple organizations, as long as the creator has user base permission to access the user and the organization. Static and dynamic distribution lists provide a quick and efficient method for targeting multiple users across the enterprise.

For example, the enterprise operator can alert IT personnel in the federal agency suborganizations with an enterprise distribution list of just IT members.

Prerequisite: Distribution lists must exist in the enterprise organization and include members of the user base of the enterprise operator. These are users from organizations that the enterprise operator can access. For more information, see Create enterprise distribution lists.

1. Log in to the BlackBerry AtHoc management system and switch to the enterprise organization.
2. Create or open an alert template, or create a blank alert.
3. Specify the title and the content.
4. For targeting a subset of enterprise users, click the **By Groups** tab.
5. Click the **Distribution Lists** folder.
6. Select a distribution list that specifies the users in the organizations that you need to target.
7. Select the devices.
8. Ensure the devices are enabled in the organizations and that you are able to reach the users in the various organizations.
9. Review and publish the alert.

Inherited content and settings in the enterprise

The following objects can be defined at the enterprise organization, and are inherited by each suborganization.

User attributes: You can find user attributes in the User Attributes section on the Settings screen.

- Attributes are inherited by lower-level organizations, except for Emergency Community and Organization Hierarchy, which exist at the suborganization level.
- Attributes defined at the system or enterprise can be viewed, but the only fields that can be modified are the Page Layout options. For the Page Layout options, you can decide whether the attribute appears on the Self Service My Profile page and the User Details page in the BlackBerry AtHoc management system. If you opt to have it appear, you can decide how much information is displayed: Basic Info, Physical Addresses, or Advanced Information.
- All aspects of attributes defined at your organization level can be modified with the exception of the attribute type and the organization the attribute is associated with.

Organization code: You can find the organization code in the Enterprise Features section on the General Settings screen.

Click **Check Readiness** beside Enterprise Features. The system checks for user uniqueness (no users have the same username or mapping ID). When the check passes, select the Enable check box next to the **Enterprise Features** field to enable enterprise aware mobile registration. When enabled, enterprise aware mobile registration enables users to sign on from a mobile device using the enterprise organization code, or the organization code for any suborganization.

Alert folders: You can configure alert folders in the Basic section on the Settings screen.

Security policies: You can configure security policies in the System Setup section on the Settings screen.

If you need to define unique security requirements for a suborganization, configure them in the Security Policy page for the suborganization, so that the change impacts only that suborganization.

Delivery templates for the BlackBerry AtHoc Desktop App: You can configure delivery templates for the desktop app in the Basic section on the Settings screen.

Audio files: You can configure audio files in the Basic section on the Settings screen.

Devices: You can configure devices in the Devices section of the Settings screen.

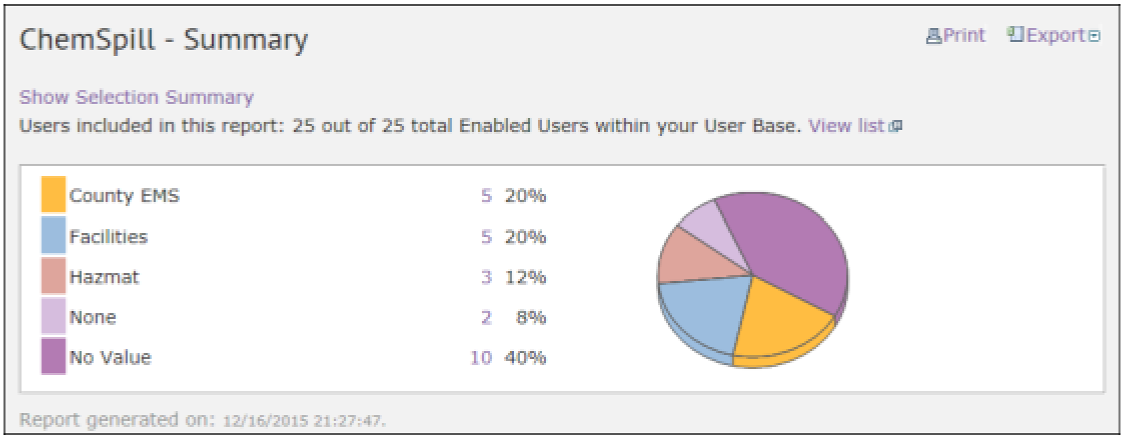
- Devices are defined at the system level using the Device Configuration Tool on the BlackBerry AtHoc server.
- Administrators can enable or disable a device for each suborganization.
- Administrators can specify whether the contact information for the device is required for each suborganization.

Available reports in the enterprise

You can create and review reports in the enterprise organization like you can in a standalone organization. In the navigation bar, click **Reports**.

The following reports are available:

- **Personnel Reports:** This report is generated using enterprise user attributes and shows views of all enterprise personnel.



ChemSpill - Summary

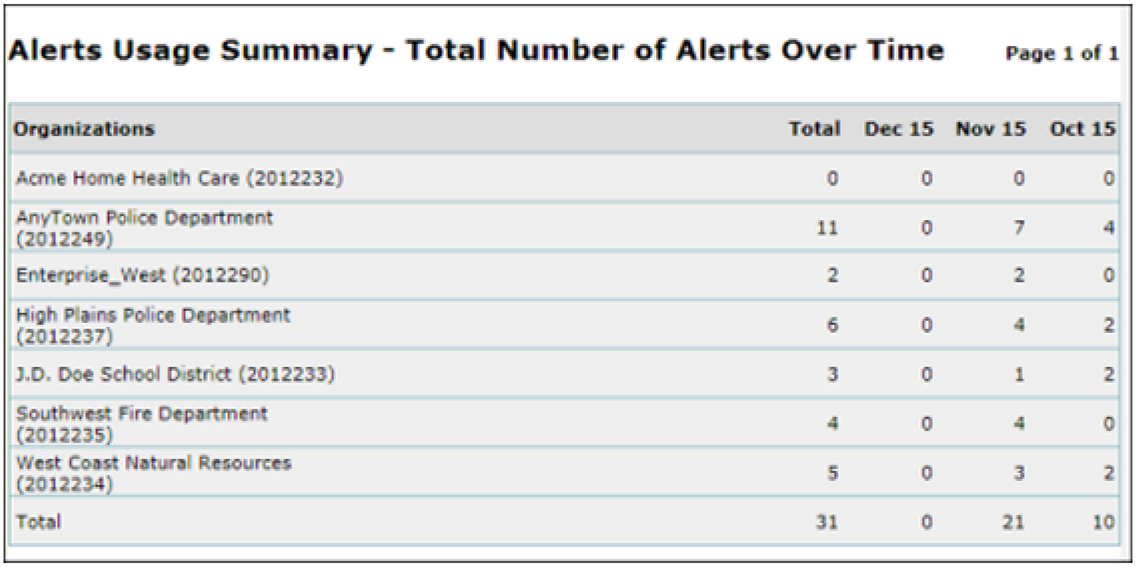
Show Selection Summary

Users included in this report: 25 out of 25 total Enabled Users within your User Base. View list

🟧	County EMS	5	20%
🟦	Facilities	5	20%
🟥	Hazmat	3	12%
🟪	None	2	8%
🟪	No Value	10	40%

Report generated on: 12/16/2015 21:27:47.

- **Alert Usage Summary:** This report shows the total number of alerts or messages by organization over time.

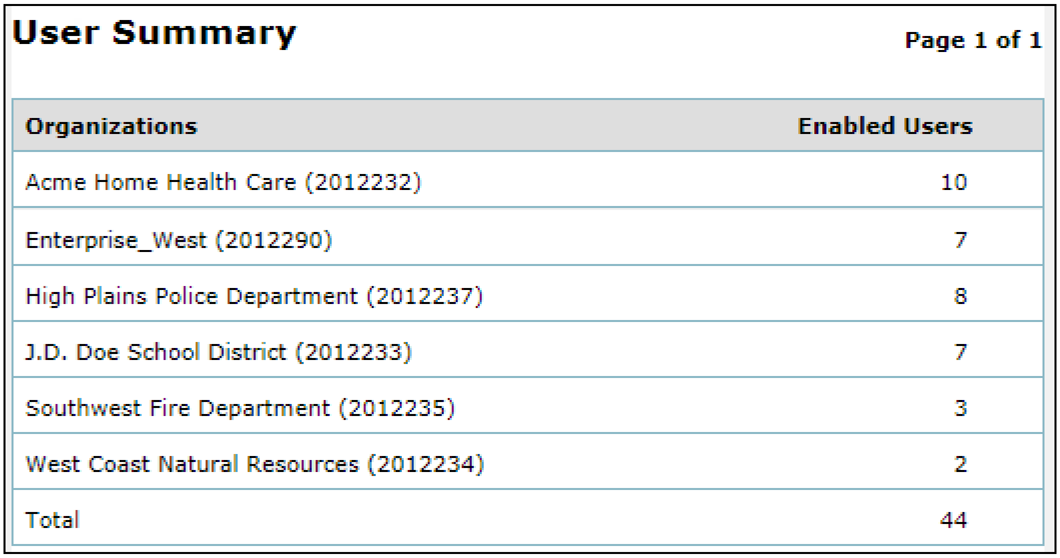


Alerts Usage Summary - Total Number of Alerts Over Time

Page 1 of 1

Organizations	Total	Dec 15	Nov 15	Oct 15
Acme Home Health Care (2012232)	0	0	0	0
AnyTown Police Department (2012249)	11	0	7	4
Enterprise_West (2012290)	2	0	2	0
High Plains Police Department (2012237)	6	0	4	2
J.D. Doe School District (2012233)	3	0	1	2
Southwest Fire Department (2012235)	4	0	4	0
West Coast Natural Resources (2012234)	5	0	3	2
Total	31	0	21	10

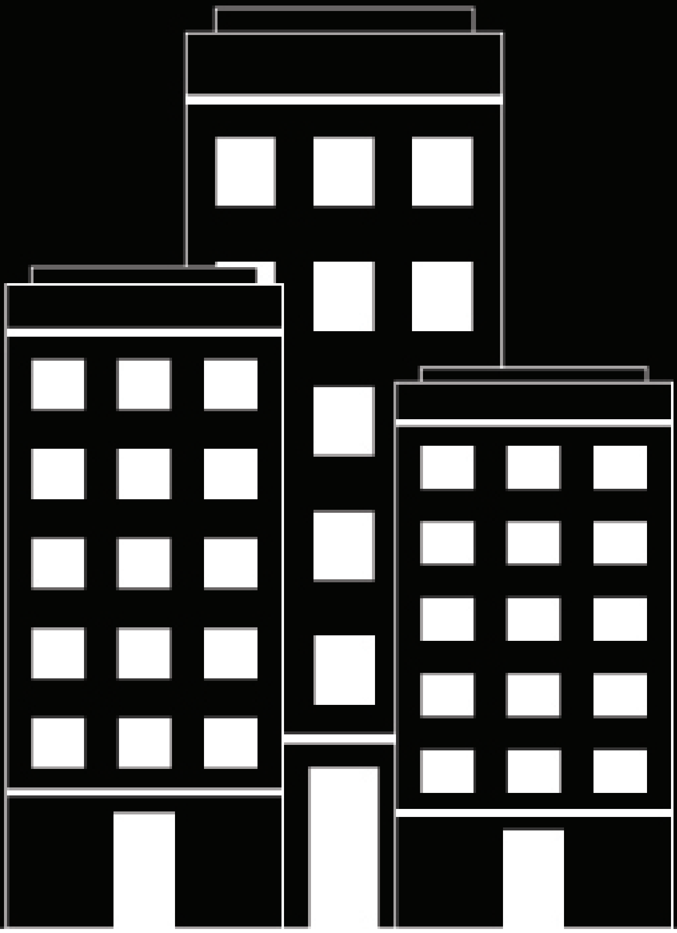
- **User Summary:** This report provides a count, by organization, of the number of enabled users.



User Summary

Page 1 of 1

Organizations	Enabled Users
Acme Home Health Care (2012232)	10
Enterprise_West (2012290)	7
High Plains Police Department (2012237)	8
J.D. Doe School District (2012233)	7
Southwest Fire Department (2012235)	3
West Coast Natural Resources (2012234)	2
Total	44



BlackBerry AtHoc

Enterprise Features

7.16

Contents

Manage enterprise features

This guide describes how to manage features for your enterprise organization in the BlackBerry® AtHoc® system.

Enable enterprise features

You can manage user accounts from the enterprise organization or from a suborganization if user uniqueness is enforced in your enterprise. When uniqueness is enforced, the system checks for uniqueness of usernames and mapping IDs in the enterprise organization and suborganizations when a new user is created from the desktop app, Self Service, SDK, or through the BlackBerry AtHoc management system. When user uniqueness is enforced, the following items are enabled:

- **A single enterprise desktop app**: Set up the desktop client to connect to the enterprise. The desktop client will then search for users across the enterprise and connect to the correct suborganization. If the user is not found, a new user is created in the enterprise.
- **A single enterprise Self Service URL**: Users in any suborganization can log in using the same Self Service URL for the enterprise organization or suborganization.
- **Mobile registration from an enterprise organization code**: Users can register from their mobile device using the organization code for the enterprise or for any suborganization.
- **Enterprise user import and export**: Users can be imported into any suborganization directly from the enterprise organization. Users from suborganizations can be exported from the enterprise.
- **User move**: Users can be moved from one suborganization to another. You can move users between suborganizations through the Users page in the management system, or through the import process.

Note: Unique email addresses are not enforced in the BlackBerry AtHoc system when user uniqueness is enabled. However, it is a best practice to have a unique email address for each user in your enterprise and suborganizations.

Enable user uniqueness

1. Log in to the BlackBerry AtHoc management system as an Enterprise Administrator.
2. In the navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. In the **Enterprise Features** section, click **Check Readiness** beside **Enterprise Features**. The system checks for user uniqueness (no users have the same username or mappingID).

   If the system finds duplicate users, the Duplicate Users Found window opens and provides a list of duplicate users, their usernames, mappingIDs, and organizations. You must modify any duplicate usernames or mappingIDs to proceed with enabling user uniqueness.
5. Click **Export to Excel** to download and save the list of duplicate users. After you update the duplicate users, run the duplicate user check again. If no duplicate users are found, a Check Passed message displays.
6. Click **Close** to return to the **General Settings** page. The Check Readiness button is replaced by an **Enable** check box.
7. Select the **Enable** check box.
8. Click **Save**.

Move users in an enterprise organization

The Enterprise User Move feature enables operators in an enterprise organization to easily move users between the different organizations in their enterprise. Enterprise Administrators can move users from the enterprise organization to any suborganization, from one suborganization to another, or from a suborganization to the enterprise organization. Enterprise operators can import users at the enterprise level, and then move them into the appropriate suborganization.

Enterprise Administrators can move users between suborganizations from the enterprise organization. Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move users from their suborganization to other suborganizations.

Select the User Move for End Users option in General Settings in a suborganization to enable users to move themselves to that suborganization in Self Service. This option is enabled by default.

Users must be unique across the enterprise and all suborganizations to use the Enterprise User Move feature. See Enable user uniqueness for more information.

When a user is moved from an organization, any roles they had in their original organization are revoked. If a user is later moved back to their original organization, the user's roles are not reinstated. The one exception is for users in the enterprise organization with the Enterprise Administrator role.

When a user is moved, any subscriptions to other suborganizations are automatically cancelled.

When a user is moved, their dependents are also moved.

The history of moved users is preserved. Sent alert reports still display all targeted users that were in the organization at the time the alert was sent.

The status of a user in their original organization (enabled or disabled) is preserved after being moved.

The attribute values for users (for example, personal device addresses) are preserved after being moved, even if those devices or attributes are not enabled in the new organization.

Once a user is moved out of an organization, they can no longer be targeted in any alerts, including draft or scheduled alerts, from that organization.

When a user is moved by an operator or moves themselves, information about the move is recorded in the User Activity section in the user's profile and in the operator audit trail.

To prevent users from being moved between organizations after you have manually moved them either through the management system or by using the .csv import process, set the Prevent User Move attribute for those users. This is useful if you want to prevent users from being moved by an external synchronization source such as LDAP or ADSync.

Move users from the management system

Enterprise Administrators can move users between their enterprise and suborganizations using the BlackBerry AtHoc management system. You can move up to 1000 users at a time. Dependent users are moved with their sponsor users.

Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move users from their suborganization to other suborganizations.

User uniqueness must be enabled before you can move users between organizations. For more information, see Enable user uniqueness.

1. In the navigation bar, click **Users** > **Users**.

2. On the **Users** screen, select the check box beside all users you want to move.
3. Click **More Actions** > **Move**.
4. On the **Move Users** window, select an organization from the **Organization** drop-down list.

   If any users you are moving have the Prevent User Move attribute enabled, the Move locked users check box appears and is selected by default. When selected, the Move locked users check box allows users to be moved regardless of whether the Prevent User Move attribute has been set.

   The **Lock all users after move** check box is selected by default. When selected, the Lock all users after move check box adds the Prevent User Move attribute to all moved users. This is useful to prevent any external synchronization sources from moving the users.
5. Click **Move**.

The users are moved to the selected organization. Any roles that the users had in their original organization are revoked. Users in an enterprise organization with the Enterprise Administrator role retain this role. Any subscriptions to other suborganizations the users had are automatically cancelled.

Move users with a .csv file

Enterprise Administrators can use the import and export process to move large groups of users between their enterprise and suborganizations.

Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move users from their suborganization to other suborganizations.

User uniqueness must be enabled before you can move users between organizations. For more information, see Enable user uniqueness.

1. In the navigation bar, click **Users** > **Users**.
2. Select the check boxes beside the users you want to move.
3. Click **More Actions** > **Export** > **Users**.
4. On the **Export Users** screen, use the **Add>** button to move the **Organization** and **Prevent User Move** columns to the Selected Columns section.
5. Use the **Add>** button to select any additional columns to include in the export file.
6. Click **Export CSV**.
7. Save the .csv file to your local system.
8. Open the .csv file on your local system.
9. Update the **Organization** column for any users you want to move. You can also add rows to include new users and specify the organization you want to add them to.
10. Update the **Prevent User Move** column. Enter **Yes** for all users to block them from being moved to another organization. Enter **No** to unblock users if they already have the **Prevent User Move** attribute set.

    Note: When creating users, the Prevent User Move check box is set and the user is created. If a user is already in an organization, the Prevent User Move attribute is respected upon import. You cannot move and then prevent a future move in the same import action when moving users with the .csv import process.
11. Save the updated .csv file.
12. In the management system, click **Back** to return to the **Users** screen.
13. Click **More Actions** > **Import** > **Users**.
14. Click **Browse** and navigate to the updated .csv file on your local system.
15. On the **Import User File**screen, verify that the **Organization** and **Prevent User Moves** columns are selected in the **Select the columns to import** section.
16. Click **Import**.

When the import process completes, you can select **Download Log** to view the results.

Manage organization subscriptions

Use organization subscriptions to enable users in an enterprise organization to receive alerts and accountability events from other suborganizations in their enterprise organization. This feature enables users to subscribe on a temporary basis to up to ten suborganizations. The subscribed user can then receive any alerts or events that are targeted to them in their home organization and in their subscribed organizations. The user's home organization is the organization where their profile is stored. A user's subscribed organization is an organization that they can be targeted in, but their profile does not get moved to.

Subscribed users can be targeted from their subscribed organization using email, SMS, phone, and mobile app devices and can be targeted using any targeting criteria such as location, groups, or attributes. Targeted devices must be enabled on both the home and subscribed organizations. When targeting subscribed users by attributes, those attributes must be enterprise-level attributes.

The organization subscription feature is disabled by default and must be enabled by a System Administrator. Enterprise Administrators select the suborganizations within their enterprise organization that are available for subscription.

Once organization subscriptions are enabled, operators can subscribe users from the BlackBerry AtHoc management system or by using the .csv user import process. Users in suborganizations can subscribe themselves to enabled suborganizations from Self Service or the mobile app. The Organization Subscription for End Users option in the Customization > Self Service section in General Settings must be selected in a suborganization for it to appear for subscription in Self Service. This option is enabled by default.

If the organization subscription feature is disabled, any existing subscriptions are cancelled. Administrators and users can set start date and end dates, or cancel their subscriptions. Users can be subscribed to a maximum of ten available organizations.

The profiles of users who are subscribed to organizations remain in their home organization.

On the subscribed organization, subscribed users are visible in search results, can be added to distribution lists, and can be targeted in alerts or events. Their profiles can be viewed, but not edited or deleted, from the subscribed organization. Two new standard user attributes "Temporary work location" and "Subscribed Organizations" have been added to enable searching and targeting subscribed users.

Standalone users and sponsor users can subscribe to organizations. Dependents cannot be subscribed to other organizations.

User uniqueness must be enabled on the enterprise organization before organization subscriptions can be enabled. For more information, see Enable user uniqueness.

Enable organization subscription

1. Log in to the BlackBerry AtHoc management system as an Enterprise Administrator.
2. In the navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, in the **Enterprise Features** section, click **Organization Available For Subscription** and select one or more suborganizations.
5. Click **Save**.

Subscribe users to organizations

This section describes how to subscribe users to suborganizations using the BlackBerry AtHoc management system or the .csv user import process. For instructions on subscribing to organizations from Self Service, see the *BlackBerry AtHoc Self Service User Guide*.

Before you begin: Before users can be subscribed to organizations, the following conditions must be met:

- The Organization Subscriptions feature must be enabled on the enterprise organization.
- The Enterprise Administrator must select the organizations that are available for subscription.

Select the Organization Subscription for End Users option in the Customization > Self Service section in General Settings in a suborganization to enable end users to subscribe to that organization from Self Service.

Subscribe a single user

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select a user from the list.
4. On the user profile screen, click **Edit User**.
5. On the user profile screen, in the **Organization Subscriptions** section, click **Add Subscription**.
6. On the **Subscribe Organization** window, select an organization from the list.
7. Click **Apply**.
8. In the **Organization Subscriptions** section, enter a date or click 📅 to select a start date for the subscription.
9. Optionally, click 📅 to set an end date for the subscription.
10. Optionally, repeat Steps 5 to 9 to subscribe the user to additional organizations. You can subscribe the user to a maximum of ten available organizations.
11. Click **Save**.

The user can now be targeted in alerts and events from the subscribed organizations.

Subscribe multiple users

You can use the .csv user import process to delete or modify organization subscriptions for multiple users.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select the users you want to subscribe to organizations.
4. Click **More Actions** > **Export** > **Users**.
5. On the **Export Users** screen, in the **All Columns** list, select **Subscribed Organizations** > **Add >**.
6. Click **Export CSV**.
7. Save the .csv file to your local system.
8. Open the .csv file.
9. Update the **Subscribed Organizations** column to add, remove, or modify the organizations for each user. You can subscribe each user to a maximum of ten available organizations.
10. Optionally, in the **Subscribed Organizations** column, add start and end dates for the subscription. Separate the start and end dates with a pipe (|) character. Use the date format of your current organization. For example: `Sub-Org1: 4/5/2021|8/8/2021, Sub-Org3: 5/5/2021|, Sub-Org4: |7/7/2021`.
11. Save the .csv file.
12. In the BlackBerry AtHoc management system, click **Back** to return to the Users screen.

13. Click **More Actions** > **Import** > **Users**.

14. On the **Import User File** screen, click **Browse** and select the .csv file on your local system.

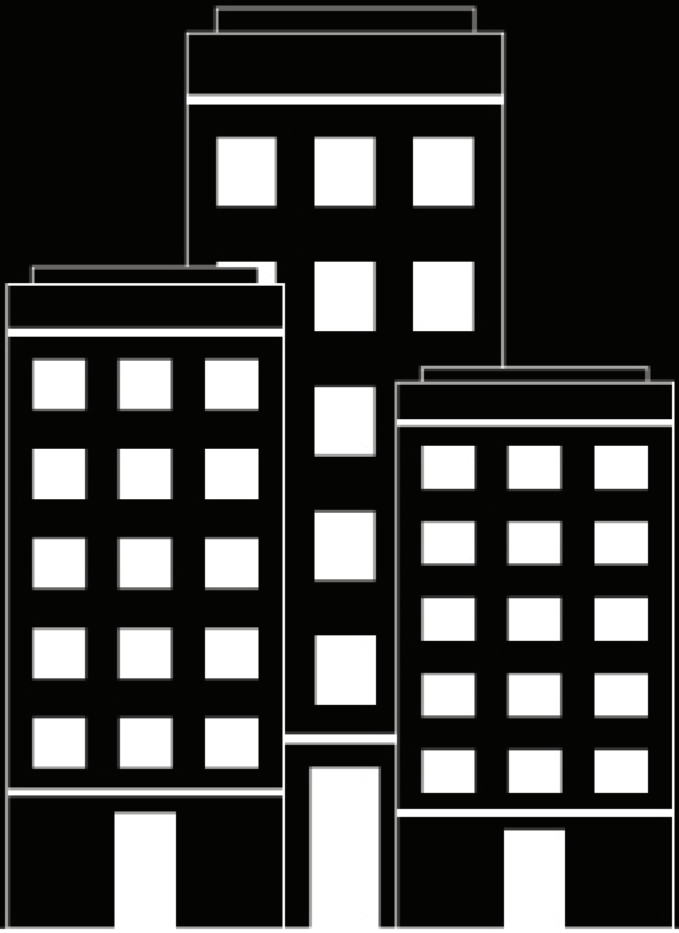
15. Click **Open**.

16. In the **Select the columns to import** section, select **Subscribed Organizations**.

17. Click **Import**.

18. Optionally, on the **Import Details** window, click **Download Log** to view the results.

The updated users can now be targeted in alerts and events from their subscribed organizations.



BlackBerry AtHoc

System Settings and Configuration

7.16

Contents

BlackBerry® AtHoc® set up and administration overview

Administrators create, configure, and manage the organization settings that operators use to communicate with their recipients as well as with other organizations. Setup includes configuring the features used by operators to communicate during situations. This guide covers the following administration tasks:

- The Manage organizations section describes how to create an organization and duplicate an existing organization. To create or migrate an existing set of organizations to an Enterprise model, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations*.
- The Configure BlackBerry AtHoc settings section describes how to configure the features provided by BlackBerry AtHoc to communicate and coordinate with teams and recipients during a crisis. The following topics are covered in this section:
    - Configure basic settings: Personalize your organization with a name, welcome or disclaimer text, and an icon. You can also customize the time zone and time formats, configure security policy settings, create a security policy message, and control default page layouts and enterprise features.
    - Manage system settings: Configure the name, URL, time zone, database archive directory, system help desk information, support page content, redirection settings, client certificates, and disclaimers for your system.
    - Security policy settings: Define password rules and complexity, enforce system-wide password updates, set session timeout, limit active sessions, configure smart card authentication settings, and enable CAPTCHA validation.
    - Monitor system health: Create, view, edit, enable, disable, delete, and refresh system health monitors.
    - View the diagnostic log: Run basic and advanced searches of the diagnostic log.
    - Organizations Manager: Create organizations, enable and disable features, manage integrated device agents, provision applications for the web API, view the operator audit trail report and the alerts usage summary report.
    - Manage system jobs: View details about system jobs, create and export a system diagnostics report.
    - Configure device gateways: Configure the mobile app and AtHoc Cloud Delivery Service gateways.
    - Configure devices: Enable and disable devices, manage mass communication devices, configure giant voice devices, configure the AtHoc Connect organization network, manage the Cloud Services gateway, configure RSS and XML feed information and failover delivery gateways.
    - Configure desktop app settings: Select general desktop software options, customize the desktop client system tray, configure client server communications and failover settings, and set the desktop software authentication type.

For information about creating and managing alert templates, specifying alert folders, managing delivery templates, and managing audio settings, see the *BlackBerry AtHoc Alert Templates* guide.

For information about managing settings for incoming alerts, see the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

For information about granting permissions for working with AtHoc Connect and updating sector visibility in the Connect profile, see the *BlackBerry AtHoc Connect* guide.

For information about settings related to users and user attributes, including creating, deleting, and editing user attributes and automatically disabling or deleting users based on attributes, see the *BlackBerry AtHoc Manage Users* guide.

Manage organizations

This section describes how to create and duplicate organizations. To learn how to work with enterprise organization hierarchies, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations*.

Create a new organization

To create a new organization in the system, you must be a System Administrator with permissions to switch between organizations from within the BlackBerry AtHoc management system.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Organizations Manager**.
4. On the **Organizations Manager** page, click **New**.
5. Enter a name for the new organization.
6. Select one of the following organization types:
   - **Enterprise**: Choose this type when logged in to the System Settings organization to create an enterprise or a stand-alone organization.
   - **Sub Organization**: Choose this type when logged in to an enterprise organization to create a member organization.
   - **Basic**: Choose this type to create a Basic organization.
7. Click **Save**. The details of the new organization appear on the Organizations Manager page.

Configure a new organization

After you have created the organization and have switched to the new organization, you can define the URLs, name, logo images, default alert templates, and Self Service defaults for that organization.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. Configure basic settings: In the **Basic** section, click **General Settings** and then complete the steps in General settings.
4. Configure devices: Complete the tasks described in Configure devices.
5. Configure gateways: Complete the tasks described in Configure device gateways.
6. Enable devices: Complete the tasks described in Enable devices on the BlackBerry AtHoc server and the "Enable a Device" task described in Enable and disable devices.
7. Create user attributes: Complete the tasks described in the "Create a user attribute" and "Configure an Organizational Hierarchy attribute" sections of the *BlackBerry AtHoc Manage Users* guide.
8. Add users: Complete the steps described in the "Create a user" section of the *BlackBerry AtHoc Manage Users* guide.

Duplicate an organization on the same server

You can copy an existing organization and rename it. Be aware that most settings are copied from the original organization, including alert templates, except as specified.

Important:

- You must be a system administrator.
- Duplication includes device and protocol duplication.
- After duplicating an organization, review all alert templates and make adjustments if necessary.
- Creating organizations using the New button in the Organizations Manager should be performed only with assistance from BlackBerry AtHoc technical support to ensure the new system has all the appropriate settings.
- By default, a duplicated organization will not have a common name. If you plan to access the duplicated organization with the BlackBerry AtHoc SDK, you must assign it a common name.
- You can duplicate a peer organization, but not a child (member) organization.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click to select the organization you want to copy.

   Note: If the list is extensive, use the search field at the top of the screen. You can also click a column heading sort the list.
4. Click **Duplicate**.
5. On the **Duplicate Organization** dialog, enter the name of the new organization.
6. Click **Save**.

The duplicate organization appears in the list on the main screen.

Duplicate organizations across systems

Duplicating organizations from one server to another is an advanced configuration task. For more information, see “Advanced server configuration” in *Install and Configure BlackBerry AtHoc*.

Configure BlackBerry AtHoc settings

Important: To access the screens, features, and functions mentioned in this section, you must be a System Administrator, Enterprise Administrator, or Organization Administrator in the BlackBerry AtHoc organization. If you do not have these roles, many of the options on the Settings screen will be grayed out.

Users who have been granted administrator permissions in BlackBerry AtHoc can set up organizations and manage settings and users within an organization.

Configure basic settings

The Basic settings cover the primary settings required to set up an organization and enable enterprise features.

General settings

You can use General Settings to personalize your organization with a name, welcome or disclaimer text, and an icon. You can also customize the time zone and time formats, configure security policy settings, create a security policy message, and control default page layouts and enterprise features.

To configure general settings that are available for enterprise organizations, see Enterprise features.

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

   The General Settings screen for the organization opens with the following fields prepopulated:

   - The **Name** field displays the name of your organization.
   - The **Organization Code** field serves as a short name used to register for Self Service and for the mobile app. The organization code must also be used in the URLs used to access Self Service and Single Sign-On (SSO). If not provided by a system administrator, the organization code is automatically generated from the organization name with spaces replaced with hyphens. You must have system administrator permissions to edit this field. The Organization Code field is mandatory.
   - The **User Login** field displays the server address that users access to log in to Self Service.
   - If Self Registration is enabled for the organization, the **Registration URL** field displays the server address that users access to register.
3. Complete the remaining fields described in the sections below.
4. Click **Save**.

Organization Details

1. Optionally, enter a **Support Email** address.
2. Optionally, in the **Logo** field, click **Browse** to upload a graphic file you want to display in the top corner of each screen. The file type must be .gif, .jpg, or .png.
3. Optionally, in the **Logo Text** field, enter a text string of up to 100 characters that appears when users hover their cursors over the logo.

Enterprise Features

The Enterprise Features section is available only for enterprise organizations that have suborganizations.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **General Settings**.
3. On the **General Settings** page, scroll down to the **Enterprise Features** section.
4. Complete the steps described in the sections below to require user uniqueness, enable user initiated move, and select organizations for subscription as needed.
5. Click **Save**.

Enable enterprise features

Enabling enterprise features in your enterprise organization enables the following items:

- **A single enterprise desktop app**: Set up the desktop client to connect to the enterprise. The desktop client will then search for users across the enterprise and connect to the correct suborganization. If the user is not found, a new user is created in the enterprise.
- **A single enterprise Self Service URL**: Users in any suborganization can log in using the same Self Service URL for the enterprise organization or suborganization.
- **Mobile registration from an enterprise organization code**: Users can register from their mobile device using the organization code for the enterprise, or any suborganization.
- **Enforcement of unique usernames and Mapping ID values for all users in an enterprise organization**: The system checks for uniqueness of usernames and mapping IDs in the enterprise organization and suborganizations when a new user is created through the desktop app, Self Service, .csv import, or the BlackBerry AtHoc management system.

1. Click **Check Readiness**. The system checks for user uniqueness (no users have the same username or mappingID). If the system finds duplicate users, the Duplicate Users Found window opens and provides a list of duplicate users, their usernames, mappingIDs, and organizations.
2. Modify any duplicate usernames or mappingIDs to proceed with enabling user uniqueness.
3. Run the duplicate user check again. If no duplicate users are found, a Check Passed message displays.
4. Click **Close** to return to the General Settings page. The Check Readiness button is replaced by an Enable check box.
5. Select the Enterprise Features **Enable** check box. The User Initiated Move check box appears.
6. Click **Save**.

Enable user move

If you have a large enterprise organization where users in your system need to move between organizations, you can enable the User Move feature. This reduces the burden on your administrators by enabling users to move themselves between the suborganizations of your enterprise organization in Self Service.

Enterprise Administrators can move users between suborganizations from the enterprise organization. Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move and subscribe users from their suborganization to other suborganizations.

When a user is moved to a different organization, their view of Self Service may change, depending on the settings of the organization they are moving to. If the user is an operator, any operator permissions they had in their original organization are revoked. If the user was an Enterprise Administrator in the enterprise organization, they retain this role in the suborganization they are moved to. If the user had roles and permissions in other organizations within the enterprise or organizations outside of the enterprise organization, they are retained. If a user has dependents, those dependents are also moved.

Prerequisites

- Require user uniqueness must be enabled.
- The User Move for End Users option must be enabled on each suborganization. This option can be set in the Customization > Self Service section in General Settings on the suborganization. This option is enabled by default.

1. Select the User Move **Enable** check box. The Available Organizations list appears. The enterprise organization and all suborganizations appear in the Available Organizations list.
2. Select the organizations that you want to be available for user move, or choose **Select All**. You can narrow the list of organizations by typing the name of an organization in the text box.
3. Click **Save**.

The list of selected organizations is shown to all users in the enterprise. End users will see the selected organizations in the Move to Organization screen in Self Service.

Select organizations for subscription

If you have an enterprise organization where users in your system may be assigned to different locations on a temporary basis, and they need to be able to receive alerts and events from their temporary location as well as their home location, you can configure organizations for subscriptions.

Before you select an organization for subscription, the Organization Subscriptions feature must be enabled. For more information, see "Manage organization subscriptions" in the *BlackBerry AtHoc Enterprise Features* guide.

Before an organization can be configured for subscription, user uniqueness must be enabled.

1. In the **Organization Available for Subscription** section, select individual organizations or choose **Select All**. You can narrow the list of organizations by typing the name of an organization in the text box.
2. Click **Save**.

The selected organizations are available for user subscription. End users will see the selected organizations when they click Add Subscription in the Organization Subscriptions section on the My Profile screen in Self Service. The Organization Subscription for End Users option must be selected in the Customization > Self Service section in General Settings on the suborganization for it to be available for users to subscribe to from Self Service. This option is enabled by default.

Customization: Text

1. In the **Homepage Welcome Message** field, enter text that will appear at the top of the Welcome screen.
2. In the **Footer Text** field, enter text that will appear on the bottom left of every screen.

   Note: This text can be a disclaimer, if one is required, or any information that all users need to see.

Customization: Locale Setting

1. In the **Locale** field, select the language and region associated with the organization.
2. In the **Date Format** field, select the date format relevant for your organization.
3. In the **Time Format** field, select the time format relevant for your organization.
4. In the **Delivery Locales** field, select the locales (languages) you want to publish alerts in. Note that after support for a locale is enabled, it cannot be disabled.
5. In the **Time Zone** field, select the correct time zone for your server.

Customization: Phone Call Setting

1. In the **Caller ID** field, enter the number you want to display on the mobile devices of alert recipients when an alert is published to them. You can enter up to 15 digits and special characters such as +.
2. In the **Default Country Code** field, select the country code that will be displayed by default whenever users enter a phone number into a field.
3. Optionally, in the **GETS** field, enter the Government Emergency Telecommunications Service (GETS) PIN number.

Customization: Desktop App

1. In the **Desktop App Logo** field, click **Browse** to upload the graphic file you want to display in the desktop app. The file must be a .gif, .jpg, or .png file type. The recommended size is 140 pixels wide by 70 pixels high.

Customization: Self Service

1. In the **Name on User Pages** field, enter your organization name.
2. Optionally, include an organization-specific disclaimer message to display to users when they log in to Self Service. The maximum size of the message is 4000 characters.

3. (For suborganizations only.) Optionally, select the **Organization Subscription for End Users** option to enable users to subscribe themselves to this organization in Self Service. This option is enabled by default.
4. (For suborganizations only.) Optionally, select the **User Move for End Users** option to enable users to move themselves to this organization in Self Service. This option is enabled by default.

Dependents

Note: To enable dependents, see Enable and disable features.

Note: The layout for dependent user pages is different than the layout for sponsors. This enables you to keep the layout page for dependents simple, providing only the needed information.

1. In the **Dependent Profile Layout** section, click **View/Edit**.
2. On the **Dependent Profile Layout** dialog, edit the XML to add, modify, or remove profile page sections.
3. Click **Save**.

Attachments

Note: To enable attachments, see Enable and disable features.

- In the **Attachments** section, select the **Enable** check box to enable adding attachments to alerts and events.

Layouts

In the **Layouts** section, you can add or update the default view for various user screens such as the user profile in Self Service, the My Profile or Users page in the management system, and user information when accessed from an alert or accountability event. You can also adjust the display of columns on the Users page and in reports and set group targeting definitions.

Click **View/Edit** to open a window to modify the layout settings.

1. **User Details - My Profile**: (Do not modify this setting without first consulting BlackBerry AtHoc customer support.) Determines the layout of standard user attributes when viewed through the My Profile page in the management system or Self Service.
2. **User Details - Full Page**: (Do not modify this setting without first consulting BlackBerry AtHoc customer support.) Determines the layout of standard user attributes when viewed anywhere outside of the main Users list. For example, when seen through the Inbox or from alert or event publishing screens.
3. **User Details - Popup View**: Determines the layout of standard user attributes when viewed anywhere outside of the main Users list. For example, when seen through alert publishing screens or in maps. Information about a user's devices and distribution list membership can also be added to a user's pop-up view.
4. **Default Columns - User Page**: Determines the columns that appear by default from the Users page in the management system.
5. **Default Columns - User Reports**: Determines the columns that appear by default when viewing alert reports or when the user list is shown in a pop-up window.
6. **Targeting Settings**: Determines the attributes that are available for targeting in the By Groups tab on the New Alert and New Event pages. The selected attributes are also available when searching for users by group. Only attributes that have predefined values are available.

Map settings

As an administrator user, you can use the Map Settings screen to set up and configure map defaults, shape layers, and distribution list layers. For more information, see the *BlackBerry AtHoc Live and Publisher Maps* guide.

External events

BlackBerry AtHoc improves emergency managers' situational awareness by providing alerts for external events that impact their organization and employees. External event categories include: Earthquake, Fire, Hurricane, and Flood.

When external events are enabled, Organization Administrators can define the locations and external events they want to monitor. When an external event occurs that impacts a selected location, it appears in the Inbox in the BlackBerry AtHoc management system and on the live map. Operators can also receive notifications on their chosen devices (email, SMS, and mobile app) when events that impact their selected locations appear in the Inbox.

Before you begin:

- IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement**.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **External Events**.
3. On the **External Events** screen, in the **Your Organizational Area** section, click ✎.
4. On the map, do any of the following:
   - Click **Create Custom Locations**, and then select a shape. Click and drag on the map to draw a shape.
   - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

   You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
5. Click **Apply**.
6. In the **External Event Types** section, select the types of external events to receive in the Inbox.

   If the external event type you need is not listed, you can submit a request to add it. Go to the BlackBerry AtHoc support portal at: https://www.blackberry.com/us/en/support/enterpriseapps/athoc/support-request. Include the Event Type keyword and region in the support request form. If available, provide the external event feed source. For example: COVID-19, United States, https://tools.cdc.gov/api/v2/resources/media/404952.rss.

   RSS, Geo-JSON, CAP, and ATOM formats are supported. Each requested feed type must have consistent location data and event type information. Requested feed types should be applicable to a regional (for example U.S. West Coast), national, or international area. For more information, see "Request a new external event type" in the *BlackBerry AtHoc External Events* guide.
7. Optionally, in the **Setup Admin Notifications** section, click **Select Targets**.
8. On the **Users** dialog, select the operators to notify when an external event occurs in the selected organizational areas. All external events that impact the organizational area appear in the Inbox in the BlackBerry AtHoc management system and on the live map. The operators you select will receive an alert about the event on the selected devices.
9. Click **Apply**.
10. From the **Devices** pull-down menu, select the devices (email, SMS, and mobile app) that the targeted operators will receive notifications on. You can select more than one device.
11. From the **Frequency** pull-down menu, select the interval to send the event notifications at. Choose **24 Hrs** or **48 Hrs**. One notification is sent for each event category. For example, Earthquake.
12. Click **Save**.

Manage system settings

The following sections describe how to configure and maintain your BlackBerry AtHoc organizations at the system level.

Specify system settings options

Use the System Settings options tab to configure the name, URL, time zone, database archive directory, system help desk information, and support page content link that are displayed throughout the BlackBerry AtHoc system. You can also configure the client certificate and BlackBerry AtHoc Cloud Services (PSS) settings.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **System Settings**.
5. Click **Edit** to configure the global settings described in the following sections.
6. Click **Save**.

System Setup Parameters

In this section, determine the following values:

- **Name**: Unique name for each BlackBerry AtHoc installation
- **Identifier**: Unique identifier for the organization determined when the organization is created
- **System Setup URL**: Web address for BlackBerry AtHoc
- **Desktop Traffic URL**: Web address for the BlackBerry AtHoc desktop app
- **Time Zone**: The time zone for the application server
- **Database Archive Directory**: Location where the database is archived. Provide the full path name relative to the computer that BlackBerry AtHoc is installed on.

Custom Content

Customize messages for the operator in every organization in the system. In this section, you can configure the following:

- **Management System Help**: Display support information text that displays on the log on screen. Typical information includes directions or a link for when the user forgets their password. HTML formatting is supported.
- **System Disclaimer Message**: Display a required disclaimer, such as limitations on liability or use of copyrighted materials. The limit is 4,000 characters. The disclaimer can display as a splash screen before operators log in or as a banner in the BlackBerry AtHoc desktop window. The banner displays regardless of the module selected from the navigation bar. For example, use a banner to notify operators that the information they are currently viewing is classified and protected from unauthorized use.

Redirection Settings

Select the check box to enable client redirection. Client redirection allows you to set up redirection rules for the desktop app. To configure redirection rules for the desktop app, click **Redirection Rules**.

For more information, see "Redirection" in the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Advanced Settings

Client Certificates

Specify client certificates for the client computer. Use the Microsoft Management Console (MMC) snap-in tool to view certificates on a Windows computer. To access, type **MMC** in the **Start** menu field. Within this section, you can configure the following:

- **Client Certificate**: Select this check box to append a client certificate.
- **Subject**: Enter the value of the Subject parameter found on the Details tab of the certificate settings.
- **Store Name**: Certificates are found in stores. Specify **Personal** or select one of the options in the drop-down list.
- **Store Location**: The stores are located either in the current user store or the local machine store.

BlackBerry AtHoc Cloud Services

BlackBerry AtHoc Cloud Services checks for messages sent between BlackBerry AtHoc and the mobile application. In this section, you can configure the following:

- **Enable Cloud Services**: Select this check box to use the mobile app or AtHoc Connect.
- **Server Address**: Enter the name of the server URL for BlackBerry AtHoc Cloud Services. The server address is provided by BlackBerry AtHoc customer support.
- **Username**: Enter the username that the Polling Agent for BlackBerry AtHoc Cloud Services uses when it polls requests from the service. The username is provided by BlackBerry AtHoc customer support.
- **Password**: Enter the password that the Polling Agent uses when polling requests from the service. The password is provided by BlackBerry AtHoc customer support.

SMS Opt-In Service

Enter the URL for the SMS Opt-In service.

System Data Maintenance

Specify the frequency of records maintenance for the system.

- **Event Viewer**: Enter the number of days after which event records are deleted.
- **Desktop Sessions**: Enter the number of days after which data is deleted for sessions of the desktop app.
- **Geo History**: Enter the number of days after which historical data for geolocation data is deleted.

URL Referrer Whitelisting

Add URLs for external domains or websites to the **Whitelisted Domain Addresses** field to allow users to access the BlackBerry AtHoc management system and Self Service from them. URLs must be in the HTTPS format. Separate URLs by commas, not spaces. The maximum number of characters allowed is 2000.

Add or remove a disclaimer for the BlackBerry AtHoc management system

If your organization requires posting a disclaimer, such as limitations on liability or use of copyrighted materials, you can create a disclaimer that displays in the form of a splash screen before operators log in to BlackBerry AtHoc. You can also customize a banner that displays in the BlackBerry AtHoc desktop window. The banner displays regardless of the module selected from the navigation bar.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.

2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **System Settings**.
5. In the text-entry box under the **Custom Content** section, type the text of the disclaimer. The limit is 4,000 characters.
6. Click **Save**.

These changes are applied at the next login to BlackBerry AtHoc management system.

To remove a disclaimer, delete the text in the text-entry box, then click **Save**.

Security policy settings

The security policy manages password rules, sessions settings, and Captcha settings. Additionally, it allows you to force users to change their passwords the next time that they log in.

Note: Security policy settings configured on an enterprise organization are inherited by each suborganization.

Define password rules

Threats of security breaches have motivated organizations to develop stringent rules governing password creation and mandatory password change cycles. BlackBerry AtHoc enables customizing the rules for password creation and password complexity to conform to your organization's policies, including compliance with the United States Department of Defense password requirements.

System Administrators and Enterprise Administrators can access the Security Policy screen, change the rules for password creation, control the visibility of the Password Never Expires setting on user profile pages, and enforce a system-wide password update for all operators the next time the operators log in.

Important: In addition to the rules covered on the Security Policy screen, consider communicating the following guidelines to your organization when defining passwords:

- Avoid words found in a dictionary, or a proper name, spelled forwards or backwards.
- Avoid simple keyboard sequences with repeated keystrokes.
- Avoid previously used passwords.
- Avoid strings that reference personal information.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **Password Update Rules** section, on the **Security Policy** screen, specify values based on the following information:

   Note: If a password rule is unnecessary in your organization, type 0 (zero) as its value.

   - **Renew Password After**: Force operators to change their passwords every *n* number of days. Type the number of days that a password is valid. Type **0** to never force operators to change their passwords.
   - **Show "Password Never Expires"**: Select this option to display the Password Never Expires option on user profile pages. This option is selected by default. You must have system administrator or enterprise administrator permissions to set this option.
   - **Reuse Password After**: Prevent operators from recycling recent passwords. For example, if you type **5** the system does not accept any of the last 5 passwords created by an operator. Type **0** to allow operators to use any previous password.
   - **Minimum Password Age**: Set the minimum time interval for changing passwords. For example, type **15** to force users to wait at least 15 days before changing their passwords.

- **Minimum Changes in Password**: Specify the minimum number of characters in a password to prevent users from using very similar passwords. For example, type **5** to force users to change at least 5 characters each time they change their passwords.
- **Lock Account After**: Prevent unauthorized attempts to guess an operator's password. Type the maximum number of login attempts allowed. Operators cannot log in using the same username after a lockout. Type **0** to allow an unlimited number of login attempts.
- **Reset Lockout After**: If a lockout occurs, reset it after a specified number of minutes. Set to **0** (zero) to prevent the lockout from being automatically reset. For this last case, to reactivate the account, the administrator must go to **Users** > **Users**. Click the user's name, then click **Edit Operator Permissions** on the user details screen. Click **Unlock** to change the status.

4. Click **Save**.

The updated password requirements go into effect for all new operators and for existing operators when their passwords expire. Operators whose passwords never expire do not have to change their passwords to conform to updated password requirements.

Configure password complexity

In addition to creating password rules, if you have the required permissions, you can configure the level of complexity required for user passwords.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Password Update Rules** section, select values for each of the following components:
    - **Minimum Length**: Specify the minimum number of characters that a password must contain. Select a value between 7 and 20.
    - **Minimum Lowercase Characters (a-z)**: Specify the minimum number of lowercase characters that a password must contain. Select a value between 1 and 6. If no lowercase characters are required, select 0.
    - **Minimum Uppercase Characters (A-Z)**: Specify the minimum number of uppercase characters that a password must contain. Select a value between 1 and 6. If no uppercase characters are required, select 0.
    - **Minimum Numeric Characters (0-6)**: Specify the minimum number of numeric characters (0-9) that a password must contain. Select a value between 1 and 6. If no numeric characters are required, select 0.
    - **Minimum Special Characters**: Specify the minimum number of special characters (!@#$%^&*()_+) that a password must contain. Select a value between 1 and 6. If no special characters are required, select 0.
4. Click **Save**.

The updated rules go into effect for all new operators and for existing operators when their passwords expire. Operators whose passwords never expire do not have to change their passwords to conform to updated password complexity rules.

Enforce a system-wide password update

If you have the necessary permissions, you can enforce a system-wide password change with the current password rules and complexity. Selecting this option forces all operators to change their password the next time they log in. The operators whose passwords are set to never expire are exempt from this enforcement.

Important: After this action is taken, it cannot be undone.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, click **Enforce password update**.

Revoke operator permissions automatically

If you are an Organization Administrator, Enterprise Administrator, or System Administrator, you can configure your BlackBerry AtHoc system to automatically revoke operator permissions. When configured, operators who have not logged into the system for the specified time have their permissions revoked. The operator's inactivity period is calculated using the Last Login Date attribute. If the operator has not logged in to the system, the inactivity period is calculated based on the date the operator was granted permissions on. When automatic revocation of operator permissions is enabled, a system job runs every 24 hours to revoke operator permissions based on the operator's last successful login.

Tip: Use the Last Login Date operator attribute to identify and notify operators whose permissions will be automatically revoked due to inactivity.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Revoke Operator Permissions** section, click **Add Condition**.
4. Select one or more roles from the **Operator Roles** list.
5. Select the number of days of inactivity from the **Auto Revoke Permissions after** list.
6. Optionally, click **Add Condition** to add an additional revocation rule. You can add up to three rules.
7. Optionally, click ⊟ to remove a revocation rule.
8. Click **Save**.

Set session timeout and continue session values

You can set the maximum amount of time a user session can be inactive before auto-logout occurs and when a timeout warning appears.

Note: Enterprise administrators can set the session timeout and warning settings for an enterprise organization or for any suborganization. If the session timeout setting is changed for an enterprise organization, the suborganizations' settings are also changed.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** page, in the **Login Session** section, enter a value (in minutes) in the **Session Timeout** field. The maximum session timeout value is 1440 (24 hours.)
4. In the **Warning Before Session Timeout** field, enter the number of minutes prior to auto-logout that the warning message appears on the user's screen. If the user does not click to continue the session before the timer runs out, they will be logged out of the system automatically.
5. Click **Save**.

The session timeout value is applied the next time a user logs in to the BlackBerry AtHoc management system.

Limit active sessions

You can configure your BlackBerry AtHoc system to limit the number of active sessions a user can have open at the same time with the same user account. Session information is maintained by a user's browser. Multiple tabs on the same browser use the same session. When the active session limit is reached, the user is prompted to close an existing session. The session that has been inactive for the longest time is terminated and the user is redirected to the login page.

Note: When the limit active sessions setting is configured on an enterprise organization, it is inherited by each suborganization that does not have this setting defined.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** page, in the **Login Session** section, select **Limit Active Sessions**.

4. Select the number of allowed active sessions from the **Active Sessions per User Account** list. You can select up to ten active sessions.
5. Click **Save**.

Enable operator login using smart cards

When Smart Card authentication is enabled in addition to regular username/password authentication, users have the option of logging in to BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. This is commonly used for Department of Defense systems.

Note: In order to use this option, you must set up Mapping IDs for each user through the Users manager.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **Smart Card Authentication** section, select **Smart Card Login**.
4. Click **Save**.

Require operator login using smart cards

When smart card authentication is required, users can *only* access BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. This is commonly used for Department of Defense systems.

Note: In order to use this option, you must set up Mapping IDs for each user through the Users manager.

If you choose to require operators to log in using smart cards, the following changes occur in the administrative side of the BlackBerry AtHoc system:

- All suborganizations of the main organization inherit the Smart Card-Only authentication method.
- The log in screen continues to display Username and Password fields because until a user attempts to log in, the system has no way of knowing what organization the user belongs to and what restrictions, if any, the user's organization has imposed on authentication.
- After the user attempts to log in with a username or password combination, the system returns an error message informing them that they must use their smart card for system authentication.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **Smart Card Authentication** section, select **Smart Card Login**.
4. Select **Require Smart Card**.
5. Click **Save**.

Enable SSO certificate revocation list checking

When Single Sign-On (SSO) is enabled for your organization, a Certificate Revocation List (CRL) is maintained. A CRL is a list of digital certificates that have been revoked and should not be trusted. If CRL checking is enabled, BlackBerry AtHoc checks the CRL before initiating a Security Assurance Markup Language (SAML) authentication request to an identity provider (IDP) or after receiving an SAML response from the IDP.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **SSO CRL (Certificate Revocation List) Settings** section, select the **Enable CRL Checking** option.

   Note: If the **SSO CRL (Certificate Revocation List) Settings** section is not visible, SSO is not enabled. For information about enabling SSO, see "Enable single sign-on" in the *BlackBerry AtHoc Manage Users* guide.
4. In the **CRL Timeout Interval** field, enter the number of seconds to allow for certificate validation information to be retrieved from the Certificate Authority (CA). The minimum is 1 and the maximum is 60 seconds. The default is 20 seconds.

5. Optionally, select the **Ignore Verification Errors** option. This option is selected by default. When selected, any error that occurs during CRL verification is added to the diagnostic log. This option does not interrupt the SSO authentication flow. If this option is not not selected, when CRL verification fails, the user is redirected to an error page.
6. Click **Save**.

Import a service provider certificate

Import a BlackBerry AtHoc signed service provider certificate for use in Single Sign-On (SSO). This enables administrators to select a BlackBerry AtHoc certificate instead of uploading and maintaining a custom SP certificate.

You must have system administrator permissions to import a service provider certificate.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Security Policy**.
5. On the **Security Policy** page, in the **Service Provider Certificate** section, click **Import Certificate**.
6. On the **Import Certificate** window, enter a valid password for the service provider certificate.
7. Click **Browse** and navigate to and select a valid BlackBerry AtHoc certificate. Only .pfx and .p12 files can be imported.
8. Click **Import**.
9. On the **Security Policy** page, click **Save**.

Enable CAPTCHA validation

A CAPTCHA field is a security test that validates whether a human is entering content into a field rather than an automated program by requiring users to enter the specific numbers or text that they see in an image into a text-entry field.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. Under **Captcha Settings**, select **Enabled**.
4. Click **Save**.

Monitor system health

The supervision and monitoring framework within BlackBerry AtHoc graphically illustrates the current status and any abnormal conditions or failures in the management system homepage, and provides access to its status and administration functions.

Overview of system health monitoring

BlackBerry AtHoc can monitor and supervise the operational status of the following:

- BlackBerry AtHoc internal modules and processes
- Integrated systems and devices

This monitoring and supervision framework operates at global and organization levels, allowing you to do the following:

- Define scheduled monitors of different types to check various system operational conditions.
- Designate normal and abnormal operating conditions.

- Define what actions to take when state transitions take place including proactive notification to system administration and operation teams.
- Access every monitor associated with the system through the System Visibility Console and view all monitors that are in an Error state from a tab on the BlackBerry AtHoc homepage.

View default health monitors

Your BlackBerry AtHoc system includes a set of default health monitors that are grouped into the sections described below. When you create a new monitor, you can add it to one of the groups or create a new group and give it any name.

Note: You must be a System Administrator, Enterprise Administrator or Organization Administrator to view health monitors. You must be an Enterprise Administrator or System Administrator to edit or create a new health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**.

   Note: Global monitors can be viewed from the Global System Health and System Health links. Organization monitors can be viewed only from the organization view. Monitors can only be edited through the Global System or organization under which they were created.

The following table describes the available default health monitors.

Section	Monitor	Description
Database		
	Database Full Backup	Runs a database query to identify the time of the most recent full database backup.
	Database Space	Runs a database query to identify how much space is available in the database and displays an error if the TempDB size falls below the threshold that you specify.
	TempDB Size	Identifies the minimum Microsoft TempDB data sizes required by BlackBerry AtHoc. The following sizes are recommended: • 1 GB for Microsoft SQL Express edition • 2 GB for Microsoft SQL Standard edition • 4 GB for Microsoft SQL Enterprise edition
Web Applications		

Section	Monitor	Description
	Bing GIS	Tests the Bing GIS URL for responsiveness. You can edit this setting through the Global System Health screen.
	Desktop Client Server Interface	Tests the Desktop Client Server Interface URL for responsiveness.
	Management System Console	Tests the Management System URL for responsiveness
	OEM	Tests the OEM URL for responsiveness.
Services		
	IIS Longevity	Tests how well the Web Application is operating by evaluating the BlackBerry AtHoc diagnostic logs.
	Scheduled Job Queue	Tests how well the Scheduled Job Queue is operating by running a query on the database.
	System Tasks	Tests how well the system tasks are functioning by running a query on the database.
	Tracking & Reporting	Tests how well the Tracking & Reporting system is operating by running a query on the database.
Delivery Gateways		
	AtHoc Cloud Delivery Service (East)	Tests the connectivity of the AtHoc cloud delivery service.
	AtHoc Cloud Delivery Service (West)	Tests the connectivity of the AtHoc cloud delivery service.
	AtHoc Mobile Service	Tests the connectivity between the current organization and the AtHoc Mobile Service.
	OEM Cloud Delivery Service (East)	Tests the connectivity of the OEM cloud delivery service.
	OEM Cloud Delivery Service (West)	Tests the connectivity of the OEM cloud delivery service.

Section	Monitor	Description
General		
	CAP Events Process	Checks the CAP events processor to see if it is correctly processing CAP events.
	CAP Polling Agent	Checks the CAP Polling agent to see if data is being correctly added to the database.
	Database Tables - Identity Seed Max Limit	This monitor checks the identity seed values across tables to determine if they are within the safe limit.
	Desktop Notifier Load Balancing	Monitors the Desktop App incoming traffic across two or more application servers. Warnings are provided when the load is not balanced evenly across all servers.
	Online Users	Identifies the number of Online Users using desktop pop-up alerts within the past 24 hours.
	IIM	Checks the status of connectivity between the BlackBerry AtHoc system and IIM.
Alert publishing		
	Delivery	Checks delivery batches for the alert publishing cycle and reports if there have been publishing errors within the last 24–48 hours.
	Publishing	Checks live publishing activity, and reports if alerts do not go live within a specified amount of time.

View system health monitors with errors

You can view the details of system health monitors that are in an Error state.

Note: You must be a System Administrator, Enterprise Administrator or Organization Administrator to view health monitors. You must be an Enterprise Administrator or System Administrator to edit or create a new health monitor.

1. In the navigation bar, click ⚙.
2. Do one of the following:

   - In the **System Setup** section, click **Global System Health** to view errors for the global system.
   - In the **System Setup** section, click **System Health** to view errors for the organization.
3. On the **System Visibility Console** or **Organization Visibility Console** screen, in the **Errors & Warnings** section, click a monitor name.

The screen that appears has a red field at the top that explains why the monitor is in an Error state. The Testing history field displays the state of the monitor during each recent test is displayed. Expand additional sections to view more detailed information about each error.

Create a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to create a new system health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor that you want to edit. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Create new monitor** at the top of the screen.

   Note: You can also click any of the **Create new monitor** links within the groups on the System or Organization Visibility Console screen. The difference is that when you click a link within a group, the New Health Monitor screen that opens has the **Is it associated with other Health Monitors?** field preset to the name of the group the link appeared within.
4. On the **New Health Monitor** screen, complete the fields in the following sections:

   - **Basic details**

     a. Enter the name of the monitor, the location where you want it to appear on the Visibility Console screen, and the time and frequency of the monitoring checks.
     b. Designate whether or not the monitor will appear on the Organization Visibility Console and whether errors and warnings about the monitor will appear on the System area on the BlackBerry AtHoc homepage.
   - **How does this Monitor test the system?**: Select the kind of test the Monitor will run on the system. Note that the type of test cannot be edited after it is saved. The following options are available:

     - Web URL Test
     - Combined Health Monitors
     - BlackBerry AtHoc Event Logs
     - Database Procedure
     - UAP Health Test

     After you make a selection, sample configuration XML for that type of test appears below the Test Configuration field. Use that as the basis for the XML code you enter into the Test Configuration field.
   - **How is the state of this Health Monitor determined?**: Designate the way the state of the monitor will be determined by selecting one of the following options:

     - **Use the most recent test result**
     - **Calculate it over multiple test results**: If you select this option, use the drop-down lists in the section to specify how the calculation should be determined. Optionally, select **Match the state if** if you want to also use "X" number of identical test results as a trigger for a state change, where you set the value for X.
   - **What happens when this Health Monitor reaches a particular state?**: For each of the Health Monitor states, specify the following:

     a. The implications of the state:

        - **Error**: The test returned an error condition on the object being tested.
        - **Warning**: The test returned a warning condition on the object being tested.
        - **Good**: The test run returned the expected results.
        - **Inoperative**: The test process failed. This does not reflect the health of the object being tested. This state indicates the operational status of the monitor itself. For example, if in a database query, the database referenced has a typo and the system cannot find the database to query.
    b. Actions to take when the monitor is in the selected state:

       Define the actions that should be taken any time a monitor transitions into each of the states. To make this process faster and less prone to errors, click **Show a list of possible actions** for each state and then add either or both of the actions **Trigger a URL** or **Send an Email** on the pop-up screen for the **Configure** field.
5. Click **Save**. The system evaluates the parameters you set. If the parameters are correct, the system creates a new monitor. If the syntax in any of the conditions is incomplete or incorrect, an error message is displayed.

Edit a health monitor

Note: You must be an Enterprise Administrator or System Administrator to edit a system health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to edit.
3. On the **Organization Visibility Console** or **System Visibility Console** screen, click the name of the monitor you want to edit. The monitor details screen opens, displaying the current state of the monitor and its recent testing history.
4. Click any or all of the sections on the screen to edit the fields within them:
    - **Testing history**:
        a. Change the granularity of the time frame displayed in the history table by clicking **Hourly**, **Daily**, **Weekly**, or **Monthly**.
        b. Click ◀ and ▶ to change the block of time you are looking at. For example, if the granularity is set to Monthly, click ◀ to display the testing history for the previous month.
    - **Basic details**:
        - Change the name of the monitor, its location on the Visibility Console screen, and the time and frequency of the monitoring checks.
        - Change the setting that determines whether the monitor appears on the Organization Visibility Console and whether errors and warnings about the monitor appear on the System tab on the BlackBerry AtHoc homepage.
    - **Database Procedure**:
        - Update the test configuration script that is used in the monitor.
    - **How is the state of this Health Monitor determined?**:
        - Change the way the state of the monitor is determined by selecting the other option: *most recent result* or *combined results*.
    - **What happens when this Health Monitor reaches a particular state?**:
        - Change the implications of any or all states, and configure different transaction actions for any or all states.
    - **Special Case: Edit the IIS Longevity Health Monitor**: If you have more than one application server, you need to modify the default settings for the IIS Longevity health monitor using the following values:

- `WarningCountThreshold`: The default value is 2. This default assumes one application server. For a multiple application server installation, change the value of `WarningCountThreshold` to (application server count) x (default). For example, if there are two application servers, the value should be 4.
- `ErrorCountThreshold`: The default value is 5. The default setting assumes one application server. For a multiple application server installation, change the value of `ErrorCountThreshold` to (application server count) x (default). For example, if there are two application servers, the value should be 10.

5. Click **Save**.

Disable a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to disable a system health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to disable. The System Visibility Console screen opens, displaying the system monitors in the system.
3. Click **Disable** in the row for the monitor you want to disable.

The System Visibility Console screen refreshes and the monitor appears with no icon next to its name and two buttons, **Enable** and **Delete**, in the row.

Enable a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to enable a system health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to enable. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Enable** in the row for the monitor you want to enable.

The System or Organization Visibility Console screen refreshes and the monitor appears with either a green ✓ or a red ● beside its name and Refresh, Disable, and Delete buttons in the row.

Delete a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to delete a system health monitor.

Note: Deleting the monitor permanently deletes all history and configuration for the monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to delete. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Delete** in the row for the monitor you want to delete.
4. On the **Delete Health Monitor** dialog, click **OK**.

The System or Organization Visibility Console screen refreshes and the monitor no longer appears on the screen.

Refresh a system health monitor

Although health monitors refresh automatically based on their internal monitor schedule, you can refresh a monitor manually at any time.

1. In the navigation bar, click ⚙.

2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to refresh. The Organization or System Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Refresh** in the row for the monitor you want to refresh.

The System Visibility Console screen refreshes and the "Last tested" information next to the monitor name updates to the current time and date.

The Testing history field on the monitor details screen also updates, displaying the time and date you manually refreshed the monitor with the words *Manually Run Test.*

View the diagnostic log

The diagnostic log allows you to view various logs and events and export that information to a .csv file, which can be then sent to BlackBerry AtHoc customer support for troubleshooting purposes. You can export a maximum of 30,000 events.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Diagnostic Log**. The diagnostic log appears.
3. Optionally, click **Refresh** to refresh the log manually and show the most recently received alerts.
4. Optionally, click **Clear Log** to remove all entries from the log.

   Note: You must be logged in to the System Setup (3) organization and have system administrator permissions to clear the diagnostic log
5. Optionally, click **Export** to export the contents of the log to a .csv file.
6. Click **Current Page** or the number of events that you want to export.

Run a basic search of the diagnostic log

To limit the number of events displayed in the diagnostic log, you can run a basic search.

1. On the **Diagnostic Log** page, in the **Search** field, enter a single search criteria such as an event ID, event type, or server name.
2. Click 🔍.

Run an advanced search of the diagnostic log

To limit the number of events displayed in the diagnostic log, you can run an advanced search.

1. On the **Diagnostic Log** page, click **Advanced**.
2. In the **Advanced search** section, enter search criteria in any combination of the following fields:

   - Event Id
   - Type
   - Server
   - Assembly
   - Module
   - Member
   - Short Message
   - Time
   - Thread Id
3. Click **Search**.

View geolocation transactions and logs

Administrators can bulk update users' physical addresses using the BlackBerry AtHoc User Sync client.

When a bulk update transaction is submitted, the Geocoding Summary and Logs settings page displays the following information:

- Date and time the transaction was submitted.
- User name of the person who initiated the transaction.
- Organization name of the users whose geolocation attributes were updated.
- The total number of records included in the transaction.
- The number of records that were successfully processed.
- The number of records that were not processed.
- The current status of each transaction.
- A link to download the log of each transaction.

The status of each transaction can be any of the following:

- **Pending**: The transaction has not yet been submitted to the API for processing.
- **In Progress**: The transaction has been submitted to the API, but the API response is not complete.
- **Partially Processed**: The API has processed some of the transaction, but is not complete. This status is usually only seen for larger transactions of over 200,000 records.
- **Completed**: The transaction is complete and all job records were successfully processed.
- **Partially Complete**: The transaction is complete but some records failed.

Note: For more information about bulk updates of users' physical addresses using the BlackBerry AtHoc User Sync client, see "How to bulk update users' physical locations" in the *BlackBerry AtHoc User Sync Client* guide.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Geocoding Summary and Logs**.
3. Optionally, change the **From** and **To** fields to view transactions from a different date range and then click **Search**. The default is 1 day.
4. Optionally, click **Clear All** to remove all transactions.
5. Optionally, click **Download to Excel** to export all displayed transactions to a .csv file.
6. Optionally, click **Download Log** in the row for a transaction to download the details of that transaction to a .csv file.

Database archiving

Database archiving is an important system task. If the database becomes full, the system will fail. From the Database Archiving Job system task, users with enterprise administrator or system administrator permissions can see the current size of databases and execute the archiving job as needed. A warning displays on the BlackBerry AtHoc homepage when the database size reaches 90% of capacity.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Archive**.

   Note: If archiving needs to be performed, a status message appears at the top of the Database Archiving screen.

5. Review the details on the **Database Archiving** screen to determine which database or databases will be archived. You can do this by comparing the current size of each database against the maximum size allowed. If previous archiving jobs have been run, details of those jobs appear in the History table below the Database Status table.
6. Click **Archive**.
7. On the **Database Archiving Activation** screen, read the entire screen of explanations and cautions about archiving.
8. In the **Data Deletion Settings** field, specify the minimum number of days old data must be in order to be archived.
9. Select the check box at the bottom of the screen to indicate you have read the explanations and understand the conditions.
10. Click **Start Archiving Job**.

    Note: If an archiving job seems to be running for a long time, check the BlackBerry AtHoc process status to make sure that the service is running.

Organizations Manager

Use the Organizations Manager to create organizations for your system.

Note: Administrators who manage multiple organizations must be assigned the system administrator role. Having only the administrator role is not sufficient and does not allow assigning operator roles in other organizations.

To assign roles, see "Grant operator permissions to a user" in the *BlackBerry AtHoc Operators Roles and Permissions* guide.

For detailed configuration steps, see "Configure the BlackBerry AtHoc management system for AtHoc Connect" in the *BlackBerry AtHoc Connect*guide.

Create an organization

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Organizations Manager**.
4. On the **Organizations Manager** page, click **New**.
5. Enter a name for the new organization.
6. Select one of the following organization types:
    - **Enterprise**: Choose this type if you are logged into the **System Setup (3)** organization and are creating an enterprise organization.
    - **Sub Organization**: Choose this type if you are logged in to an enterprise organization and are creating a member organization.
    - **Basic**: Choose this type if you are creating a basic organization.
7. Select a locale for the organization.
8. Click **Save**. Information about the new organization appears in the list.
9. To change the BlackBerry AtHoc interface to display the organization you just created, complete the following steps:
    a. In the navigation bar, click your username, and then click **Change Organization**.
    b. On the **Change Organization** screen, click the name of the organization you just created, and then click **OK**.
    c. The system refreshes and displays the new organization.
10. Configure the new organization using the tasks outlined in Configure a new organization.

Enable and disable features

Note: The Feature Enablement section is for internal use only.

You can enable and disable features at a system, enterprise, or individual organization level. You must have system administrator permissions to enable or disable features.

Feature enablement is inherited from parent organizations by default. Feature enablement on a system level is inherited by all organizations in the system. Feature enablement on an enterprise organization is inherited by its suborganizations. You can override these inheritance rules by explicitly enabling or disabling a feature on an enterprise or individual organization.

1. Log in to the management system as a system administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Feature Enablement**. The Feature Enablement page opens and displays the features currently available in the system.

   The Organization column displays the organization where the feature is explicitly enabled. The Enabled column displays the current status of the feature, and whether this value is due to inheritance. For example, True in the Enabled column indicates that the feature is enabled in the current organization, while Inherit (True) indicates that the feature is enabled due to inheritance rules.

   Note: If a feature has been explicitly enabled or disabled in the organization you are currently logged in to, the feature row appears in bold.
4. Click the row for the feature you want to enable or disable.
5. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True** to enable the feature, **False** to disable the feature, or **Inherit**. If you select Inherit, the feature status is inherited from the parent organization.

   Note: The Inherit option is not displayed for a system level organization.
6. Optionally, select the **Force all children to inherit** option if you want the feature status you are setting to be inherited by all child organizations, regardless of the feature status set on those child organizations.

   Note: This option is not available for sub organizations.
7. Click **Save**.

Note: Some features require additional steps before they are fully disabled. For more information, see Additional steps to disable features.

Additional steps to disable features

After you disable the following features on the **Feature Enablement** screen, they require additional steps to be performed before they are completely disabled. In the following table, the Default disable action column describes the state of the feature when it is disabled on the Feature Enablement screen. The Additional steps column describes the steps you need to perform after disabling the feature on the Feature Enablement screen.

Feature	Default disable action	Additional steps
IsAdvancedQuerySupported	• The Advanced Query section is hidden in alert templates. • Users targeted by advanced query in alert templates are removed. • Users targeted by advanced query are still targeted in existing alert templates.	Open and save the template.

Feature	Default disable action	Additional steps
IsCallBridgeSupported	• Existing alert templates do not display call bridge information. • Alerts published from the alert publishing page using an existing alert template display call bridge information.	Open and save the template.
IsDependentSupported	• Dependents are not displayed on alert templates. • Targeted user counts on alert templates are correct. • Alerts published from existing alert templates still target dependents. The number of targeted dependents is included in the targeting summary on the Alert Summary page and in reports.	Open and save the template.
IsIndividualUserTargetingSupported	• The targeted user count in existing alert templates is 0. • Alerts sent using existing alert templates can still target individual users.	Open and save the template.
IsMassDeviceTargetSupported	• The Mass Device section is not visible in existing alert templates. • The Mass Device section is not displayed on the Review and Publish window. • Alerts sent from existing alert templates are targeted to mass devices. • Targeted mass devices are displayed on the alert summary and in advanced reports.	Open and save the template.
IsPlaceholderSupported	• Placeholders are displayed during alert publishing. • Placeholder default values are displayed. • Placeholders are resolved after an alert is published.	Delete all instances of placeholders and save the template.

Feature	Default disable action	Additional steps
IsTargetByAreaSupported	• The Target By Location section is not displayed in alert templates. • The Targeted Users count in alert templates is not updated. • Alerts published from existing alert templates target users by location.	Open and save the template.
IsAccountabilitySupported	• All existing live events continue.	End all live events.
IsWAMSupported	• Background jobs do not support weather modules.	Disable all weather alert rules.
IsFillCountSupported	• Users are still targeted with fill count when sending an alert from an existing alert template.	Remove fill count criteria and save the template.
IsDeviceDeliveryOrderSupported	• Device delivery order is still supported on existing alert templates.	Open and save the template.
IsAlertTemplateSettingSupported	• The Content section still appears in template settings for existing alert templates. • The Content section does not appear when creating a new alert template.	Clear any custom settings and save the template.
IsChannelSupported	• The folder drop-down menu does not appear when creating a new alert template. • Folders can be created and folder restrictions can be added to existing alert templates.	Open and save the template.
IsDeviceOptionSupported	• Device options can still be set from an alert email. • Device options are disabled in the BlackBerry AtHoc management system.	Clear any custom device option settings and save the alert template.
IsDropboxSupported	• Existing alert templates continue to retrieve files from DropBox. • New alert templates do not display the DropBox option.	Remove links to DropBox and save the alert template.

Feature	Default disable action	Additional steps
IsGroupBlockingSupported	• Alerts are not sent to blocked users.	Clear user restrictions (blocked distribution lists or users) and save the alert template.
IsPrintAlertSupported	The **Print** button is still visible in the Report page.	This feature cannot be disabled.
IsSchedulingSupported	• Alerts sent from existing alert templates still end after the scheduled duration.	End or cancel all existing scheduled alerts in the organization.
IsScheduledLocationAccessSupported	• Scheduled location access continues to function for existing alert templates.	Clear all existing scheduled location access criteria in the organization.
IsRecordedAudioSupported	• Alerts published from existing alert templates still include audio files.	Remove all references to audio files and save the template.

Manage the agents for integrated devices

If you have the necessary permissions, the Integration Manager screen allows you to view and edit agents for communicating with external devices, such as fire panels.

Note: The full Configuration XML for public agents is visible on the System Setup (3) organization. For enabled organizations, only the relevant Configuration XML is displayed.

Provision applications that can call the web API

You can provision a new API integration with the BlackBerry AtHoc management system. You must have be an Organization Administrator, Enterprise Administrator, or System Administrator to provision applications. You must be a System Administrator to enable a provisioned application.

Note: The Client ID and Client Secret can only be used in the organization in which they are created. If the Client ID and Client Secret are created in the System Setup (3) organization, they can be used in any organization. If the Client ID and Client Secret are created in an enterprise organization, they can be used in any of that enterprise's suborganizations. If the Client ID provided does not follow these inheritance rules, a 400 (Bad request) error code is returned.

1. Log in to theBlackBerry AtHoc management system as an organization administrator, enterprise administrator, or system administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **API Applications**.
4. On the **API Applications** window, click **New**.
5. On the **New API Application** window, enter a name for the API integration.
6. (System administrators only) Next to **Status**, select **Enabled**.
7. In the **Authentication** section, select a Grant Type. The default is Password. If you select Implicit, enter a redirect URI in the text box that appears.

8. Click **Save**. A Success message appears that includes the Client ID and Client Secret.
9. Take note of the displayed Client Secret. It is displayed only once and will need to be regenerated if lost.

Note: After you provision your application in the BlackBerry AtHoc management system, contact BlackBerry AtHoc customer support to have the application reviewed and enabled.

Reset the client secret

If you need to reset the client secret for your API integration, complete the following steps:

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **API Applications**. The API Applications window opens.
4. Optionally, enter a name in the search box to filter the list of applications.
5. Optionally, select **Enabled Applications** or **Disabled Applications** from the **All Applications list** to filter the list of applications.
6. Click the application you want to modify.
7. Click **Reset Client Secret**. A confirmation window opens.

   Note: Any existing calls to the selected API with the existing client secret will be blocked when you reset the client secret.
8. Click **Continue**. You are returned to the API application window. The new client secret is displayed.
9. Take note of the displayed client secret.
10. Click **Save**.
11. Add the new client secret to your authentication payload.

Configure API throttling settings

Note: The API Throttling section is for internal BlackBerry AtHoc use only.

Throttling of API usage is required to protect BlackBerry AtHoc server resources from being over-used, or used in ways that are not intended by BlackBerry AtHoc that can result in slow responsiveness. Throttling limits are applied to overall API usage by any single caller, client, organization, or endpoint. If an API call has reached its throttle limit, the server returns a 429 (Too Many Requests) error.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **API Throttling**.
5. On the **API Throttling** page, complete the steps in the following topics to configure client and endpoint whitelists, general rules, and client rules.
6. Click **Save**.

Whitelist

In the Whitelist section, System Administrators can specify endpoints and clients to be whitelisted. Whitelisted clients and endpoints are exempt from API throttling.

1. Select one or more clients from **Client Whitelist** pull-down menu to add them to the whitelist.
2. Click **Add Endpoint** to add an endpoint to the whitelist. A new row appears in the list.

   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. In the **URL** field, enter a URL.

c. Click **Save**.

The endpoint is added to the endpoint whitelist.

3. Optionally, click ✎ to edit an endpoint.
4. Optionally, click ✖ to remove an endpoint.

General rules

In the General Rules section, system administrators can add general rules that apply to all endpoints.

1. Click **Add General Rule**. A new row appears in the list.
   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. Optionally, in the **URL** field, append a URL to **api/v2/**. Use ***** as a wildcard in a URL. Enter only ***** to specify all endpoints.
   c. Specify a time (in minutes) and a limit for the number of requests.
   d. Click **Save**.
2. Optionally, click ✎ to edit a general rule.
3. Optionally, click ✖ to remove a general rule.

Client rules

In the Client Rules section, system administrators can add rules that apply to specific clients. Rules applied to a specific client override rules specified in the General Rules section.

1. Click **Add Client Rule**.
2. In the **Add Client Rule** window, select a client from the pull-down list.
3. Click **Add Client Rule**. A new row appears.
   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. Optionally, in the **URL** field, enter the client URL.
   c. Specify a time (in minutes) and a limit for the number of requests.
   d. Click **Save**.
4. Optionally, repeat Step 3 to add additional client rules. You can add multiple rules for a single client.
5. Click **Add**.
6. Optionally, click ✎ to edit a client rule.
7. Optionally, click ✖ to remove a client rule.

View the operator audit trail

The operator audit trail enables authorized users to audit the system based on a specific operator or action performed in the BlackBerry AtHoc system, such as login attempts or password changes. The operator audit trail retains data for 6 months.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Operator Audit Trail**.
3. From the **Operator Audit Trail** screen, you can perform any of the following actions:
   - Change the report time frame by selecting different **From** and **To** dates. Enter the dates manually or click 📅 and select each date on the pop-up calendar. The report that is generated will then include activities between and including the To and From dates you select.
   - Enter an operator name or ID in the **User** field to view their activity in the system. If no value is entered in this field, all operators are included in the report.

Note: The User field is not case-sensitive. You can use the **?** wildcard as a substitute for a single letter or the ***** wildcard as a substitute for a string of letters.

- View all activities by leaving the **Entity** field set to the default value of **All Entities** or view activities for a specific entity by selecting one from the list.

  To further filter activities, select an entity and then select **Search by Specific Action(s)**. In the **Action(s)** field, click the list and select each of the actions that you want to use as filter criteria.

  Note: If you apply filtering criteria, you must click **Search** to refresh the screen and view the updated results list.
- Export or print the System Log Report by completing either of the following steps:
  - If Microsoft Excel is installed on your computer, click **Download excel file**, then either save the report to a location on your machine or open the report directly.
  - Click **Printer friendly report** to view the formatted report in a new browser window, then use the browser's **Print** command to print the report.

View an alerts usage summary report

Alerts Usage Summary reports are used to determine how many reports or messages have been sent out within a designated amount of time. To create one of these reports, see "Create and view an alerts usage summary report" in the the *BlackBerry AtHoc Alert Tracking and Reporting* guide.

Manage system jobs

You can manage common system jobs such as database archiving and purging log data in BlackBerry AtHoc. If you have administrator permissions, for each system job you can do any of the following:

- View the status of historical runs (start time, end time, duration, result.)
- Determine the next scheduled run date and time.
- Manually run the system task.

View details about system jobs

The System Tasks screen displays a list of all automated jobs in the system.

1. Log in to the BlackBerry AtHoc management system.
2. Click the down arrow beside your log in name and select **Change Organization**.
3. Change to the **System Setup (3)** organization.
4. In the navigation bar, click ⚙.
5. In the **System Setup** section, click **System Jobs**.
6. On the **System Tasks** screen, click the name of any task to view additional details.
7. On the task details screen, you can perform any of the following tasks:
   - View a description of the task.
   - View the run interval, the last run time, and last run result for the task.
   - View a history of the most recent runs of the task, including the start time, end time, duration and result of each run.
   - Click **Click to Disable** or **Click to Enable** to change the status of the task.
   - Click **Run now** to manually initiate the task.
   - Click **OK** in the **Result** column in the **History** section to view the job log for any recent run.

Descriptions of System Jobs

The following jobs are displayed on the System Tasks screen:

- **AtHoc Connect Update Alert Responses**: This job updates AtHoc Connect with organization alert responses.
- **AtHoc Connect User-Base Sync**: This job synchronizes the IAC user base with the agreement state in AtHoc Connect.
- **Auto Delete Users**: This job deletes end users based on the settings configured on the Disable and Delete End Users screen.
- **Auto Disable Users**: This job disables end users based on the settings configured on the Disable and Delete End Users screen.
- **Batch Geocoding: Postprocessor**: This job verifies job statuses, downloads, processes submitted requests, updates the database, and sends an email for the completed uploads.
- **Batch Geocoding: Preprocessor**: This job creates Bing batch geocoding requests if the addresses are not found in the local geocoding lookup table.
- **Cap Event Processor**: This job processes captured inbound CAP events and publishes an alert for each inbound alert based upon the rules configured for the agent.
- **Cap Feed Poller**: This job fetches the index feed and creates a queue entry in the BlackBerry AtHoc database queue.
- **Delivery Batch Recovery**: This job recovers batches with incomplete delivery due to gateway related failures.
- **Delivery Batch Retry**: This job resets delivery batches that have either timed out or completed with error.
- **Desktop Sessions Maintenance**: This job cleans up stale sessions and updates the online users graph that is visible on the homepage.
- **Email Publisher**: This job processes alert publishing requests that are sent by email.
- **External Events - Orgs Sync**: This job provisions organizations for external events.
- **Feed Poller**: This job polls feeds from various sources.
- **Feed Processor**: This job processes feeds from various sources.
- **IEM IPAWS Plugin Agent - For All VPS**: This job communicates with IPAWS for all organizations on the server.
- **Process Accountability Event Job for Recipient Re-Compute**: This job manages accountability event recipient re-computation.
- **Process Accountability Event Job for Reminder**: This job manages accountability events related to sending reminder alerts.
- **Process Accountability Events for End**: This job manages accountability event lifecycle and status management.
- **Process Accountability Events for Status Update**: This job manages the status attribute value changes for affected uses during the accountability event lifecycle.
- **Process Accountability Events Tracking Summary**: This job manages the accountability events tracking summary.
- **Process Alerts Tracking Summaries**: This job generates an alert tracking summary for live alerts and alerts that have ended within the past 4 hours.
- **Process Geo Fencing**: This is a background job that is used for geofence targeting to send alerts to users who enter a specified location during a live alert.
- **Process Inbound Event for Report Category**: This job manages the triggering alert for Report Inbound Event.
- **Process NDMS Tracking - ATHOC-NDMS-EAST**: This job retrieves tracking data from AtHoc Cloud Delivery Service (East) and updates Alert reports within the system.
- **Process NDS Tracking- ATHOC-NDMS-WEST**: This job retrieves tracking data from AtHoc Cloud Delivery Service (West) and updates alert reports within the system.
- **Process OEM Tracking - UAP-OEM-EAST**: This job retrieves tracking from the OEM Cloud Delivery Service (East) and updates alert reports within the system.

- **Process OEM Tracking - UAP-OEM-WEST**: This job retrieves tracking from the OEM Cloud Delivery Service (West) and updates alert reports within the system.
- **Process Situational Response Incident Steps for End**: This job manages ending incident steps for ended alert and events.
- **Purge Older Logging Data**: This job removes any temporary or transient data from the database tables that is no longer required. Runs daily at 11:00 PM.
- **Rebuild Database Indexes**: This job performs weekly index maintenance on the databases.
- **Sync Cross System Dist Lists**: This job synchronizes Distribution Lists within the master organization with the latest distribution lists in sub organizations.
- **System Diagnostics Report**: This job runs diagnostic stored procedures and collects the output in a diagnostic log.

Create and export a system diagnostics report

During a service call, BlackBerry AtHoc customer support might ask you to export the System Diagnostics Report and then send the results to them. The System Diagnostics Report job runs every day at 12:00 PM and the report appears in the Diagnostic Log as an event. If asked, you might also need to run the report job before exporting the report.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **System Jobs**. The System Tasks screen opens, displaying a list of all automated jobs in the system.
3. If requested by BlackBerry AtHoccustomer support, run the diagnostics job by completing the following steps:

    a. Click **System Diagnostics Report** at the bottom of the tasks list.
    b. On the **System Diagnostics Report** screen, click **Run now**.
4. After the report runs, click ⚙.
5. In the **System Setup** section, click **Diagnostic Log**.
6. Use the search field at the top of the screen to find all of the System Diagnostics Reports in the system.
7. In the results list, click the most recent report to open it.
8. Click **Export** at the top of the screen.
9. When prompted, save the diagnostic log to the default file, `AtHocEventViewer.xml`.
10. Send the report to your contact in BlackBerry AtHoc customer support.

Purge ended alerts

System administrators, enterprise administrators, and organization administrators can enable alert purging by selecting purge criteria for an organization. The purge criteria is the number of days after an alert or event has ended.

Important: Purged alerts and events cannot be recovered.

The purge deletes all ended alerts, events, and their related attachments from the system. Purging ended alerts and events is disabled by default and can be enabled per organization. Suborganizations do not inherit purge criteria from the enterprise organization.

Any changes made to the purge criteria take effect at the next scheduled purge.

Only ended alerts and events are purged. Drafts alerts and events, templates, manual logs, the operator audit trail, and scheduled and recurring alerts are not purged.

For events, purge criteria are applied after the last alert for the event is published. For example, if an event is for 30 days with one recurring alert per day, and the purge criteria is set to 120 days, then all 30 alerts are purged on the 121st day after the last alert for the event is ended.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Purge Ended Alerts**.
3. Optionally, in the **Status** section, click the link in the in the **Result** field to view information about the last purge job, including the date of the last purge and the number of alerts that were purged.
4. In the **Schedule** section, select the purge criteria from the **Purge Ended Alerts** list. You can select to purge ended alerts and events after 90, 120, or 180 days.
5. Click **Save**.

Manage SMS Opt-In

SMS Opt-In enables operators to allow community members, visitors, event participants, or other users outside of their organization to subscribe to receive alerts by SMS. These outside users can subscribe to receive alerts by sending a text event code via SMS.

Organization Administrators create event codes, and then share the event code and the short code with users. When a user opts-in by sending an SMS with the event code, they are added to the BlackBerry AtHoc management system. Operators can then target them in alerts.

Entries are added to the operator audit log when SMS Opt-In is enabled or disabled.

Configure the SMS Opt-In service URL

The SMS Opt-In service URL is pre-populated with the following URL: `https://optin.athoc.com`. Configuring a different SMS Opt-In service URL is optional.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. Click ⚙.
4. On the **Settings** page, in the **System Setup** section, click **System Settings**.
5. On the **System Settings** page, click **Edit**.
6. Scroll down to the **Advanced Settings** section.
7. In the **SMS Opt-In Service** section, enter a URL in the **Service URL** field.
8. Click **Save**.

Activate SMS Opt-In

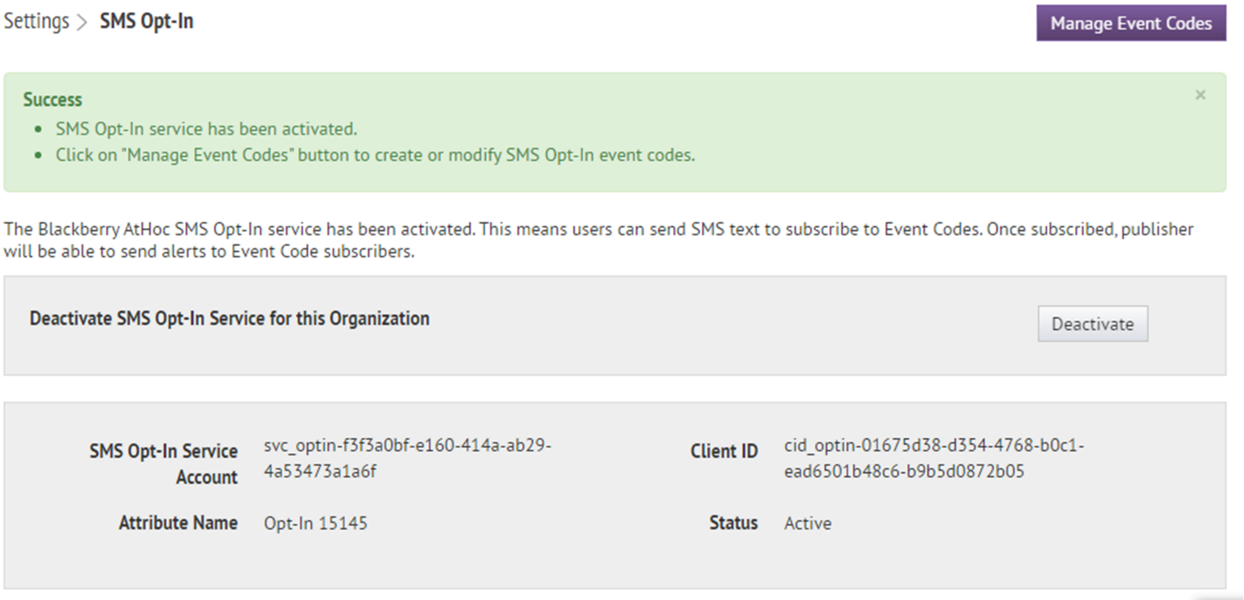
Before you begin:

- You must be an Organization Administrator, Enterprise Administrator, or System Administrator to enable and activate SMS Opt-In.
- SMS Opt-In is disabled by default. To enable it, log in as a System Administrator and go to **Settings** > **System Setup** > **Feature Enablement** and set the IsSMSOptInEnabled feature to True.

Entries are added to the operator audit log when SMS Opt-in is enabled or disabled.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **Users** section, click **SMS Opt-In**.
4. On the **SMS Opt-In** page, click **Activate**.

- A success message and details about the SMS Opt-In service are displayed on the **SMS Opt-In** page.
- A multi-select picklist attribute is automatically created that can be used to target users in alerts.


Settings > SMS Opt-In

Success

- SMS Opt-In service has been activated.
- Click on "Manage Event Codes" button to create or modify SMS Opt-In event codes.

The Blackberry AtHoc SMS Opt-In service has been activated. This means users can send SMS text to subscribe to Event Codes. Once subscribed, publisher will be able to send alerts to Event Code subscribers.

Deactivate SMS Opt-In Service for this Organization

SMS Opt-In Service Account	svc_optin-f3f3a0bf-e160-414a-ab29-4a53473a1a6f	Client ID	cid_optin-01675d38-d354-4768-b0c1-ead6501b48c6-b9b5d0872b05
Attribute Name	Opt-In 15145	Status	Active

Make the Opt-In user attribute available for targeting and user management

When you enable SMS Opt-In, an Opt-In user attribute is automatically created. In order to target users in alerts and events using this SMS opt-in user attribute, you must make it available for targeting.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, in the **Layouts** section, click **View/Edit** beside **Targeting Settings** .
5. On the **Group Targeting Definition** window, in the **Available Fields** column, click the **Opt-In** *<opt-in-number>* attribute.
6. Click **Add**.
7. Optionally, use the control buttons on the right to move the Opt-In attribute higher or lower in the **Selected Fields** list.
8. Click **Save**.
9. On the **General Settings** screen, click **Save**.
10. In the navigation bar, click **Users** > **User Attributes**.
11. On the **User Attributes** screen, click the **Opt-In** *<opt-in-number>* attribute.
12. On the user attribute details page, in the **Page Layout** section, select a value from the **User Details - Full Page** pull-down menu. Do not leave this option set to **Do Not show**.
13. Click **Save**.

Create an event code

Create an event code so that you can target users outside your organization with SMS alerts.

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event Codes**.
4. On the **Manage Event Codes** page that opens in a new tab on your browser, click **New**.
5. On the **Create New Event code** window, enter an event code name. Spaces and the following characters are not allowed: `!$%&^()={},;\:?"<>|\
6. In the **Event Code** field, enter an event code. This is the code that you will provide to your end users. They send this event code in an SMS to subscribe to alerts.
7. Optionally, in the **Expiration** field, select a date for the event code to expire. When an event code expires, users can no longer use the event code.
8. Click **Save**.

After you finish: When you promote your event code, include the following text: `Text` *`[event-code]`* `to` *`[sms-number]`*. If you do not know the SMS number, see SMS numbers for U.S. hosted systems and SMS numbers for European hosted systems.

SMS numbers for U.S. hosted systems

Country	Primary SMS number	Backup SMS number
Canada	73101	73102
Japan	81502	80447
New Zealand	2316	2575
United Arab Emirates	3775	6991
United States	28462	73101

SMS numbers for European hosted systems

Country	Primary SMS number	Backup SMS number
Canada	555666	333666
Croatia	815517	815518
Japan	85136	80447
New Zealand	4840	8434
United Arab Emirates	1727	2496
United Kingdom	65165	65465
United States	333666	444666

Edit an event code

Event codes can be edited until they expire. Event codes cannot be deleted.

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event codes**.
4. Optionally, on the **Manage Event Codes** window, enter an event code in the **Search** field and click 🔍 to narrow the list of event codes.
5. On the **Manage Event Codes** window, click ✎ on the row for the event code you want to edit.
6. Optionally, update the **Event Description**, **Event Code**, and **Expiration** fields.
7. Click **Save**.

Deactivate SMS Opt-In

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. Click **Deactivate**.

Configure device gateways

To set up alert delivery devices, you must configure the gateway for each device. The gateway is an API that translates alert text to XML format and delivers it to the provider for a device. The provider can be a BlackBerry AtHoc service such as AtHoc cloud telephony or a third-party provider.

Note: When a device delivery gateway is added, deleted, reordered, or configured, it is captured in the operator audit trail. To view these entries in the operator audit trail, click ⚙ > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select specific actions from the **Action(s)** list.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click the name of the device gateway that you want to configure.

   The gateway configuration settings screen opens. The values that you need to provide depend on the device you want to configure. The following table describes how you can find configuration values for a particular device.

Gateway	Documentation
ADT Giant Voice	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
AM Radio Broadcast	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
AM Radio Transmitter	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
American Signal Giant Voice	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
American Signal Giant Voice - V2	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
AtHoc Cloud Delivery Service (East Coast)	Configure the hosted gateway for cloud services
AtHoc Cloud Delivery Service (West Coast)	Configure the hosted gateway for cloud services
Mobile App	Configure the BlackBerry AtHoc mobile app
AtHoc Connect	*BlackBerry AtHoc Connect*
ATI Giant Voice	*BlackBerry AtHoc ATI Giant Voice System Installation and Configuration Guide*

Gateway	Documentation
Benbria Classroom Emergency Notification	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
BlackBerry Messenger	*BBM Enterprise Alerts Installation and Administration Guide*
Cable TV + Radio	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Cable TV Scroller	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Cisco IP Phone Display	*BlackBerry AtHoc IP Phone Gateway Setup and Operation Guide for Cisco IP Phone Blast*
Cisco UCM (Blast)	*BlackBerry AtHoc Cisco IP Phone Blast NDS Installation Guide*
Cisco UCM (TAS)	*BlackBerry AtHoc Telephony Alerts System Operations Guide*
Cisco Unified Communication Manager	*BlackBerry AtHoc Telephony Alerts System Operations Guide*
Desktop App	• Configure desktop app settings • *BlackBerry AtHoc Desktop App Installation and Configuration Guide*
Eaton WAVES	*BlackBerry AtHoc Eaton WAVES Giant Voice System Installation and Configuration Guide*
Emergency Digital Information Service (EDIS)	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Federal Signal Giant Voice	*BlackBerry AtHoc Federal Signal Giant Voice System Installation and Configuration Guide*
IPAWS CAP Exchange, EAS, NWEM, and WEA,	*BlackBerry AtHoc IPAWS Plug-in for NDS Installation and Configuration Guide*
Land Mobile Radio	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.

Gateway	Documentation
Land Mobile Radio - Eastman	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
LRAD Giant Voice	*BlackBerry AtHoc LRAD Giant Voice System Installation and Configuration Guide*
Microsoft Lync Server	*Microsoft Lync Server 2013 Plug-In for NDS Configuration Guide*
Monaco Warning System	*BlackBerry AtHoc Monaco Warning System Installation and Configuration Guide*
Motorola ACE 3600	*BlackBerry AtHoc Motorola ACE3600 Installation and Configuration Guide*
OEM Cloud Delivery Service (East)	Configure the hosted gateway for cloud services
OEM Cloud Delivery Service (West)	Configure the hosted gateway for cloud services
On-Premise Email	—
RGM Digital Signage	*BlackBerry AtHoc Digital Signage Installation and Configuration Guide*
RSS Feed	Configure RSS feed information for RSS and Atom content feeds
SiRcom	*BlackBerry AtHoc SiRcom Installation and Configuration Guide*
Talk-A-Phone Giant Voice	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
TechRadium	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Text Messaging	Configure the text messaging device for hosted SMS
TTY/TDD Phone	Manage a TTY/TDD phone device
Twitter	*BlackBerry AtHoc Twitter Configuration and User Guide*
Whelen Giant Voice, v1	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.

Gateway	Documentation
Whelen Giant Voice, v2	*BlackBerry AtHoc Whelen Giant Voice System Installation and Configuration Guide*
Xml Feed	Configure XML feed information for mass communication devices
Xml Feed Reset	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Zetron Pager	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway.
Zetron Pager Group	Custom device gateway: Contact BlackBerry AtHoc customer support if you need to configure this gateway

3. Configure the values based on the device and information provided by BlackBerry AtHoc customer support or the configuration information provided in the referenced documents.
4. Click **Save**.

Configure the BlackBerry AtHoc mobile app

Use the Devices screen to verify available devices, check settings, and if necessary, disable or restore specific devices such as mobile devices for the Personal Safety Service. You can also control and edit permissions to make certain device addresses only available to operators, or to end users, or to both roles.

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

For more information about Mobile App settings, see "Configure mobile alert settings" in the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

Configure the mobile app gateway

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

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

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mobile App**.

   The Mobile App gateway configuration screen opens with the default settings that are listed in the following table.

Option	Description
Notification Delivery Server Settings	
Notification Delivery Server Address	`https://mobile.athoc.com`

Option	Description
Username	Must be between 3 and 100 characters long.
Password	Must be between 3 and 100 characters long.
Debug Trace	**Default:** No Yes Avoid performance degradation by enabling debug tracing for the mobile delivery gateway only while actively debugging the mobile notifications for the mobile app.
Features	
Alerts	Selected. Available for all users.
Collaboration	Selected. Available for all users and operators.
Map	Not selected. Available for all users.
Alert Publishing	Selected. Available for operators only.
Advanced Features	Selected. When selected, advanced features display. Select a distribution list to give access to advanced features to a group of users. Options include: • Emergencies • Check In/Check Out • Reports • Tracking: When this option is selected, the Tracking Interval option displays. Select a tracking interval. • My Profile Page: When this option is selected, the "Show Preferred language selection to support bilingual alerts" option displays. For more information about advanced features, see Role-based permissions for the mobile app.
Settings	
Photo Quality	**Default:** Low High
Video Quality	**Default:** Low High

Option	Description
Emergency Contact Number	Designate the emergency contact telephone number. If no phone number is entered in the field, the mobile app will not have an emergency contact number button.
Support Email Address	Enter an email address that administration log and feedback from the mobile app can be sent to.
Enable Mobile Analytics	Collects mobile app usage analytics. No personal, private, or sensitive information is collected. **Default:** No Yes
Enable Personal Alert Button	Enables sending an emergency using a paired personal alert button. Emergencies must be enabled in Advanced Features. **Default:** Yes No
Enable Jail-Break/Root Detection	Enables the mobile app to check if the device OS security has been compromised. **Default:** No Yes
Send Location with Response	Sends user location information with alert or event responses. **Default:** Yes No
User Choice	Enables each mobile user to choose whether to send location information with alert or event responses. **Default:** No Yes This option is visible only when "Yes" is selected for Send Location with Response.

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

3. Click **Copy Default Settings**.
4. In the **Notification Delivery Server Address** field, enter the NDS address you received from your system administrator. By default, the URL points to `mobile.athoc.com`.
5. Add the user name and password provided by BlackBerry AtHoc.
6. In the **Features** section, select the options that will be available to users when they are using their mobile device:

- **Alerts**: Users can receive alerts.
- **Collaboration**: Enables the Collaboration feature for all users and operators.
- **Alert Publishing**: Operators can publish alerts.
- **Advanced Features**: Advanced features are available to a selected group of users. When you select this option, advanced features are displayed. Each mobile feature in the Advanced Features section includes its own menu to select a distribution list. To learn about the advanced features, see Role-based permissions for the mobile app.

7. In the **Settings** section, select the photo and video quality.
8. In the **Emergency Contact Number** field, enter the phone number of the operations center to which emergencies are sent from mobile devices.
9. In the **Support Email Address** field, enter an email address where logs are sent for error debugging.
10. In the **Enable Mobile Analytics** section, select whether to enable the mobile app to collect usage analytics.
11. In the **Enable Personal Alert Button** section, select whether to enable users to send an emergency duress message using a paired personal alert button.
12. In the **Enable Jail-Break/Root Detection** section, select whether to enable the mobile app to check if the device OS security has been compromised.
13. In the **Send Location with Response** section, select whether to send location information with alert or event responses. When **No** is selected, location information is prevented from being returned with alert or event responses even if mobile location services are active on the mobile device.
14. In the **User Choice** section, select whether to enable mobile users to choose to send location information with alert or event responses. This option is only available when **Yes** is selected in the **Send Location with Response** section.
15. Click **Save**.

Assign an AtHoc mobile gateway to a phone

To assign an AtHoc mobile gateway to a phone and set up mobile phone notification, see Configure mobile phone notification.

Configure mobile phone notification

After BlackBerry AtHoc customer support has set up the correct Notification Delivery Server (NDS) address, you can assign an AtHoc mobile gateway to the phone and enable mobile phone notification.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, click **Mobile App**.
4. On the **Mobile App** page, click **Edit**.
5. In the **Name** field, enter `Mobile App`.
6. In the **Common Name** field, enter the following text with no space between the words: `mobileNotification`.
7. In the **Delivery Gateways** section, click **Add a Delivery Gateway** > **Mobile App**.
8. Click **Save** in the top menu bar.
9. Click **More Actions** > **Enable** in the top menu bar if the device is not yet enabled.

Role-based permissions for the mobile app

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

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

   Note: Only one distribution list can be used for the organization.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Mobile App**.
4. On the **Mobile app** screen, in the **Features** section, select **Alerts** to grant permission to receive alerts on mobile devices.
5. Select **Alert Publishing** to provide publishing permission to operators.
6. Select **Advanced Features** to provide advanced features to a group of users. When selected, the **Select advanced features** section appears.
7. In the **Select advanced features** section, select one or more features and distribution lists that the user can access from the mobile app:

   - **Emergencies**: Send duress messages.
   - **Check In/Check Out**: Perform user check-ins and check-outs on the map.
   - **Reports**: Send field reports.
   - **Tracking**: Track mobile device location for a specified amount of time.
   - **My Profile Page**: Enable users to edit their My Profile page and manage their organization subscriptions.

     When selected, the **Show Preferred language selection to support bilingual alerts** option appears. Select this option to display the Preferred Language field on the My Profile screen on the mobile app. This option enables users to choose to receive alerts in their preferred language.
8. After selecting an advanced feature, choose a distribution list that can use the selected feature.
9. Make any other needed changes for the mobile app settings.
10. Click **Save**.

Configure devices overview

You must specify the devices that users receive alerts on. For example, a user can receive an alert on multiple devices, including smart phones, SMS, tablets, desktop pop-ups, work or home phones, through loudspeakers, or email.

Perform the following high-level tasks to configure devices that end users receive alerts on:

1. Enable devices on the BlackBerry AtHoc server.
2. Configure the device delivery gateway.
3. Configure and enable the device from the Devices screen.
4. Verify that the device appears in the End User details display settings.

For additional configuration steps that must be completed for mass communication devices, see Manage mass communication devices.

Enable devices on the BlackBerry AtHoc server

The first step in configuring devices for BlackBerry AtHoc is to enable the device on the BlackBerry AtHoc server. When you enable the device, it appears in the list of gateways on the Settings screen and in the list of devices in Devices.

1. Log in as an administrator to the server that BlackBerry AtHoc runs on.
2. Navigate to the following folder: `../Program Files (x86)/AtHocENS/ServerObjects/Tools`.
3. Open the following application: `AtHoc.Applications.Tools.InstallPackage`.
4. On the **Configure Device Support** screen, select the check boxes next to each device needed for the organization.
5. Click **Enable**.
6. Click **Close**.

Duplicate a device on the BlackBerry AtHoc server

You must apply Hot Fix release HF-304 before you can duplicate a device on the BlackBerry AtHoc server.

When you enable a device on the BlackBerry AtHoc server, you have the option to create a duplicate of that device. Only Giant Voice devices can be duplicated. If you attempt to duplicate a non-Giant Voice device from the Configure Device Support screen, an error is displayed.

When you duplicate a device, it appears in the list of gateways on the Settings screen and in the list of devices in the Devices screen with a "-DUP1" extension. You can create additional duplicates of the same device, as needed. Each duplicate is appended with a new "-DUP#" extension. For example, ATI-DUP1, ATI-DUP2, and ATI-DUP3.

You can duplicate a Giant Voice device up to six times. There is a 30 character limit to the ID of the duplicated device.

1. Log in as an administrator to the BlackBerry AtHoc server.
2. Navigate to the following folder: `../Program Files (x86)/AtHocENS/ServerObjects/Tools`.
3. Open the following application: `AtHoc.Applications.Tools.InstallPackage`.
4. On the **Configure Device Support** screen, select the check box next to the device you want to duplicate.
5. Click **Duplicate**.
6. Optionally, click **Enable**.
7. Click **Close**.

Configure devices

If you are an administrator, you can use the Devices screen to verify available devices, check settings, set the device delivery priority for enabled personal devices, and enable and disable devices. You can also control and edit permissions to make certain device addresses available only to operators, or to end users, or to both roles.

Availability of delivery devices other than the AtHoc desktop software depends on the BlackBerry AtHoc edition and licensed delivery devices. Contact your BlackBerry AtHoc account manager for details.

Note: When a device's common name, display name, group order, or contact information is updated, it is captured in the operator audit trail. To view these entries in the operator audit trail, click ⚙ > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select specific actions from the **Action(s)** list.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.

   The **Personal Devices** tab of the Devices screen displays the available devices and their details in a table with the following columns:

   - **Device Name**: Displays a description of the device type.
   - **Delivery Gateway**: Displays the designated delivery gateways, if applicable.
   - **Group**: Displays the type of alert that gets delivered, such as email or phone.
   - **# Users**: Displays the number of users that have the personal device enabled in their profile.

   Disabled devices are grayed out in the display. Disabled devices are not available for delivering alerts. Each device has a default delivery template that defines the appearance and formatting used to deliver alerts.
3. Optionally, set device delivery priority.
4. Optionally, use the **Search For Device** 🔍 field to search for a device. Click **Advanced**, and select from the **Delivery Gateway**, **Group**, and **Status** drop-down menus to refine the search results.
5. Optionally, click the **Mass Devices** tab to view and edit mass devices.
6. Click the device name to configure the related template.

For more information on device configuration, see View and edit device details.

Enable and disable devices

If you have administrator permissions, you can use the Devices screen to disable and enable specific devices to control which devices appear in the user profile and to add them to the list of devices for alert targeting.

Enable a device

Only devices that have at least one associated gateway can be enabled. Although some devices have a gateway already assigned to them, for other devices such as Xml Feed, Twitter, or Zetron Pager, you must first open the device's details screen and add the gateway manually before you can enable the device.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, select the check box in the row for the device you want to enable.
3. Click **More Actions** > **Enable**.
4. Click **OK**.

Disable a device

1. From the list, select the check box in the row for the device you want to disable.
2. Click **More Actions** > **Disable**.

3. Click **OK**.

Set device delivery priority

Operators can set the priority of alert delivery by device type. When enabled, the device delivery preference feature prevents end uses from receiving the same alert on multiple devices. When configured, end users receive alerts on their enabled devices in the order specified at the organization level or at the alert level selected by the operator. End users can also set a device priority for the devices they have enabled and provided an address for in their user profile. By default, the device delivery preference is in this order:

- Mobile App
- Email
- Text Message
- Pager
- Fax
- Phone TTT/TDD Phone
- User Callback
- Lync

Additional enabled devices are added to the bottom of the list.

Note: The BlackBerry AtHoc desktop app does not support device delivery preference.

Note: When a device's delivery priority is changed, it is captured in the operator audit trail. To view this entry in the operator audit trail, click ⚙ > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select **Device Delivery Preference Updated** from the **Action(s)** list.

Before you begin:

- Device delivery preference must be enabled for your organization.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Devices**.
4. On the **Devices** page, on the **Personal Devices** tab, click **Edit**.
5. Optionally, to change the delay interval, select the number of minutes from the **Delay Interval** pull-down menu. The delay interval is the time in minutes that the system waits before sending an alert to the next device. The default delay interval is 2 minutes. The delay interval is consistent between each priority level.
6. Optionally, to change the delivery priority for any device in the list, click ↕ and drag the device to the desired priority position. When organization-defined or system-defined is selected in an alert or event template, the alert or event is targeted to devices in the order they appear in the list.
7. Click **Save**.

Add a device to the user details contact information

After you enable the gateway and configure the device on the Devices page, you might need to add the device to the list of available devices for end users. BlackBerry AtHoc provides a draft list that you might need to modify so that a user can add contact information in their profile.

Prerequisite

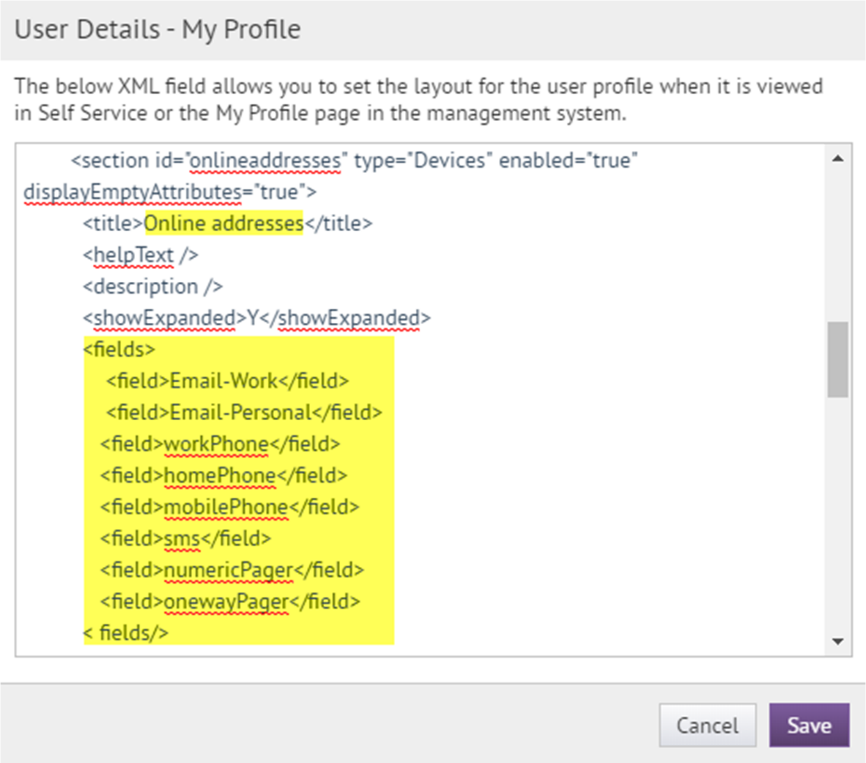
To add a device to the end user device display list, you must know its common device name. To determine a common device name, complete the following steps:

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. Click to open each device you need the common name for.

   The **Common Name** field appears in the **Details** section.
4. Write down the common name so that you can insert it when adding a device to the end user device list.

To add a device to the end user device display, complete the following steps:

1. Log in to BlackBerry AtHoc as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. Scroll down to the **Layouts** section.
5. In the **User Details - My Profile** row, click **View/Edit**.
6. In the **User Details - My Profile** window, scroll down to the **<Online addresses>** section.
7. Check to see if the needed devices are in the list. If not, manually add them in the XML file.



User Details - My Profile

The below XML field allows you to set the layout for the user profile when it is viewed in Self Service or the My Profile page in the management system.

```
     <section id="onlineaddresses" type="Devices" enabled="true"
displayEmptyAttributes="true">
      <title>Online addresses</title>
      <helpText />
      <description />
      <showExpanded>Y</showExpanded>
      <fields>
        <field>Email-Work</field>
        <field>Email-Personal</field>
       <field>workPhone</field>
       <field>homePhone</field>
       <field>mobilePhone</field>
       <field>sms</field>
       <field>numericPager</field>
       <field>onewayPager</field>
      < fields/>
```

8. If the devices are not in the list, add `<field></field>` values for each device using the common device names that you wrote down in the prerequisite section above.
9. Click **Save**.
10. On the **General Settings** page, click **Save**.

Manage mass communication devices

To manage support for a mass communication device such as a digital sign, a loudspeaker, or an XML feed, complete the following tasks:

- Enable devices on the BlackBerry AtHoc server
- Configure device gateways
- Configure devices
- Create a mass device endpoint

Mass device types and categories

Mass devices in BlackBerry AtHoc are divided into these categories: Giant Voice, Feed, Social, and Common.

The following table lists the supported mass devices and their categories.

Mass device	Mass device category
ALERTUS-BEACON	Giant Voice
AM-RADIO	Common
BENBRIA	Common
CATV	Common
EAS	Common
EMERGE-ENOTIFY	Common
FIRE-PANEL - 8 Channels	Common
FIRE-PANEL - 16 Channels	Common
GIANT-VOICE-ACE3600	Giant Voice
GIANT-VOICE-ATI	Giant Voice
GIANT-VOICE-FEDSIG	Giant Voice
GIANT-VOICE-WHELEN-V2	Giant Voice
IIM-LRAD	Giant Voice
IIM-SERIAL-GIANT-VOICE	Giant Voice
IIM-ZETRON-PAGER	Pager
IIM-ZETRON-PAGER-GROUP	Pager
INDUSTRIALSTROBE-BEACON	Common
LAND-MOBILE-RADIO-EASTMAN	Common
LAND-MOBILE-RADIO-V2	Common
MINITOR_V_TWO_TONE	Common

Mass device	Mass device category
MONACO-WARNING-SYSTEM	Giant Voice
MOTOTRBO_TWO-WAY_RADIOS	Common
PUBLIC-ADDRESS-SYSTEM	Common
PUBLIC-FEED (CWS)	Common
PUBLIC-FEED-V2 (CWS v2)	Common
SN-FEED (XML)	Feed
SN-FEED-SECONDARY (RSS)	Feed
SN-TWITTER	Social
UAP-DS (RMG Digital Signage)	Common
UAP-IAC	Common
UAP-IPAWS	Common
UAP-IPAWS-NWEM-EAS	Common
UAP-IPAWS-WEA2	Common
UAP-LED	Common
VOICE-DTMF	Giant Voice
Zetron Pager	Common

Create a mass device endpoint

To distribute messages through mass communication devices like a digital sign, you must create a BlackBerry AtHoc mass device endpoint. Creating a mass device endpoint makes the mass device available for targeting in alerts.

Mass devices are divided into these categories: Giant Voice, Feed, Social, and Common. Complete any of the following tasks to create mass device endpoints.

Note: You must have Operator or End Users Manager privileges to create a mass device endpoint.

Note: You can export the information about mass device endpoints to a .csv file by selecting the endpoints on the Mass Device Endpoints screen, and then selecting **More Actions** > **Export**.

Giant Voice

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.

4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **Configuration** section, select a Giant Voice Type: **Pole**, **Zone**, **Key**, or **Other**.
6. Enter the address for the Giant Voice device.
7. (For Giant Voice Key type only) Enter the **Giant Voice Key XML**.
8. Click **Save**.

Feed

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **General** section, enter a common name. Enter a value between 4 and 80 characters long. The following special characters are not allowed: (` ! $ % ^ ( ) = { } , ; : ? " < > | [space])
6. In the **Configuration** section, enter a title for the feed. Enter a value between 1 and 100 characters.
7. Optionally, enter a description for the feed.
8. Select whether to require authentication. The default is **No**. If you select **Yes**, enter an authentication username and password.
9. Optionally, enter a URL to use to access alerts through the content feed.
10. Click **Save**.

Social

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **Configuration** section, if no Twitter account already exists, click **Provide Twitter Credentials**.
6. On the **Twitter / Authorize an application** page, enter the account name and password for your Twitter account.
7. Click **Authorize app** to give permission to BlackBerry AtHoc to tweet to this Twitter account.
8. On the **New Mass Device Endpoint** screen, click **Save**.

Common

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.

5. In the **Configuration** section, enter the address for the mass device. The following special characters are not allowed: (`!^=<>)

View and edit device details

Note: You should consult BlackBerry AtHoc customer support before editing the values for a device to ensure that your changes will not have a negative impact on the way the device operates.

Note: You must have the enterprise administrator role to edit the details of a device.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, click to select a device.

   The screen refreshes to display the settings for the device, divided into the following three sections: Details, Help Text, and Delivery Gateways.

   The Details section varies by device. Use the Help Text section to change the help text in the targeting, contact, or contact information tool tip. The Delivery Gateways section provides information about device-specific gateways. A device must have at least one associated gateway before it can be enabled. For more information on enabling devices, Enable and disable devices.
4. Click **Edit** to modify the details, help text, or delivery gateway details.
5. Click **Save**.

Configure Giant Voice devices

The following integration gateways are related to Giant Voice loudspeaker systems:

- ADT Giant Voice
- American Signal Giant Voice
- American Signal Giant Voice - v2
- ATI Giant Voice
- Eaton WAVES
- Federal Signal Giant Voice
- LRAD Giant Voice
- Monaco Warning System
- SiRcom
- Talk-a-Phone Giant Voice
- Whelan Giant Voice - v1
- Whelan Giant Voice - v2

To learn how to configure Giant Voice gateways, see the BlackBerry AtHoc integrations documentation at the following URL: https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/integrations/

Configure the AtHoc Connect organization network

The Organization feature provides inter-agency communications between organizations that have joined AtHoc Connect. Organizations are members of AtHoc Connect that you can add as a connection. You can then publish alerts to that connection or subscribe to alerts that they publish.

To learn how to set up the gateway and device for AtHoc Connect, see the *BlackBerry AtHoc Connect User Guide*.

Manage the Cloud Services Gateway

BlackBerry AtHoc provides hosted SMS, email, and telephony notification services. If your organization uses any of these services, you need to configure and enable the gateway.

The following sections describe these configuration tasks:

1. Enable the Cloud Services Gateway on the BlackBerry AtHoc server.
2. Enable the Cloud Services Gateway on the Settings screen.
3. Configure and enable the Cloud Services devices. Complete only the sections that correspond with the services your organization uses:
   - Hosted SMS Text Messaging
   - Hosted Email
   - Hosted Telephony

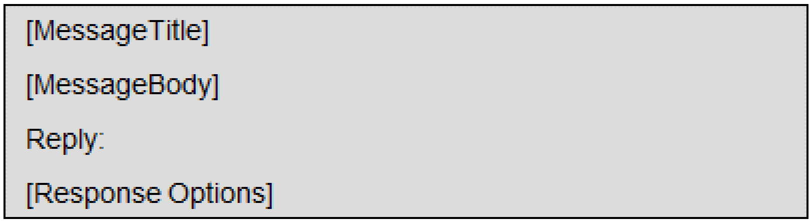
Configure the hosted gateway for cloud services

Use this gateway to set up devices using the AtHoc or OEM Cloud Delivery Service. After configuring this gateway, you can set up telephony (TAS), email (OPM), and SMS.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click to open one of the following gateways, based on information supplied by your BlackBerry AtHoc services representative:
   - AtHoc Cloud Delivery Service (East)
   - AtHoc Cloud Delivery Service (West)
   - OEM Cloud Delivery Service (East)
   - OEM Cloud Delivery Service (West)
3. Click **Copy default settings** at the top of the screen.

   The default templates for the services appear in the SMS and Email template fields.
4. Enter the user name and password values provided to you by BlackBerry AtHoc customer support.
5. Optionally, for TAS, you can enter a Caller ID (ANI) value to override the default value for the account.

   The value should be a valid phone number or extension that is 4-16 numeric characters.
6. For the SMS (texting) template, replace the existing template, with the following template:



```
[MessageTitle]

[MessageBody]

Reply:

[Response Options]
```

7. Optionally, modify the SMS XML template fields for your organization by adding placeholders.

   The following table describes the parameters that you can add to either the SMS or the Email template. The placeholders values are preset:

Placeholder	Required	Purpose and Values
[MessageBody]	Yes	The contents of the SMS message (the alert text.)
[MessageTitle]	Yes	The title of the SMS message.
[PublishedAt]	No	The time when the alert is published.

Placeholder	Required	Purpose and Values
[PublishedBy]	No	The operator account name that sends the alert.
[RecipientName]	No	The name of recipients the alert is sent to.
[ResponseOptions]	No	The response options provided for the recipient of the text message. If empty, the Response Option instruction line does not appear in the alert. The default is `Reply:`, but can be customized text like “Select a response.”
[SelfServiceUrl]	No	Link to the user’s Self Service screen.
[Severity]	No	The value of the Severity field for the alert.
[SystemName]	No	The name of the current organization.
[TargetUrl]	No	The URL in the optional "More Info Link" field, provided for more information.
[Type]	No	The category of the alert, such as Safety.
[OrganizationName]	No	The organization name that is displayed in the BlackBerry AtHoc title pane.

8. Optionally, if you use the hosted email service, you can configure a custom "From" address in the **From Display Name** field. The From Display Name must include a valid email address in angle brackets. For example, XYZ Alerts<Alerts@xyz.com>.

   Note: The From Display Name email domain must be registered with the AtHoc Cloud Delivery system before use. Using an invalid email address will prevent emails from being delivered.

After setting up the Cloud Delivery Services Gateway, you can configure the related devices from the Devices screen.

- Hosted SMS text messaging
- Hosted email
- Hosted Telephony

Configure the text messaging device for hosted SMS

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** page, on the **Personal Devices** tab, click **Text Messaging**.
4. On the **Text Messaging** page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization.
6. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
7. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option users are still able to provide the information, but it is not required.

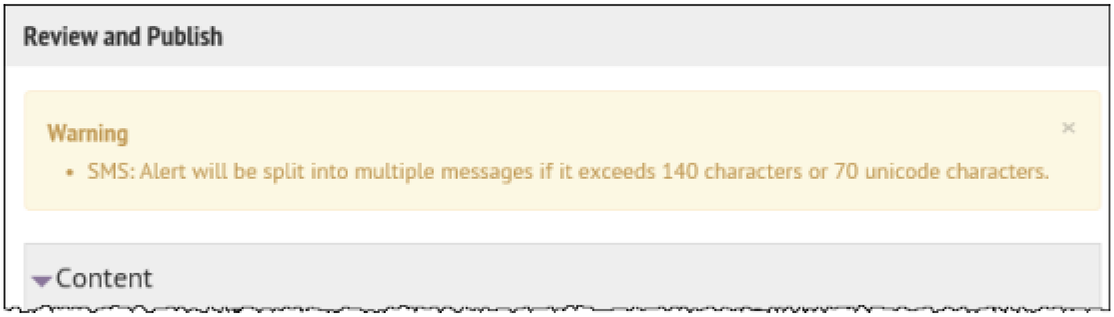
8. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must have the enterprise administrator role to edit the Help Text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if you want to remind operators that text messages have a character limit, you can enter the following text:

     "SMS: Alert will be split into multiple messages if it exceeds 140 characters or 70 unicode characters."

     The text then appears at the top of the Review and Publish screen.

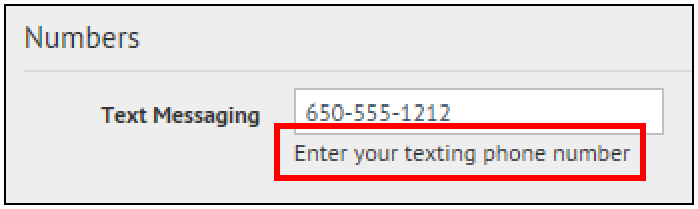


Review and Publish

Warning

- SMS: Alert will be split into multiple messages if it exceeds 140 characters or 70 unicode characters.

   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.

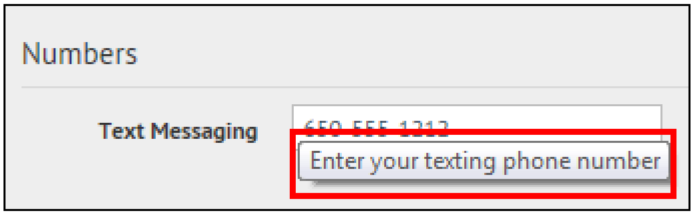


Numbers

Text Messaging: 650-555-1212

Enter your texting phone number

   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



Numbers

Text Messaging: 650-555-1212

Enter your texting phone number

9. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select AtHoc **Cloud Delivery Service**. You can specify up to three gateways for the Hosted SMS device.
10. Click **Save**.
11. If you are ready to make the device available for alert publishing, click **More Actions** > **Enable**. The Hosted SMS Text Messaging device is then fully configured.

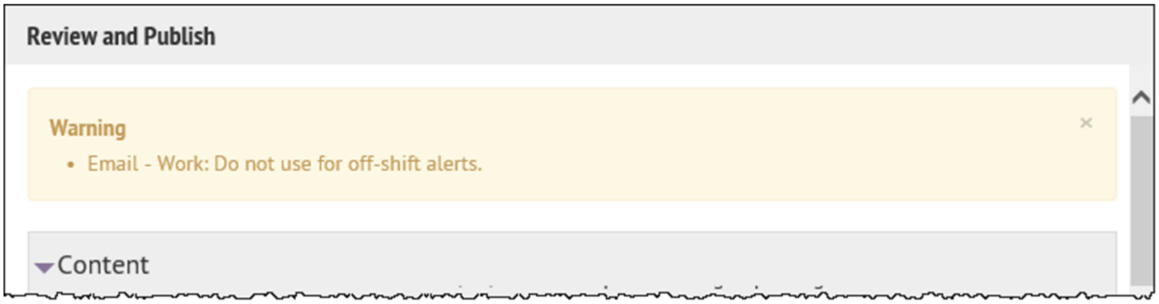
Manage the hosted email service

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** page, on the **Personal Devices** tab, click an email device.
4. On the device details page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization.
6. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.

7. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option, providing the information will be optional.
8. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to edit the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if the device is a work email account, you can enter, "Email - Work: Do not use for off-shift alerts" so that users know not to select the device if they are trying to contact people who are not at work.

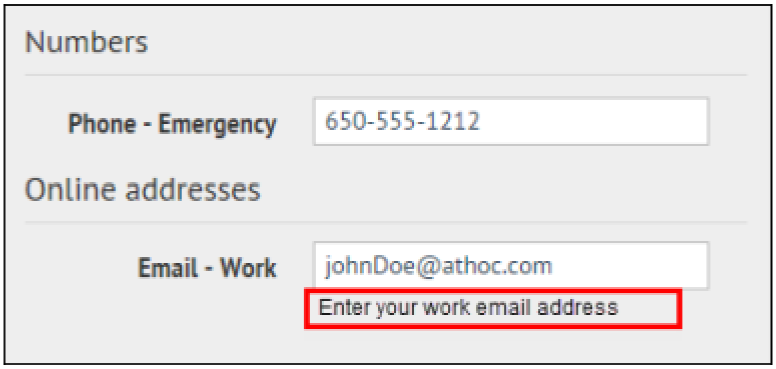


Review and Publish

Warning

- Email - Work: Do not use for off-shift alerts.

   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.



Numbers

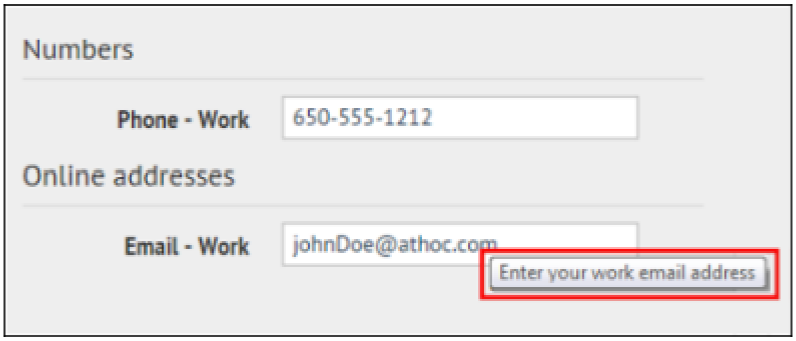
Phone - Emergency: 650-555-1212

Online addresses

Email - Work: johnDoe@athoc.com

Enter your work email address

   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers the cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



Numbers

Phone - Work: 650-555-1212

Online addresses

Email - Work: johnDoe@athoc.com

Enter your work email address

9. In the **Delivery Gateway** section, click **Add a Delivery Gateway** and then select **AtHoc Cloud Delivery Service Gateway** or **OEM Cloud Delivery Service**, either East or West, based on the information BlackBerry AtHoc customer support has provided.
10. Click **Save**.
11. If you are ready to make the device available for alert publishing, click **More Actions** > **Enable**.

The device is available for alert publishing.

Manage the hosted telephony service

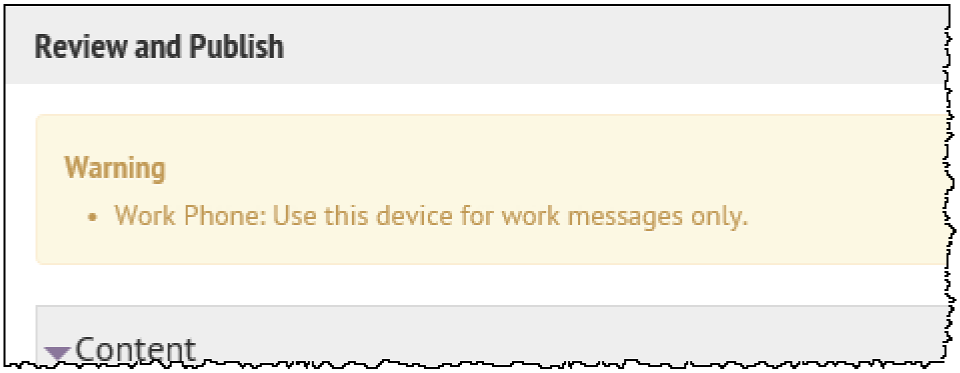
1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** page, in the **Personal Devices** tab, click a phone device such as **Phone-Work** or **Phone-Mobile**.
4. On the device details page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must have the enterprise administrator role to update the Name, Common Name, and Device Group Order.
6. In the **Contact Info Editing** field, select either **All** or **End Users** depending on whether you want everyone or just end users to have the ability to edit their contact info.
7. Optionally, select the **Enable GETS** option to enable Government Emergency Telecommunications Service (GETS) calls. GETS calls can be made only from land lines and not from mobile phones.
8. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option, users will still be able to provide the information but it will not be required.
9. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to modify the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if the phone is a work phone, you can enter the following text:

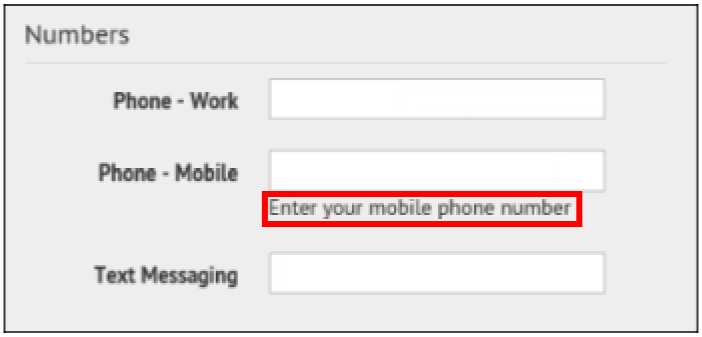
     "Work Phone: Use this device for work messages only."

     The text then appears at the top of the Review and Publish screen.



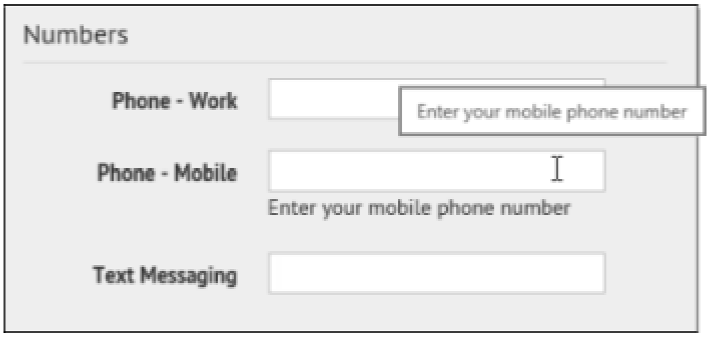
Work Phone: Use this device for work messages only.

   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.



Enter your mobile phone number

   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



Numbers

Phone - Work

Enter your mobile phone number

Phone - Mobile

Enter your mobile phone number

Text Messaging

10. In the **Delivery Gateways** section, select one of the **AtHoc Cloud Delivery Service Gateway** options, either East or West.
11. Click **Save**.
12. Click **More Actions** > **Enable**.

The device is available for alert publishing.

Configure RSS feed information for RSS and Atom content feeds

Mass communication devices include the IP Integration Module for RSS and Atom feeds. These devices use the templates for the RSS feed.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **RSS Feed**.
3. Click **Copy default settings** at the top of the screen to use the correct settings for the content feed.

   RSS or Atom feeds should have the following settings:

   - In the **Supported Formats** field, **Syndication: Atom** and **Syndication: RSS 2.0** are selected.
   - In the **Identity Source** field, the **End User** option is selected.
4. Click **Save**.

Configure XML feed information for mass communication devices

Mass communication devices include the IP Integration Module for loud speakers, as well as RSS and Atom feeds. These devices use the templates for the XML Feed.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Xml Feed**.
3. On the **Xml Feed** screen, specify the mass communication device you want to configure.

   - If you use Atom or RSS feeds, complete the following steps:

     a. In the **Feed Formats** section, select **Syndication: Atom** and **Syndication: RSS 2.0**.
     b. In the **Feed Source** section, select **End User**.
   - If you use an IIM CapCon feed for outdoor loud speakers, complete the following steps:

     a. In the **Feed Formats** section, select **Syndication: CapIndex** and **Syndication: CapIim**.
     b. In the **Feed Source** section, select **Delivery Gateway ID**.
4. Click **Save**.

Configure failover delivery gateways

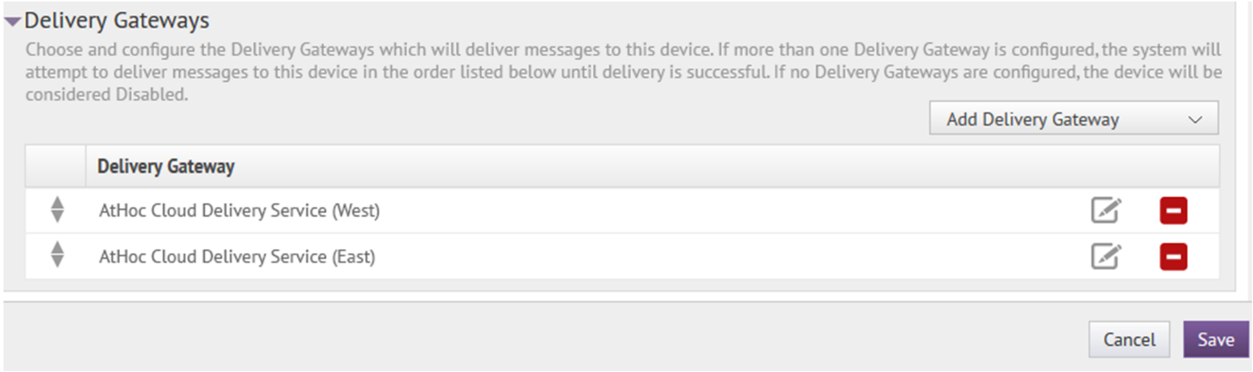
The Delivery Gateway Failover feature adds redundancy to various devices such as phones that can be connected to multiple gateways. If one gateway fails, the other gateway takes over.

Most gateways have only one type of supported gateway and you enable a second gateway of the same type on a failover server. However, certain device groups have multiple gateways that manage alerts for the device. You can use a different gateway if the device is in the same group, where a group includes related devices such as phones, email, or text messaging.

Configuration of delivery gateway failover is handled from the Devices screen. The following list shows groups with multiple devices or gateways and specifies which gateways can be used with a device group.

- **Email**: AtHoc Cloud Delivery Service (East and West), OEM Cloud Delivery Service (East and West)
- **Pager**: AtHoc Cloud Delivery Service (East and West)
- **Phone**: AtHoc Cloud Delivery Service (East and West)
- **Texting**: AtHoc Cloud Delivery Service (East and West)
- **Fax**: AtHoc Cloud Delivery Service (East and West)
- **TTY**: AtHoc Cloud Delivery Service (East and West)

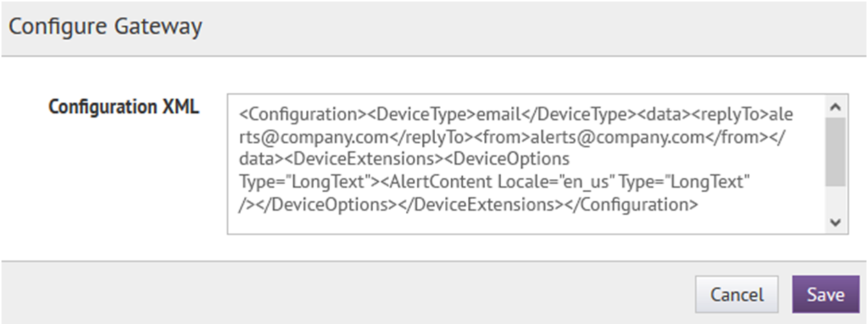
1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click a device name.
4. On the device details screen, click **Edit**.
5. Assuming that the device has a primary gateway configured, in the **Delivery Gateways** section, click **Add a Delivery Gateway** to add a second gateway.



Choose and configure the Delivery Gateways which will deliver messages to this device. If more than one Delivery Gateway is configured, the system will attempt to deliver messages to this device in the order listed below until delivery is successful. If no Delivery Gateways are configured, the device will be considered Disabled.

	Delivery Gateway
⇕	AtHoc Cloud Delivery Service (West)
⇕	AtHoc Cloud Delivery Service (East)

6. Click ✎.
7. On the **Configure Gateway** window, modify the XML statements as needed for your organization.



Configuration XML

```
<Configuration><DeviceType>email</DeviceType><data><replyTo>alerts@company.com</replyTo><from>alerts@company.com</from></data><DeviceExtensions><DeviceOptions Type="LongText"><AlertContent Locale="en_us" Type="LongText" /></DeviceOptions></DeviceExtensions></Configuration>
```

8. Click **Save**.

Manage a TTY/TDD phone device

Note: Only the EN-US locale is supported on TTY/TDD phone devices.

1. In the navigation bar, click ⚙.

2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click **TTY/TDD Phone**.
4. On the **TTY/TDD Phone** page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must have the enterprise administrator role to update the Name, Common Name, Group Name, and Device Group Order.
6. Optionally, select **Users Must Provide Contact Info For This Device in Self Service** if you want to require users to provide that information. If you do not select this option, users are still able to provide the information, but it is not required.
7. Optionally, select the **Enable GETS** option to enable Government Emergency Telecommunications Service (GETS) calls. GETS calls can be made only from land lines and not from mobile phones.
8. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
9. Optionally, in the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must have the enterprise administrator role to edit the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if you want to remind operators that TTY/TDD phone messages have a character limit, you can enter the following text:

     "TTY/TDD Phone: Alert will be split into multiple messages if it exceeds 140 characters or 70 unicode characters."

     The text then appears at the top of the Review and Publish screen.
   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.
   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.
10. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select **AtHoc Cloud Delivery Service (West)** or **AtHoc Cloud Delivery Service (East)**.
11. Click ✎.
12. On the **Configure Gateway** window, replace the content with the following:

    ```
    <Configuration><DeviceType>TTY</DeviceType></Configuration>
    ```
13. Click **Submit**.
14. Click **Save**.
15. Click **More Actions** > **Enable** if you are ready to make the device available for alert publishing.

    The TTY/TDD Phone device is then fully configured.

Manage a pager device

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click one of the following pager devices:
   - **Pager**
   - **Pager (Numeric)**
   - **Pager (One Way)**

- **Pager (Two Way)**
- **Pager Group**

4. On the device details page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must have the enterprise administrator role to update the Name, Common Name, Group Name, and Device Group Order fields
6. Select a **Device Group Order** from the list.
7. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
8. Optionally, select **Users Must Provide Contact Info For This Device in Self Service** if you want to require users to provide that information. If you do not select this option, users can provide the information, but it is not required.
9. Optionally, in the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must have the enterprise administrator role to edit the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen.
   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.
   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.
10. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select AtHoc **Cloud Delivery Service (West)**, or **Zetron Pager**.
11. Click **Save**.
12. Click **More Actions** > **Enable** if you are ready to make the pager device available for alert publishing.

The pager device is then fully configured.

Configure desktop app settings

If you are an administrator, you can configure desktop app settings such as general display items, the system tray menu, client server communications, and failover.

Most settings for the BlackBerry AtHoc desktop app are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. However, the settings described in the following sections might require editing over time and are of interest to most administrators because they affect things such as the time intervals for viewing new alerts and updating user configurations, as well as end user login expiration times.

For information about advanced features such as redirection, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Select general desktop software options

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, in the **Basic Options** section, select or deselect the check boxes beside the following values:

- **Show Welcome message for first-time sign-on**: Causes a web page with a welcome message to appear when the desktop app connects for the first time.
- **Right-click to dismiss Desktop pop-up**: Allows end users to dismiss the desktop pop-up with a right mouse click.
- **Show uninstall option in control panel and Start menu**: Shows the Uninstall button in the toolbar of the "Uninstall or change a program" dialog in Programs and Features when the AtHoc[edition] application is selected from the list of applications.
- **Collect workstation information**: Allows the desktop app to send the IP address, computer name, username, and domain name to the BlackBerry AtHoc server. This reduces the amount of user information that is transferred over the network. When this option is deselected, IP targeting does not work.
- **Stop checking for updates when Desktop is locked**: Prevents the desktop app from checking for updates when an end user's desktop is locked. This option is useful in environments where users do not turn off their computers.

4. In the **Email Address To Send Client Logs** field, enter an email address (`sendlog@athoc.com`) to send the desktop app log to. When the user selects the "Send <organization name> Log" in the Start menu for the desktop app, the email address entered in this field receives a copy of the log file.
5. In the **ActiveX Object Name** field, enter the ActiveX object name for the desktop app. This is used when creating the JavaScript code that is sent by the server to the desktop app in response to requests and in alerts. For example, when the user selects the “Access Self Service” menu option, selects a response option, or clicks a button on an alert.
6. In the **Audio** section, select how the desktop app works with built-in speakers. Select **Consider end user system settings** to prevent the desktop app from overriding the end user's local system speaker settings. Select **Always turn on speaker** to override local speaker settings. When this option is selected, the **Desktop Volume Threshold** slider control appears. This option specifies the volume level that the desktop app sets the audio to.

   Note: The operating system does not provide a way for the desktop app to distinguish between headphones and speakers. When end users are wearing headphones that are plugged into the computer's audio jack, an incoming alert may sound extremely loud.

Customize the desktop client system tray

The system tray icon () appears in the system tray when the desktop app is running. You can change the order of the links that appear in the desktop app system tray using an XML-based menu control. You can also move the link separator up or down and add additional link separators as needed.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, in the **System Tray Menu** section, select **Display System Tray Icon**.
4. In the **Available Menu Items** section, click **Manage Menu Items**.
5. On the **Desktop App Menu Items** window, click **Add Menu Item**.
6. On the **Add Menu Item** window, enter a name and URL for the new menu item.
7. Click **Save**. Take note of the ID of the new menu item.
8. Click **Close**.
9. In the **Menu Configuration** field, add the new menu item to the menu configuration XML. Menu items have this format: <Item Id="8009" Type="Link"/>.
10. Optionally, add a separator to the Menu Configuration XML. Separators have this format: <Item Type="Separator" />
11. Optionally, cut and paste the code for each additional function to add or move menu items and separators.
12. Click **Save**.

The following menu items are available:

Option	Included by default	Code
About	Yes	8005
Access My Profile	Yes	520
Access Self Service	Yes	521
Always Minimize Deskbar to System Tray	No	8015
Auto Hide Deskbar	No	8012
BlackBerry AtHoc Management System	Yes	532
Check for New Alerts	Yes	8009
Clear Search Box History	No	8002
Connection Options...	No	8008
Deskbar always on top	No	8013
Dismiss All Audio Notifiers	No	8021
Dismiss All Desktop Popups	No	8020
Dismiss All Popups	Yes	8022
Enable Popup Auto Focus	No	8025
Exit	No	8006
Show Deskbar	No	9002
Uninstall	No	8004
Update My Device Info	Yes	531
Update My Info	Yes	530

The following is a sample Menu Configuration XML:

```
<SystrayLayout>
   <Item Id="8009" Type="Link" />
   <Item Id="8022" Type="Link" />
   <Item Type="Separator" />
   <Item Id="521" Type="Link" />
   <Item Id="530" Type="Link" />
   <Item Id="531" Type="Link" />
   <Item Type="Separator" />
   <Item Id="8005" Type="Link" />
```

```
  </SystrayLayout>
```

For more information, see "System tray menu" in the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure client server communications

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

You must have system administrator permissions to configure client server communications.

Most settings in the Desktop App settings page are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. The settings in the Client Server Communications section of the Desktop App settings page are used to configure the settings that govern communication between the BlackBerry AtHoc server and the desktop app, and the rate at which new alerts and user configuration updates are checked.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, scroll down to the **Client Server Communications** section.
4. Select a value from the **Check Update Interval** list.

   The Check Update Interval (CU) determines how frequently the desktop app polls the server for updates, including alerts. A lower value causes end users to receive desktop pop-up alerts sooner. A higher value causes users to receive desktop pop-up alerts later. The minimum value is 30 seconds. The maximum value is 15 minutes. The recommended value is 2 minutes.
5. Select a value from the **Reconnect Interval** list.

   The Reconnect Interval specifies the interval the desktop app waits before attempting to contact the server again when the connection is lost. The minimum value is 1. The maximum value is 10. The recommended value is 2.
6. Select a value from the **Recovery Interval** list.

   The Recovery Interval specifies the number of check update intervals the desktop app waits before attempting to contact the server again when the server responds to a Sign On (SO) or CU with an error. The minimum value is 1. The maximum value is 10. The recommended value is 2.
7. Enter a value in the **Start-up Delay** field.

   The Start-up Delay setting is a fractional value between 0 and 1 inclusive that is used to determine the amount of delay before the desktop app first attempts to sign on. A value of 0 specifies no delay and a value of 1 specifies to wait one full check update interval. A value of .5 specifies a delay of 50% of the check update interval.
8. Enter a value in the **Communication Session Expires After** field.

   This option determines when the desktop app session is reset on the server. The default value is 86400 seconds (24 hours). When the desktop app session expires, the desktop app performs a sign on at the next CU.
9. Enter a value in the **Override Default Communication Session Expiration Time After** field.

   This setting cleans up system sessions that were created by the SYSTEM user. Sessions that are created by the SYSTEM user when desktop apps are deployed with the installation script and RUNAFTERINSTALL is set to "Y". Sessions can be created by the SYSTEM user when the installation script is used to update computers after the desktop app is installed.

   This option also enables desktop apps to perform a sign on in environments where users do not turn off their computer. This option provides a way to configure desktop apps to redirect during SO.
10. Click **Save**.

For more information, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure failover settings

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

Most settings in the Desktop App settings page are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. The settings in the Failover section of the Desktop App settings page are used to enable the primary BlackBerry AtHoc server to fail over to a secondary server when the primary server becomes unresponsive and CUs fail.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, scroll down to the **Failover** section.
4. Enter the URL for the failover server.
5. Select a value from the **Reconnect attempts before Failover** list.

   This setting specifies the number of attempts that the Desktop app makes to contact the primary server before switching to the failover server.
6. Click **Save**.

For more information, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure user authentication

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods from the **Desktop App** > **Authentication Method** list:

   - **LDAP Attribute**: This option enables the desktop app to authenticate with an Active Directory attribute that you provide in the **Attribute** field. The desktop app queries this attribute directly from the signed-in user's directory profile and sends it to the server. This option allows the desktop app to operate while sending less user information to the server. When this option is selected, the desktop app does not send Windows user names or domain names in sign on or check update query strings.

     This option requires desktop app version 6.2.x.271 or later.
   - **Smart Card**: This option enables smart card authentication. Select the number of client certificates to collect. The recommended value is 3.

     a. From the **Number of Certificates** list, select the number of client certificates to collect. The recommended value is 3.
     b. Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=(?<edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.
     c. Optionally, in the **Client Regular Expression** field, enter a client regular expression in the following format: `.*?(^)(?:(?!\s-[A||E||S]).)*`. This format extracts information from the client certificate subject name to find the identical certificates for authentication. The regular expression provided in the UI is a sample expression that may not be suitable for your environment. You can build you own regular expression or contact BlackBerry AtHoc customer support to configure this field.
   - **Defer to Self Service**: This option configures the desktop app to use the user authentication method selected for Self Service. When this method is selected, end users will see a login window. When the user clicks Log In, they are redirected to Self Service to complete the sign in process. This process depends on the authentication method selected by the administrator.

     If the Self Service authentication method is set to Username and Password, the users sees a registration window and must provide their first name, last name, username, password, confirm their password, and fill in a captcha. The user has the option to register as a new user or to sign in with their existing user credentials.

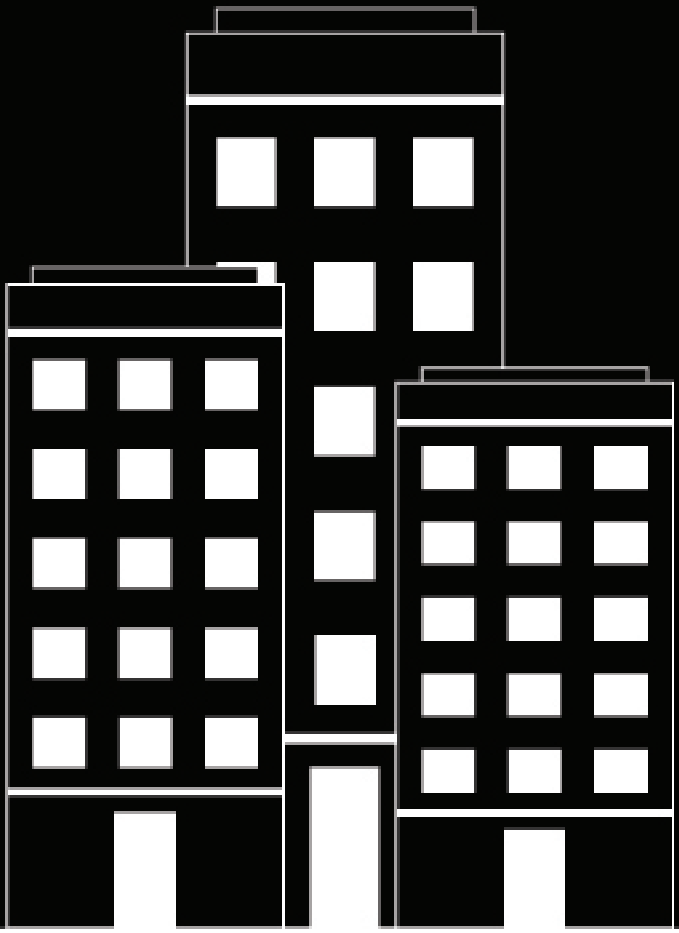
  If the Self Service authentication method is set to Smart Card, the user sees a certificate selection screen and must pick a certificate. They may also be required to enter a PIN.

  If the Self Service authentication type is set to Windows Authentication, the user sees a Windows credentials screen and must provide their username and password.

  If the Self Service authentication method is set to Single Sign-On, the user is sent to the SSO URL.

- **Windows Authentication**: This option configures the desktop app to use only the Windows username and password or to use both the Windows username and the domain.

4. Optionally, if LDAP Attribute, Smart Card, or Windows Authentication is selected, you can select the **Create new user if an account is not found** option to configure the desktop app to create a user at sign on if the user does not already exist.
5. Click **Save**.



BlackBerry AtHoc

API Quick Start

7.16

Contents

What is the BlackBerry AtHoc API?

BlackBerry® AtHoc® integrates with existing systems and investments to create a comprehensive end-to-end crisis communication system. A common integration use case is to synchronize all user contact details between an authoritative source and BlackBerry AtHoc. This integration is possible thanks to an extensible set of web APIs. The APIs are designed to integrate a BlackBerry AtHoc system with other systems to make alerting more successful.

BlackBerry has incremented the web-based API to include new REST endpoints. The new REST-based web APIs are referred to as the BlackBerry AtHoc API V2.

This document describes how to get started using the BlackBerry AtHoc API V2. This document assumes that the reader is familiar with the BlackBerry AtHoc product, the end-user interaction, and the use of the management system. Familiarity with API V1 is helpful but not required.

This document also assumes that the reader has a customer relationship with BlackBerry or is working as a developer for a BlackBerry customer.

This document does not contain a full list of the available API endpoints. This list, including detailed definitions of each endpoint, is available in the interactive documentation installed with BlackBerry AtHoc and can be accessed at [*server-address*]/api/v2/docs.

Key differences between API Version 1 and API Version 2

The BlackBerry AtHoc API V2 makes establishing new integrations easier for developers. It follows the popular REST pattern with HTTP methods and JSON-formatted payloads. The authentication and authorization are OpenID Connect and OAuth 2.

The following table summarizes the differences between the API V1 and V2:

	API Version 1	API Version 2
Payload format	XML over HTTP	JSON over HTTP
Authorization	Inline username and password	OpenID Connect with OAuth2 JWT Access Tokens
Calling pattern	HTTP POST of Custom XML Payload Definitions	REST with HTTP methods GET, PUT, POST, DELETE
Scenarios covered	• User Sync • Distribution List • Sync Alert • Publishing Get Content	• User Sync • Distribution List Sync • Get Content • Accountability Officer
Unique identifier for users	MID (mapping ID)	LOGIN_ID (username)

System level guidelines

Throttling limits

- There are throttling limits in place when calling the API. Try to optimize the workflow of calls to the API to achieve the maximum work within the number of allowed calls.
- Your calls may be blocked if they exceed the defined limits of your system or organization.

Dates and times

- Dates and times will be in the organization time zone unless otherwise specified.

User synchronization

- Use batches to update multiple users in one request instead of single-user updates in each call.
- Do not exceed more than 1000 users in each call because the SyncBy endpoints are in real-time. If you need to synchronize more than 1000 users in a call, use the background job CSV import endpoint.
- Don't store UserIDs inside your application. The identifier for the user is username or mapping ID.

Attributes

- The API GET method does not retrieve CommonName attributes when they contain the following special characters : + @ #
- Common names may be optional in the user interface.
- The following APIs do not support attributes whose common name {commonName} or attribute value common name {valueCommonName} contains the forward slash (/) character:

HTTP type	URL
GET	/orgs/{orgCode}/attributes/{commonName}
GET	/orgs/{orgCode}/attributes/{commonName}/Values
GET	/orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}
DELETE	/orgs/{orgCode}/attributes/{commonName}/values
POST	/orgs/{orgCode}/attributes/{commonName}/values
PUT	/orgs/{orgCode}/attributes/{commonName}/values
PUT	/orgs/{orgCode}/attributes/{commonName}/values/{ValueCommonName}
DELETE	/orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users
PUT	/orgs/{orgCode}/attributes/{commonName}/Values/{valueCommonName}/Users

Set up your environment

Create a user account with operator permissions

To use the BlackBerry AtHoc API, you must create a user account with operator permissions. The user must have the SDK User role and permissions to access the specific API module. For example, you must have the User Manager role to access the User Sync API.

Provision an application that can call the web API

To provision a new API integration with the BlackBerry AtHoc management system, you must have organization administrator, enterprise administrator, or system administrator permissions. You must have system administrator permissions to enable a provisioned application.

Note: The Client ID and Client Secret can be used only in the organization in which they are created. If the Client ID and Client Secret are created in the System Setup (3) organization, they can be used in any organization. If the Client ID and Client Secret are created in an Enterprise organization, they can be used in any of that Enterprise's suborganizations. If the Client ID provided does not follow these inheritance rules, a 400 (Bad Request) error code is returned.

1. Log in to the BlackBerry AtHoc management system as an organization administrator, enterprise administrator, or system administrator.
2. In the navigation bar, click ⚙.
3. In the System Setup section, click **API Applications**.
4. On the **API Applications** window, click **New**.
5. On the **New API Application** window, enter a name for the API integration.
6. (System administrators only) Select the **Enabled** check box beside **Status**.
7. In the Authentication section, select a Grant Type. Password is the default. If you select Implicit, enter a redirect URI in the text box that appears.
8. Click **Save**. A success message appears that includes the Client ID and Client Secret.
9. Take note of the displayed Client Secret. It is displayed only once and will need to be regenerated if it is lost.

Note: After you provision your application in the BlackBerry AtHoc management system, contact BlackBerry AtHoc Customer Support to have the application reviewed and enabled.

Set up an organization code in the BlackBerry AtHoc system

Complete the following task to set up an organization code for your specific organization in the BlackBerry AtHoc management system. This organization code is not propagated to PSS, so if you already have an organization code in PSS, use that one to complete this task.

This task is not required if an organization code for your organization has already been provided to you.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Switch to the specific organization.
3. Go to **Settings** > **General Settings**.
4. In the **Organization Details** section, enter the organization code. Do not use spaces.

Authentication

The BlackBerry AtHoc API V2 uses OAuth2-compliant authentication and authorization. To call the API, the client must first obtain an access token. Each organization has one access token. You will need to request an access token for every individual organization that you are calling against. The authentication step returns an access token which will be used when it calls the APIs.

The access token is only useful if the user has an operator role required to access the specific API module. For example, the User Manager role is required for User Sync. For more information, see Required roles for API access.

The parameter acr_values should contain the organization code in a key value pair with the Key=tenant (for example, acr_values=tenant:<OrgCode>) where <OrgCode> is the organization code of the organization that you want to access the API for.

Scope should be a space-delimited string of the resources that you want to access. If you also need long-term access to the API, you can request a Refresh Token with the offline_access scope. For example, openid profile athoc.iws.web.api offline_access.

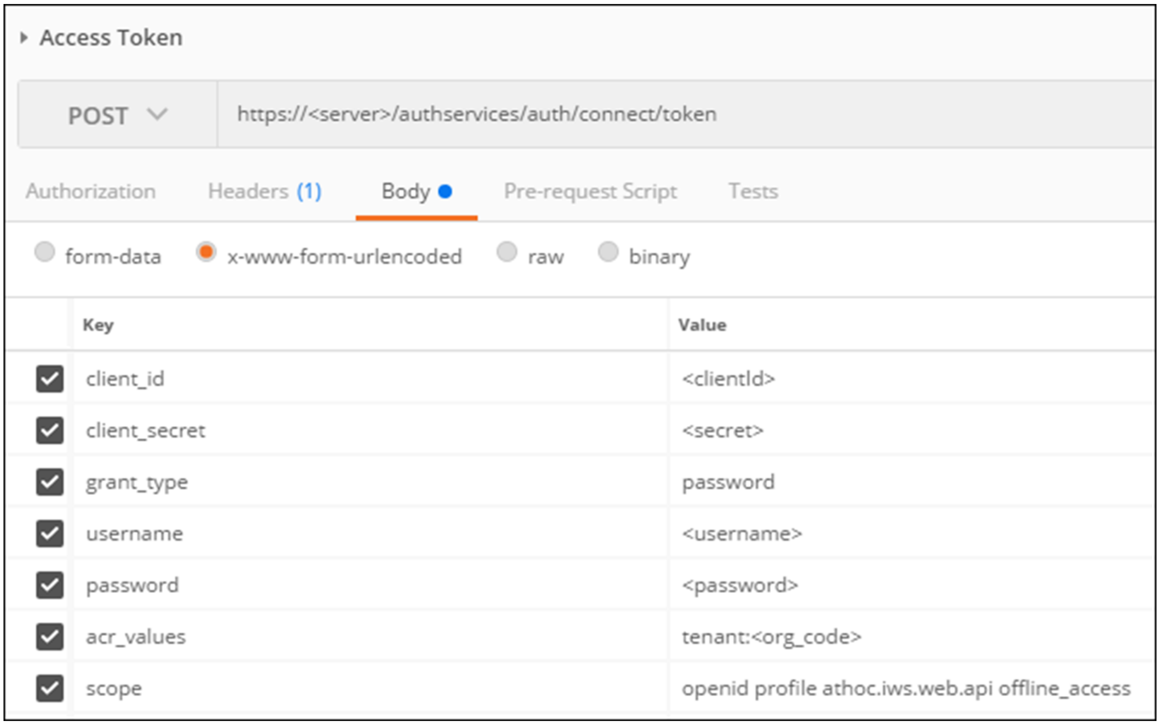
Depending on your application and security requirements, you can obtain an access token from any of the following supported grant types:

- Password Grant
- Authorization Code Grant
- Implicit Grant
- Change Org Grant
- Refresh Token Grant

Password grant

The resource owner password grant type allows requesting tokens on behalf of a user by sending the user's name and password to the token endpoint. This is "non-interactive" authentication and is generally not recommended. There may be instances in certain legacy or first-party integration scenarios where the password grant type is useful, but the general recommendation is to use an interactive flow like implicit or auth code for user authentication.

The following is a Postman request for an Access and a Refresh Token using the Password Grant:



▸ Access Token

POST https://<server>/authservices/auth/connect/token

○ form-data ● x-www-form-urlencoded ○ raw ○ binary

	Key	Value
☑	client_id	<clientId>
☑	client_secret	<secret>
☑	grant_type	password
☑	username	<username>
☑	password	<password>
☑	acr_values	tenant:<org_code>
☑	scope	openid profile athoc.iws.web.api offline_access

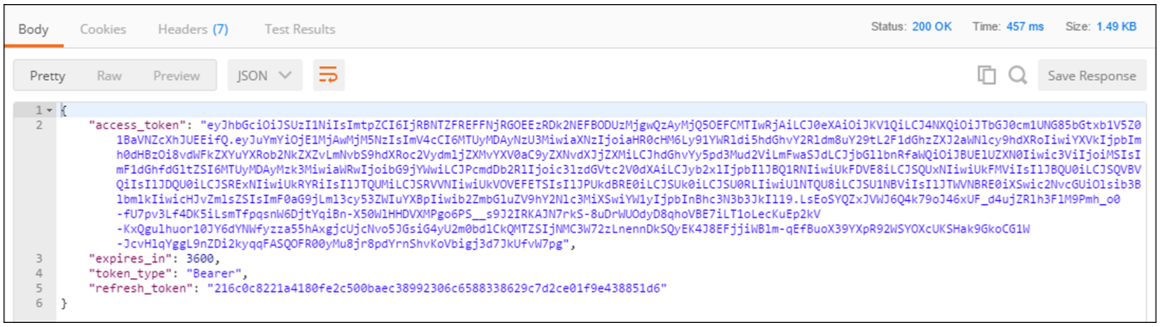
HTTP URL: https://<server>/authservices/auth/connect/token

HTTP Verb: POST

Parameters: Form encoded body containing the following fields with values:

client_id, client_secret, grant_type, username, password, acr_values, scope

You should see the response with the Access and Refresh Tokens with an HTTP Status Code of 200 OK. You can now use the access_token for calling the API resources (and use the refresh token to retrieve a new access and refresh token without resubmitting the user credentials).



Status: 200 OK Time: 457 ms Size: 1.49 KB

```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjRBNTZFREFFNjRGOEEzRDk2NEFBODUzMjgwQzAyMjQ5OEFCMTIwRjAiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJTbGJ0cm1UNG85bGtxb1V5Z0
        1BaVNZcXhJUEEifQ.eyJuYmYiOjE1MjAwMjM5NzIsImV4cCI6MTUyMDAyNzU3MiwiaXNzIjoiaHR0cHM6Ly91YWRldi5hdGhvY2Rldm8uY29tL2F1dGhzZXJ2aWNlcy9hdXRoIiwiYXVkIjpbIm
        h0dHBzOi8vdWFkZXYuYXRob2NkZXZvLmNvbS9hdXRoc2VydmljZXMvYXV0aC9yZXNvdXJjZXMiLCJhdGhvYy5pd3Mud2ViLmFwaSJdLCJjbGllbnRfaWQiOiJBUElUZXN0Iiwic3ViIjoiMSIsI
        mF1dGhfdGltZSI6MTUyMDAyMzk3MiwiaWRwIjoibG9jYWwiLCJPcmdDb2RlIjoic3lzdGVtc2V0dXAiLCJyb2xlIjpbIlJBQ1RNIiwiUkFDVE8iLCJSQUxNIiwiUkFMViIsIlJBQU0iLCJSQVBV
        QiIsIlJDQU0iLCJSRExNIiwiUkRYRiIsIlJTQUMiLCJSRVVNIiwiUkVOVEFETSIsIlJPUkdBRE0iLCJSUk0iLCJSU0RLIiwiUlNTQU8iLCJSU1NBViIsIlJTWVNBRE0iXSwic2NvcGUiOlsib3B
        lbmlkIiwicHJvZmlsZSIsImF0aG9jLml3cy53ZWIuYXBpIiwib2ZmbGluZV9hY2Nlc3MiXSwiYW1yIjpbInBhc3N3b3JkIl19.LsEoSYQZxJVWJ6Q4k79oJ46xUF_d4ujZRlh3FlM9Pmh_o0
        -fU7pv3Lf4DK5iLsmTfpqsnW6DjtYqiBn-X50WlHHDVXMPgo6PS__s9J2IRKAJN7rkS-8uDrWUOdyD8qhoVBE7iLT1oLecKuEp2kV
        -KxQgulhuor10JY6dYNWfyzza55hAxgjcUjcNvo5JGsiG4yU2m0bdlCkQMTZSIjNMC3W72zLnennDkSQyEK4J8EFjjiWBlm-qEfBuoX39YXpR92WSYOXcUKSHak9GkoCG1W
        -JcvHlqYggL9nZDi2kyqqFASQOFR00yMu8jr8pdYrnShvKoVbigj3d7JkUfvW7pg",
    "expires_in": 3600,
    "token_type": "Bearer",
    "refresh_token": "216c0c8221a4180fe2c500baec38992306c6588338629c7d2ce01f9e438851d6"
}
```

Authorization code grant

The authorization code flow provides a way to retrieve tokens on a back-channel as opposed to the browser front-channel. The authorization code grant supports client authentication. The following is the recommended flow for native applications such as mobile apps and Windows forms.

Step 1: An application requests an authorization code from the authentication server.

```
GET https://<server>/AuthServices/Auth/connect/authorize?
```

```
response_type=code
&client_id=<client_id>
&redirect_uri=<your_app_callback_url>
&scope=openid profile athoc.iws.web.api offline_access
&state=<guid>&acr_values=tenant:<org_code>
&code_challenge=<ClientGenerated_CodeChallenge>
&code_challenge_method=S256
```

state This is an opaque value that the application adds to the initial request. During authentication, the application sends this parameter in the authorization request, and the authorization server returns this parameter unchanged in the response. This value must be used by the application to prevent cross-site request forgery (CSRF) attacks. This value can also be used by the application to restore the previous state of the application.

For more information about the state parameter, see:

https://auth0.com/docs/api-auth/tutorials/authorization-code-grant

https://auth0.com/docs/protocols/oauth2/oauth-state

code_challenge: The code_challenge is a Base64-URL-encoded string of the SHA256 hash of the code_verifier. Your application saves the code_verifier for later and sends the code_challenge with the authorization request to your authorization server's authorization URL.

For more information about the code_challenge parameter, see

https://developer.okta.com/authentication-guide/implementing-authentication/auth-code-pkce

Step 2: The browser redirects the user to the login screen.

The browser redirects the user to the login screen. Upon entering login credentials, if the credentials are valid, the browser has the authentication code in the URL. If the credentials or organization code are invalid, the browser displays HTTP status code 400 "Bad Request."

Step 3: The client requests the access_token based on the authentication code in step 2.

```
POST https://<Server>/AuthServices/Auth/connect/token
{
     "grant_type":"authorization_code",
     "code":"<code>" //code returned in browser from 2nd Step
     "redirect_uri":"<your_app_callback_url>",
       "client_id":"<client_id>",
       "code_verifier":"<ClientGenerated_CodeVerifier>"
}
```

Step 4: The authentication server sends the access token response.

```
{
   "expires_in":3600,
   "token_type":"Bearer",
   "refresh_token":"ljiweoriwoer...",
   "access_token":"okljhgfdsighijuhdfgdkljhgdflkgjlkjdlfkgj..."
}
```

Implicit grant

The implicit grant type is optimized for browser-based applications. The implicit grant type is used for user authentication-only (both server-side and JavaScript applications), or for authentication and access token requests (JavaScript applications). In the implicit flow, all tokens are transmitted through the browser. Advanced features such because refresh tokens are not allowed as the security of the tokens cannot be guaranteed.

The implicit grant flow has the following steps:

1. Your application directs the browser to the authentication server sign-in page, where the user authenticates.
2. The authentication server redirects the browser to the specified redirect URI, and includes the access and ID tokens as a hash fragment in the URI.
3. Your application extracts the tokens from the URI.
4. Your application can now use these tokens to call the resource server (for example, an API) on behalf of the user.

Starting this flow is very similar to the authorization code flow except that the `response_type` is `token` or `id_token` instead of `code`.

Step 1: Your browser makes a request to authorize the endpoint of the authorization server.

```
GET https://<server>/AuthServices/Auth/connect/authorize?
response_type=token
&client_id=<client_id>
&redirect_uri=<your_app_callback_url>
&scope=openid profile athoc.iws.web.api offline_access
&state=<guid>
&acr_values=tenant:<org_code>
```

Step 2: The user logs in.

If the user does not have an existing session, this will open the authentication server sign-in page. After authenticating, or if the user has an existing session, the user arrives at the specified `redirect_uri` with a token as a hash fragment.

Step 3: The authentication server sends a redirect response.

```
https://localhost:8080/#
access_token=eyJhkjughfs...
&token_type=Bearer&expires_in=3600
&scope=openid
&state=<state>
```

Your application must now extract the tokens from the URI and store them.

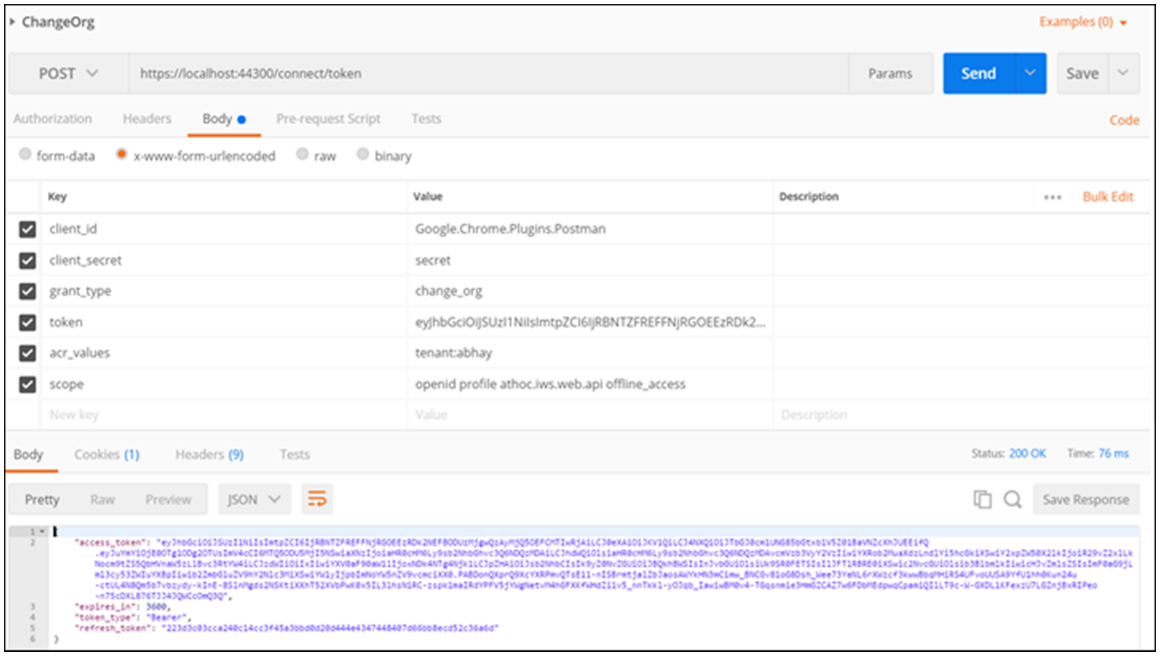
Change organization grant

The change organization grant has been specifically designed for external applications that allow their users to switch between multiple organizations.

When the application has received an access token based on user credentials, the same access token can be used as the user’s identity to get new access tokens for organizations that the user has access to.

The response of this call is a new Access (and Refresh) token based on the user's permissions within the new organization. If the user is not authorized in this organization, an error is returned.

The following is a Postman request and response for the change_org grant:



	Key	Value	Description
☑	client_id	Google.Chrome.Plugins.Postman	
☑	client_secret	secret	
☑	grant_type	change_org	
☑	token	eyJhbGciOiJSUzI1NiIsImtpZCI6IjRBNTZFREFFNjRGOEEzRDk2...	
☑	acr_values	tenant:abhay	
☑	scope	openid profile athoc.iws.web.api offline_access	
	New key	Value	Description

```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjRBNTZFREFFNjRGOEEzRDk2NEFBODUzMjgwQzAyMjQ5OEFCMTIwRjA1LCJ0eXAiOiJKV1QiLCJ4NXQiOiJTbGJ0cm1UNG85bGtxb1V5Z01BaVNZcXh3UEE1fQ
      .[illegible]",
    "expires_in": 3600,
    "token_type": "Bearer",
    "refresh_token": "223d3c03cca240c14cc3f45a3bbd0d20d444e4347448407d66bb8ecd52c36a6d"
}
```

Note: The change organization grant type must be requested from BlackBerry AtHoc Customer Support for the provisioned application. The change organization grant is an add-on grant that can be added to any provisioned application using the implicit, authentication code, and password grants.

URL: https://<server>/AuthServices/Auth/connect/token

HTTP Verb: POST

Parameters:

- **client_id**: <client_id>
- **client_secret**: <secret>
- **grant_type**: change_org
- **scope**: openid profile athoc.iws.web.api
- **acr_values**: tenant:<org_code>
- **token**: <current valid access token>

API Error Response: If the user is not authorized for the given tenant (organization), the following error code is returned:

```
401: Unauthorized
```

Refresh tokens

Refresh tokens enable granting long-term access to APIs. You should keep the lifetime of access tokens as short as possible. However, you want to avoid forcing the user to perform repeated front-channel round trips to the authentication server to request new access tokens.

Refresh tokens allow new access tokens to be requested without user interaction. Every time the client refreshes a token, it needs to make an authenticated back-channel call to the authentication server. This call allows verifying if the refresh token is still valid or has been revoked.

Refresh tokens are supported in the authorization code and resource owner password flows. To request a refresh token, the client must include the offline_access scope in the token request and must be authorized for that scope.

Refresh tokens expire after 30 days. Refresh tokens have a sliding lifetime window of 15 days. The lifetime of a refresh token is renewed by the amount of time specified in the SlidingRefreshTokenLifetime parameter. After 30 days, the client must reauthenticate, regardless of the validity period of the most recent refresh token acquired by the application.

To obtain a new access token from a refresh token, send the following information:

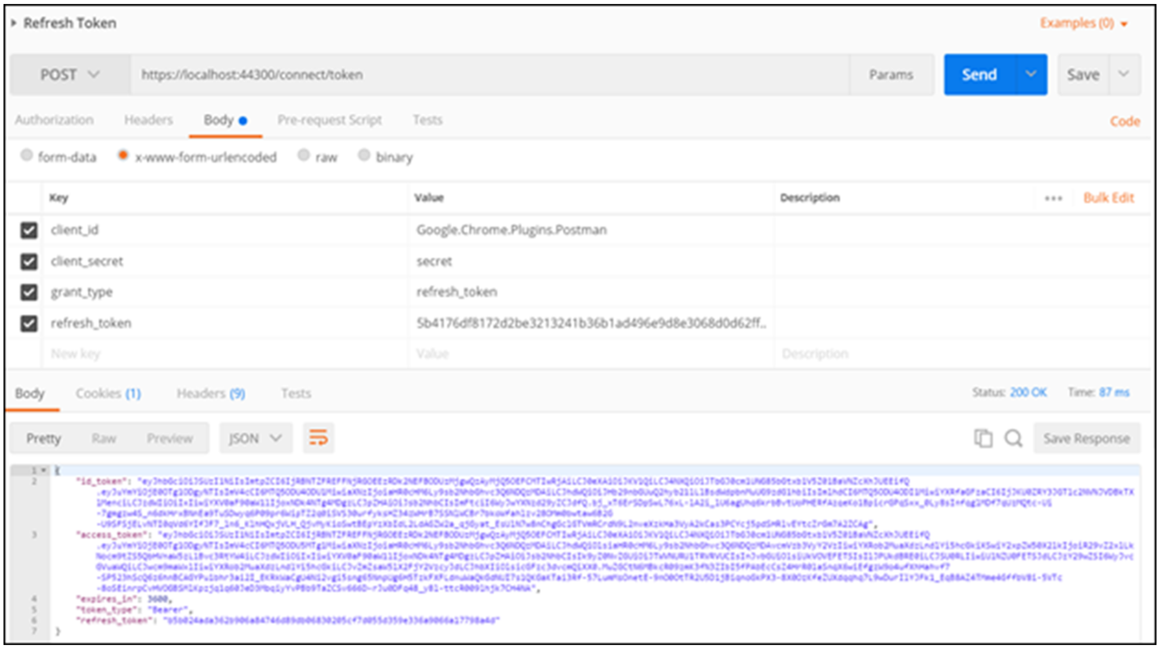
URL: https://<server>/AuthServices/Auth/connect/token

HTTP Verb: POST

Parameters:

- **client_id** <client_id>
- **client_secret**: <secret>
- **grant_type**: refresh_token
- **refresh_token**: <current valid refresh token>

The following is a Postman request and response for the refresh_token grant:



https://localhost:44300/connect/token

	Key	Value	Description
☑	client_id	Google.Chrome.Plugins.Postman	
☑	client_secret	secret	
☑	grant_type	refresh_token	
☑	refresh_token	5b4176df8172d2be3213241b36b1ad496e9d8e3068d0d62ff...	
	New key	Value	Description

Status: 200 OK Time: 87 ms

```
{
    "id_token": "[illegible]",
    "access_token": "[illegible]",
    "expires_in": 3600,
    "token_type": "Bearer",
    "refresh_token": "[illegible]"
}
```

Authentication errors

This topic describes the error codes you may see when authentication of an API client fails. When authentication fails because the client is disabled or not present, a 400 error code is displayed. The following table explains the errors:

Error code	Cause	Action to correct
invalid client	The client name does not exist or is incorrect, or the client secret is invalid.	Check that the client is provisioned in the API application page and that it is in the Enabled state. Reset the client secret and use the new one.
unsupported_grant_type	The grant type is invalid.	The Grant type cannot be empty. Check that the Grant type is populated with one of the following supported grant type values: Implicit, authorization_code, Password, Change_org.
invalid_grant	The username or password is invalid, or the tenant code is invalid.	Make sure that the user credentials are valid and the correct organization code is passed.
invalid_scope	The scope is invalid.	The Scope cannot be empty. The mandatory Scope value is **openid profile athoc.iws.web.api. offline_access**. The offline_access scope value is an optional value that is required only when requesting a refresh token.

If you received an error, verify the following items:

1. Your client is properly provisioned and your client_id and secret are valid.
2. Your client has the password grant configured and allowed.
3. Your username and password fields are correct.
4. The user exists in the organization defined in the acr_values tenant:<org_code>.
5. The operator account is not locked.

Reset the client secret

If you need to reset the client secret for your API integration, complete the following steps:

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click ⚙.
3. In the System Setup section, click **API Applications**. The API Applications window opens.

4. Optionally, enter a name in the search box to filter the list of applications.
5. Optionally, select **Enabled Applications** or **Disabled Applications** from the All Applications list to filter the list of applications.
6. Click the application that you want to modify.
7. Click **Reset Client Secret**. A confirmation window opens.

   Note: Any existing calls to the selected API with the existing client secret will be blocked when you reset the client secret. Any existing calls to the selected API with the existing client secret will be blocked when you reset the client secret.
8. Click **Continue**. You are returned to the API application window. The new client secret is displayed.
9. Take note of the displayed client secret.

Call the API

You can call the BlackBerry AtHoc web API through a URL in your browser.

To access the BlackBerry AtHoc API, complete the following steps:

1. Log in to the BlackBerry AtHoc management system as an SDK User.
2. In the address bar of your browser, replace "athoc-iws" with "api/v2/docs" . The web API page opens.
3. Enter your organization ID in the **Authorize** field.
4. Click **Authorize**. The Available authorizations window opens.
5. Select the scope option.
6. Click **Authorize**. You are directed to a login page.
7. Enter your username and password.
8. Click **Log In**.

Resolve response codes

The following table lists response codes and how to resolve them:

Response code	Description	Steps to resolve
400	Bad Request	Check that the payload and its format are correct. Check for validation errors and take necessary actions to correct the payload.
401	Unauthorized	Make sure that the access token is present, correct, and not expired.
403	Forbidden	• The operator does not have sufficient operator permissions to execute the request. Log in to the BlackBerry AtHoc management system to modify the roles for the operator. • The password used is changed or expired. Generate a new authentication token.
404	Not Found	The resources you are trying to find are not present in the system. Pass valid parameters.
429	Too Many Requests	There is a restriction on the number of API calls allowed. Try the service again. If you continue to see this response code, contact your administrator and request that the API throttling limit be increased to allow the client to perform more requests.
500	Internal Server Error	Report this error to BlackBerry AtHoc customer support at athocsupport@blackberry.com.
503	Service Unavailable	The server is currently unable to handle the request due to a temporary overload or scheduled maintenance. Wait and try again.

Code samples

BlackBerry AtHoc has created a set of code written in C# that can be used as a template to call the APIs. This code handles authentication and allows you to use the .Net methods and functions instead of calling the REST endpoints directly.

Contact your implementation engineer or BlackBerry AtHoc Customer Support for the .zip file that contains these code files. You can also access code samples by clicking the **API Development Kit** link at [*server-address*]/api/v2/docs/apiguide.html.

Required roles for API access

The following table lists the operator roles that are required to access API calls. You must have at least one required role to access each API.

API	Required role
GetOperatorAuditLog	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • System Administrator
GetAllDevices	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
GetDevice	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
GetOrgDevices	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
GetOrgMassDevices	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
GetOrganizations	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Distribution List Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
GetOrganization	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Distribution List Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
SyncByCommonNames	• Alert Manager • Advanced Alert Manager • End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
GetUsers	• Alert Manager • Advanced Alert Manager • End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
GetUserProfile	• Alert Manager • Advanced Alert Manager • End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator

API	Required role
UserSearchBasic	• Alert Manager • Advanced Alert Manager • End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
UserSearchAdvanced	• Alert Manager • Advanced Alert Manager • End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
AlertUsersTargeted	• Accountability Manager • Accountability Officer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • Basic Administrator • Basic Operator
AlertDeviceCoverge	• Accountability Manager • Accountability Officer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • Basic Administrator • Basic Operator

API	Required role
GetEvent	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetEventStatusSummary	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetEventDetailsWithStatus	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetUserEventStatusHistory	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
UpdateUserStatus	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetAccountabilityTemplates	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetAccountabilityTemplateDetails	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
PublishEvent	• Accountability Manager • Enterprise Administrator • Plan Incident Manager • Plan Manager

API	Required role
GetEvents	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetAccountabilityEventOfficers	• Accountability Manager • Accountability Officer • Enterprise Administrator • Plan Incident Manager • Plan Manager
GetOrgAllApiClients	• Enterprise Administrator • Organization Administrator • System Administrator
GetApiClientDetails	• Enterprise Administrator • Organization Administrator • System Administrator
SaveApiClient	• Enterprise Administrator • Organization Administrator • System Administrator
ResetApiClientSecret	• Enterprise Administrator • Organization Administrator • System Administrator
GetAttachmentDetails	• Accountability Manager • Accountability Officer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • Basic Administrator • Basic Operator

API	Required role
GetAllAttributes	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
GetAttribute	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
UpdateAttribute	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • System Administrator
GetAttributeValues	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
GetAttributeValue	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
AddAttributeValues	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
UpdateAttributeValues	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
UpdateAttributeValue	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
DeleteAttributeValues	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
UpdateUserAttributeValue	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
DeleteUserAttributeValue	• End Users Manager • Enterprise Administrator • Organization Administrator • Basic Administrator

API	Required role
GetDeliveryTemplates	• Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • System Administrator
GetEmailDeliveryTemplatePreview	• Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • System Administrator
GetDesktopPopupDeliveryTemplatePreview	• Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • System Administrator
GetDeliveryTemplateDetails	• Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • System Administrator
PostEventLog	• Enterprise Administrator • Organization Administrator • System Administrator
GetInboundAndExternalEvents	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Connect Agreement Management • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Basic Administrator • Basic Operator

API	Required role
GetInboundAndExternalEvent	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Connect Agreement Management • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Basic Administrator • Basic Operator
GetAllLists	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
GetAllStaticLists	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
GetAllDynamicLists	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator

API	Required role
SyncStaticLists	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
DeleteStaticLists	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
GetStaticListRelations	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
SetStaticListRelations	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Basic Administrator
PostStaticDistributionMembers	• Alert Manager • Advanced Alert Manager • Enterprise Administrator • Organization Administrator • Basic Administrator

API	Required role
GetOperatorsPermission	• Enterprise Administrator • Organization Administrator • System Administrator • Basic Administrator
GetOperatorPermissionDetails	• Enterprise Administrator • Organization Administrator • System Administrator • Basic Administrator
PublishAlert	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Basic Administrator • Basic Operator
UpdateAlert	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Basic Administrator • Basic Operator
GetAlertTemplates	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Basic Administrator • Basic Operator

API	Required role
GetAlertTemplate	- Alert Manager - Advanced Alert Manager - Alert Publisher - Advanced Alert Publisher - Draft Alert Creator - Enterprise Administrator - Organization Administrator - Plan Incident Manager - Plan Manager - Report Manager - Basic Administrator - Basic Operator
GetAlertTypes	- Accountability Manager - Accountability Officer - Activity Log Manager - Activity Log Viewer - Alert Manager - Advanced Alert Manager - Alert Publisher - Advanced Alert Publisher - Collaboration Manager - Connect Agreement Manager - Draft Alert Creator - End Users Manager - Enterprise Administrator - Organization Administrator - Plan Incident Manager - Plan Manager - Report Manager - SDK User - System Administrator - Basic Administrator - Basic Operator

API	Required role
GetAlertSeverities	• Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Collaboration Manager • Connect Agreement Manager • Draft Alert Creator • End Users Manager • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • SDK User • System Administrator • Basic Administrator • Basic Operator
GetAlerts	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • Basic Administrator • Basic Operator

API	Required role
GetAlertDetails	• Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • Report Manager • Basic Administrator • Basic Operator
GetAlertFolders	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • Enterprise Administrator • Organization Administrator • Plan Incident Manager • Plan Manager • System Administrator
GetAlertSummaryReport	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator
GetAlertHierarchySummaryReport	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator

API	Required role
GetAlertDeviceSummaryReport	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator
GetAlertDistributionListSummaryReport	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator
GetAlertResponseDetail	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator
GetAlertDetailsByUser	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator

API	Required role
GetAlertDetailsByUsersDevices	• Alert Manager • Advanced Alert Manager • Advanced Alert Publisher • End Users Manager • Enterprise Administrator • Organization Administrator • Report Manager • Basic Administrator • Basic Operator
GetRolesController	• Enterprise Administrator • Organization Administrator • System Administrator • Basic Administrator

MTLS service error codes

The BlackBerry AtHoc MTLS service returns error codes in the form of a JSON file in the following format:

```
{
      "errors" : [
          {
              "code" : "<error-code-1>",
              "field" : "<field-name>",
              "message" : <error-message>"
          },
          {
              "code" : "<error-code-2>",
              "field" : "<field-name>",
              "message" : "<error-message>"
           }
      ]
}
```

Error code	Handler	Error message
HTTP 403	IIS	The user certificate is invalid or unable to contact the Certificate Authority (CA.)
HTTP 401	IIS	The user certificate is expired or blacklisted.
HTTP 500	IIS	Other (internal server error.)
1020	Mobile MTLS Token Service	The request contains an invalid RedirectUri. The parameter exists in the query string and is not an empty value.
1030	Mobile MTLS Token Service	The request contains an invalid organization code.
2010	Mobile MTLS Token Service	MTLS authentication is not configured for the organization (based on the organization code and Client ID.
2020	Mobile MTLS Token Service	The primary regex (CAC/PIV) is not defined for the organization.
2030	Mobile MTLS Token Service	The mapping ID cannot be extracted from the certificate. The regex is invalid or the mapping ID is empty.

Error code	Handler	Error message
3010	Mobile MTLS Token Service	The user could not be found in BlackBerry AtHoc. The mapping ID is not set for the user.
3020	Mobile MTLS Token Service	The user is disabled or deleted in BlackBerry AtHoc.

AtHoc Query Language attribute types

The following table lists the AtHoc Query Language (AQL) attribute types and their supported operators in the BlackBerry AtHoc API.

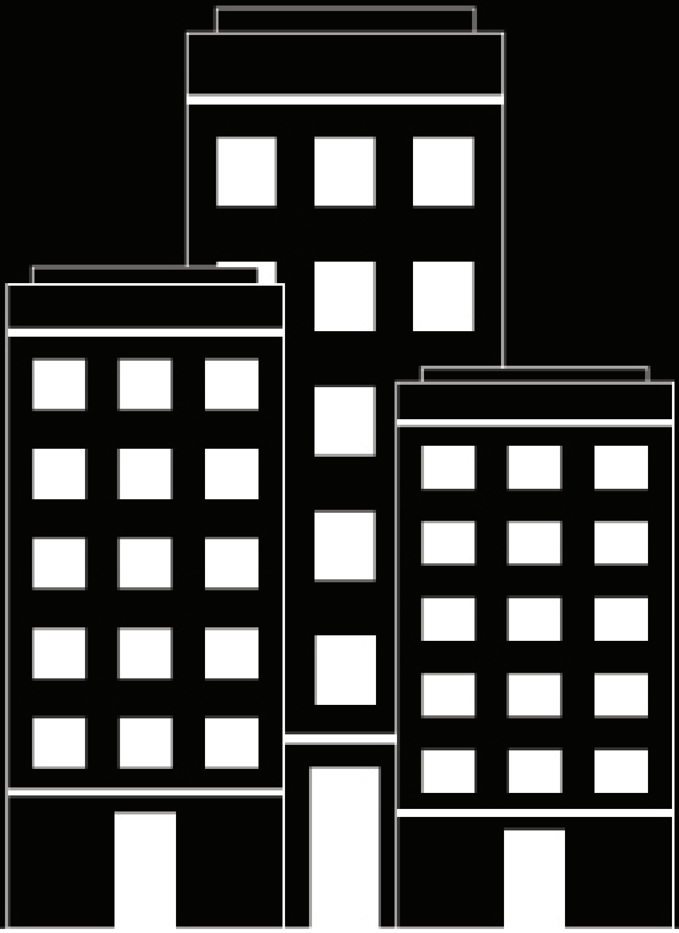
Attribute type	Operators	AQL example
Checkbox		
	• IsYes	• <checkbox> pr
	• IsNoOrEmpty	• <checkbox> npr
Date		
	• Equals	• <date> eq '1/1/1900'
	• NotEquals	• <date> ne '1/1/1900'
	• Before	• <date> lt '1/1/1900'
	• After	• <date> gt '1/1/1900'
	• IsEmpty	• <date> npr
	• IsNotEmpty	• <date> pr
Date Time		
	• Before	• <datetime> lt '1/1/1900', <datetime> lt 'D:0', <datetime> lt 'D:+1', <datetime> lt 'D:-999'. D:0 means Now, D:+1 means 1 day from now, D:-999 means before 999 days.
	• After	• <datetime> gt '1/1/1900'
	• IsEmpty	• <datetime> npr
	• IsNotEmpty	• <datetime> pr
Multi Select		
	• Equals	• <multiselect> eq '<val1>,<val2>,<val3>'
	• NotEquals	• <multiselect> ne '<val1>,<val2>,<val3>'
	• IsEmpty	• <multiselect> npr

Attribute type	Operators	AQL example
	• IsNotEmpty	• <multiselect> pr
Number		
	• Equals	• <number> eq 100
	• NotEquals	• <number> ne 100
	• LessThan	• <number> lt 100
	• GreaterThan	• <number> gt 100
	• GreaterThanOrEqualTo	• <number> ge 100
	• LessThanOrEqualTo	• <number> le 100
	• IsEmpty	• <number> npr
	• IsNotEmpty	• <number> pr
Single Select		
	• Equals	• <singleselect> eq '<val1>'
	• NotEquals	• <singleselect> ne '<val1>'
	• IsEmpty	• <singleselect> npr
	• IsNotEmpty	• <singleselect> pr
Status (Single Select)		
	• Equals	• <status> eq '<val1>'
	• NotEquals	• <status> ne '<val1>'
	• IsEmpty	• <status> npr
	• IsNotEmpty	• <status> pr
Text		
	• Equals	• <text> eq '<value>'
	• NotEquals	• <text> ne '<value>'
	• StartsWith	• <text> sw '<value>'
	• EndsWith	• <text> ew '<value>'

Attribute type	Operators	AQL example
	• Contains	• <text> co '<value>'
	• DoesNotContain	• <text> nco '<value>'
	• IsEmpty	• <text> npr
	• IsNotEmpty	• <text> pr
Org Hierarchy		
	• At	• <orghierarchy> eq '<val1>,<val2>,<val3>'
	• AtOrBelow	• <orghierarchy> sw '<val1>,<val2>,<val3>'
	• NotAt	• <orghierarchy> ne '<val1>,<val2>,<val3>'
	• NotAtOrBelow	• <orghierarchy> nsw '<val1>,<val2>,<val3>'
Roles		
	• Equals	• SYS:role eq '<val1>,<val2>,<val3>'
	• NotEquals	• SYS:role ne '<val1>,<val2>,<val3>'
	• IsEmpty	• SYS:role npr
	• IsNotEmpty	• SYS:role pr
Device		
	• Equals	• <device> eq '<address>'
	• NotEquals	• <device> ne '<address>'
	• StartsWith	• <device> sw '<address>'
	• EndsWith	• <device> ew '<address>'
	• Contains	• <device> co '<address>'
	• DoesNotContain	• <device> nco '<address>'
	• IsEmpty	• <device> npr

Attribute type	Operators	AQL example
	• IsNotEmpty	• <device> pr
Geolocation		
	• IsInside	• <location> in '<namedshape>'
	• IsOutside	• <location> nin '<namedshape>'
Users		
	• Include	• :USERS eq '<user1>,<user2>,<user3>'
	• Exclude	• :USERS ne '<user1>,<user2>,<user3>'
Distribution Lists		
	• Equals (MemberOf / belongs to)	• :LISTS eq '<list1>,<list2>,<FolderLineage>'
	• Not Equals (NotMemberOf / not belongs to)	• :LISTS neq '<list1>,<list2>,<FolderLineage>'
Alert Targeting or Result Based Targeting (RBT)		
	3 Parameters	• :ALERT ('<guid>','<response>','<fillcount>')
	• :ALERT	• :ALERT [Name eq '<guid>' AND Response eq '<response>']
	• :RESPONSE	• :ALERT [Name eq '<guid>']
	• :FILLCOUNT	• :ALERT [Name eq '<guid>' AND Response eq '<response>' AND FillCount eq '<fillcount>']
Event Based Targeting (EBT)		
	3 Parameters	• :ALERT ('<guid>','<response>','<fillcount>')
	• EVENT	• :EVENT ('<guid>','<response>','<property>', '<value>')
	• :RESPONSE	• :EVENT [Name eq '<guid>' AND Response eq '<response>' AND

Attribute type	Operators	AQL example
	• :RESPONSEMETA	• :STATUS.'<metaproperty>' eq '<value>']



BlackBerry AtHoc

Single Sign-On

7.16

Contents

Enable single sign-on as an authentication method

The Single Sign-On feature is not enabled by default. A system administrator must enable SSO in the Feature Enablement settings in the BlackBerry® AtHoc® management system. For more information, see "Enable and disable features" in the *BlackBerry AtHoc System Settings and Configuration* guide.

When SSO is enabled for your organization, if your users are already authenticated and signed in using your identity provider (IDP), they do not need to sign in again to access the BlackBerry AtHoc management system or Self Service.

Note: SSO is supported on the desktop app when the authentication method is set to "Defer to Self Service" and Self Service is enabled for SSO.

If a user is not signed in, they are redirected to their organization's customer IDP login when they attempt to sign in. This IDP is managed by your organization or by a third party vendor that provides IDP services. The IDP authenticates the user. The user is then redirected to BlackBerry AtHoc. If the user is already signed in to the IDP they are automatically redirected to the BlackBerry AtHoc management system or Self Service with an active session.

You must have organization administrator, enterprise administrator, or system administrator permissions to enable single sign-on as a user authentication method.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select the Single Sign-On (SSO) **Enable** check box.
5. Click **Save**.

Enable single sign-on for Self Service

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Self Service** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/selfservice/*organization-code*. This URL is used when users attempt to access Self Service using SSO authentication.
5. Optionally, if you selected **Single Sign-On** as the authentication method, select **Username and Password** from the **Alternative Authentication Method** list to enable both SSO and Username/Password user authentication.

   Note: When an alternative authentication method is added, the Self Service sign-in URL is appended with /sso for single sign-on authentication. For example, <*server*>/selfservice/*organization-code*/sso.
6. Click **Configuration**.

   Note: If the **Configuration** button is not available, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
7. On the **Self Service SSO configuration** window, export SP and IDP settings and then import IDP settings.

   Note: You can also configure the IDP and SP settings manually. For more information, see Configure identity provider settings and Configure service provider settings.
8. Click **Apply**.
9. Click **Save**.

Enable single sign-on for the BlackBerry AtHoc management system

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Management System** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/client/*organization-code*. This URL is used when a user attempts to access the BlackBerry AtHoc management system using SSO authentication.

   Note: If the **Authentication Method** list is disabled, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
5. Click **Configuration**.
6. On the **Management system SSO configuration** window, export SP and IDP settings and then import IDP settings.

   Note: You can also configure the IDP and SP settings manually. For more information, see Configure identity provider settings and Configure service provider settings.
7. Click **Apply**.
8. Click **Save**.

Import a service provider certificate

Import a BlackBerry AtHoc signed service provider certificate for use in Single Sign-On (SSO.) This enables administrators to select a BlackBerry AtHoc certificate instead of uploading and maintaining a custom SP certificate.

You must be a System Administrator to import a service provider certificate.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Security Policy**.
5. On the **Security Policy** page, in the **Service Provider Certificate** section, click **Import Certificate**.
6. On the **Import Certificate** window, enter a valid password for the service provider certificate.
7. Click **Browse** and navigate to and select a valid BlackBerry AtHoc certificate. Only .pfx and .p12 files can be imported.
8. Click **Import**.
9. On the **Security Policy** page, click **Save**.

Configure identity provider settings

The identity provider (IDP) provides authentication for users. The service provider (SP), in this case BlackBerry AtHoc or Self Service, requests authentication from the IDP.

When SSO is enabled for access to the BlackBerry AtHoc management system or Self Service, when a user logs in, they are redirected to their organization's IDP for authentication. If the user is already logged in to the identity provider, the authentication request is processed and sent to the service provider, and the user is granted access without the need to log in again.

1. Log in to the BlackBerry AtHoc management system as an organization administrator or enterprise administrator.
2. Click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** page, in the **Assign Authentication Methods to Applications** section in the **Self Service** or **Management System** section, click **Configuration**.

   Note: If the **Configuration** button is not available, SSO is not enabled. For more information, see Enable single sign-on as an authentication method.
5. Do one of the following:

   - Import IDP settings.
   - On the **Management system SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, configure the following **General Settings**.

     a. **Identity Provider Name**: Each SAML configuration is identified by a unique identity provider name. This name is internal to the configuration and is not exposed to partner providers. This field is required only when there are multiple SAML configurations. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
     b. **Sign On Service URL**: Enter the URL of the location of the identity provider's SSO service where SAML authentication requests are sent as part of a SP-initiated single sign-on.
     c. **Sign On Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
     d. **Logout Service URL**: The URL of the local service provider's single log out service where SAML logout messages are received. If single logout is not required, leave this field blank. For more information, see SSO logout service.
     e. **Logout Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
     f. **Artifact Resolution Service URL**: Optionally, enter an artifact resolution service URL. The service provider uses the Artifact Resolution Protocol to exchange an artifact for the actual SAML message referenced by the artifact.
     g. **Artifact Resolution Service Binding**: Optionally, select **SOAP**, **POST**, **REDIRECT** or **ARTIFACT** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default is **SOAP**.
     h. **Name ID Format**: Optionally, select **Email Address**, **Persistent**, or **Transient** as the format to be used by the SP and IDP to identify a subject name identifier.
     i. **User Mapping Attribute**: Optionally, select the attribute that identifies the user. This attribute is retrieved from the SAML assertion metadata. The default is **Subject Name**.
     j. **Attribute Name**: Enter the name of the attribute used to identify the user.
6. Configure the following **Security Settings**:

a. **SAML Response Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML responses sent to the partner service provider must be signed. Sending signed authentication requests is highly recommended, but optional.

b. **Assertion Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML assertions sent to the partner service provider must be signed.

Note: You must select **Signed** for either **SAML Response Signature** or **Assertion Signature** or both.

Note: You must have a valid certificate installed for your organization.

c. **Signature Algorithm**: Select an algorithm. The default is **RSA-SHA256**.

d. **Assertion Encryption**: Select **Encrypted** or **Unencrypted**. When **Encrypted** is selected, SAML assertions sent to the partner service provider must be encrypted.

e. If **Assertion Encryption** is set to **Encrypted**, select an **Assertion Algorithm**. The default setting is **AES128**.

f. In the **Certificate*** field, click **Browse** to navigate to and select a certificate file. Only .cer and .crt files are supported.

7. Optionally, add the following **Additional information**:

a. **Company Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>

b. **Company Display Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>

c. **Company URL**

d. **Contact Person Name**

e. **Role or Department**

f. **Email Address**

g. **Telephone Number**

8. Do one of the following:

- If you are modifying an existing SSO configuration, click **Apply**, and then click **Save** on the **User Authentication** page.
- For a new SSO configuration, configure Service Provider settings.

Configure service provider settings

1. Log in to the BlackBerry AtHoc management system as an organization administrator or enterprise administrator.
2. Click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** page, in the **Assign Authentication Methods to Applications** section in the **Self Service** or **Management System** section, click **Configuration**.
5. In the **Management system SSO configuration** or **Self Service SSO configuration** window, scroll down to the **Service Provider** section.
6. Configure the following **General Settings**:

    a. **Service Provider Name**: Enter the name of the service provider that sends the SAML authentication request. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>

    b. **Assertion Consumer Service URL**: This field is pre-populated with the service provider's endpoint URL that receives the SAML from the identity provider. The assertion consumer service URL is appended with the organization code. For example:

    - Self Service URL: `https://domain/SelfService/Account/NewSSO/`*`organization-code`*
    - BlackBerry AtHoc management system: `https://domain/Client/`*`organization-code`*

    c. **Logout Service URL**: This field is pre-populated with the URL of the service provider's endpoint that receives SAML log out messages. For more information, see SSO logout service.

    d. **Custom Logout URL**: Optionally, enter a custom URL to redirect users to at logout.

    e. **Custom Logout Service Binding**: Optionally, select **POST** or **Redirect** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner IDP. The default setting is **POST**.
7. Configure the following **Security Settings**:

    a. **SAML Request Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML authentication requests received from the partner service provider must be signed. Receiving signed authentication requests is optional, but highly recommended.

    b. If **SAML Request Signature** is set to **Signed**, select a **Signature Algorithm**. The default setting is **RSA-SHA256**.

    c. In the **Certificate*** section, do one of the following:

    - Select **Use BlackBerry Certificate** to use the signed BlackBerry certificate.

      Note: A system administrator must upload a valid BlackBerry signed certificate for this option to appear.
    - Select **Use Custom Certificate** and click **Import Certificate**. On the **Import Certificate** window, enter a password and click **Browse**. Navigate to and select a valid certificate file. Click **Import**. Only .pfx and .p12 file types are supported.
8. Click **Apply**.
9. On the **User Authentication** page, click **Save**.

SSO logout service

If the logout URL is configured in the identity provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider forwards the logout request to an identity provider.
3. The identity provider validates the logout request.
4. The identity provider sends a logout request for the user to all other service providers that the identity provider is aware of that the user has an active security session with.
5. The identity provider terminates the user's sessions and sends a response to the original service provider.
6. The original service provider informs the user that they have been logged out.

If the logout URL is displayed in the Service Provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider terminates any of the user's active sessions that are handled by a third-party service.
3. The service provider forwards the logout request to the logout URL.

If the logout URL is not configured for either for identity provider or the service provider, when a user requests a logout, the service provider terminates the user's active session and displays the login page (for the BlackBerry AtHoc management system) or the sign out page (for Self Service.)

The following table describes the log out flows for the BlackBerry AtHoc management system:

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom logout URL.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the organization's SSO login URL.
Session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Sign out or session timeout	IDP	No	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the custom logout URL.
Session timeout	IDP	No	No	The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Sign out	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.
Sign out	IDP	No	No	The end user is signed off locally and redirected to the manual login page.

The following table describes the log out flows for Self Service:

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the sign out page.

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	IDP	No	No	The end user is signed off locally and redirected to the sign out page.

Export SP and IDP settings

When you configure single sign-on, you can export settings data from the IDP and SP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Export**. The IDP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
2. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Service Provider** section, in the **General Settings** section, click **Export**.

   Note: Password and private key information is excluded from service provider metadata exports.

   The SP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
3. Click **Save**.

Import IDP settings

When configuring SSO, you can export and then import settings data from the IDP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Import**.
2. On the **Import Identity Provider Configuration** window, click **Browse** to select the .xml file that contains your IDP configuration.
3. Click **Open**.
4. Click **Import**. The fields in the Identity Provider section are populated with the data from the imported .xml file. If any fields were filled in before the import, they are over-written. If the .xml file contains any invalid fields, an error is displayed and no settings are imported.
5. Click **Apply**.

Import an existing IDP configuration

If you have an existing database-driven implementation of SSO and want to migrate to the improved user-interface based SSO solution, you can migrate the settings configuration from your IDP and import it into the BlackBerry AtHoc management system.

Contact your account representative or BlackBerry AtHoc customer support to obtain a copy of the `Utilities.zip` file needed to perform an SSO migration.

Note: Only IDP configurations can be imported. The SP configuration must be entered manually in the BlackBerry AtHoc management system. See Configure service provider settings.

1. Open a Windows command prompt and navigate to the following folder:

   ```
   <installed-directory>\AtHocENS\ServerObjects\Tools\SSO\EasyConnect
   ```

2. Run the following command to create and export a SAML metadata XML file:

   ```
   ExportMetadata.exe –partner <name> [-config <directoryName] [-baseurl <url>] [-
   file <filename>]
   ```

   where:

   - partner <*name* >: The name of the partner IDP configured in the `idp-partner.config` file or the partner SP configured in the `sp-partner.config` file.
     - If you specify a partner IDP, the corresponding local SP metadata is generated for the partner IDP.
     - If you specify a partner SP, the corresponding local IDP metadata is generated for the partner SP.
   - [-baseurl <*url*>]: Specify the directory that contains the EasyConnect configuration files. If you do not specify this directory, the export defaults to C:\EasyConnect\EasyConnectServer.
   - [-file <*filename* >]: Optionally, specify the name of the generated SAML metadata file. By default, the export uses the file name metadata.xml.

     Examples:

     - ExportMetadata.exe –partner ExampleIdentityProvider
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory"**
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com"*
     - ExportMetadata.exe –partner ExampleIdentityProvider config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com" -file "<File path>"**

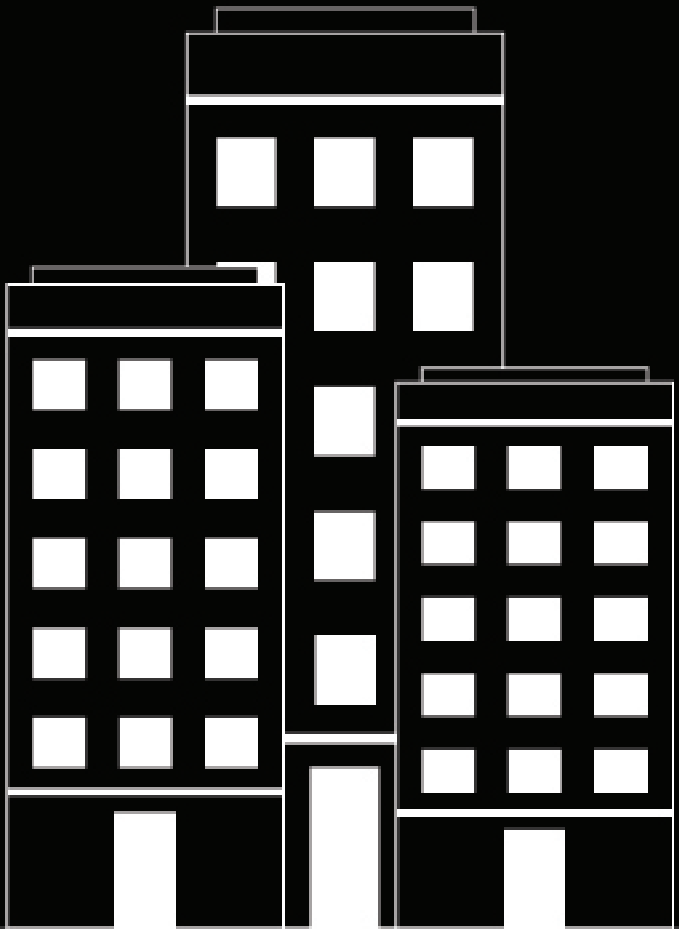
3. Log in to the BlackBerry AtHoc management system and use the SSO IDP import feature to import the IDP metadata. See Export SP and IDP settings and Import IDP settings.

Enable SSO certificate revocation list checking

When single sign-on is enabled for your organization, a CRL is maintained. A CRL is a list of digital certificates that have been revoked and should not be trusted. If CRL checking is enabled, BlackBerry AtHoc checks the CRL before initiating a SAML authentication request to an identity provider or after receiving an SAML response from the IDP.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **SSO CRL (Certificate Revocation List) Settings** section, select the **Enable CRL Checking** option.

   Note: If the **SSO CRL (Certificate Revocation List) Settings** section is not visible, single sign-on is not enabled. See Enable single sign-on for Self Service and Enable single sign-on for the BlackBerry AtHoc management system.
4. In the **CRL Timeout Interval** field, enter the number of seconds to allow for certificate validation information to be retrieved from the CA. The minimum is 1 and the maximum is 60 seconds. The default is 20 seconds.
5. Optionally, select the **Ignore Verification Errors** option. If this option is selected, a certificate that fails verification will continue to be used and an error is logged. If this option is not selected, any certificate that fails verification is not used.
6. Click **Save**.



BlackBerry AtHoc

Smart Card Authentication

7.16

Contents

What is smart card authentication?

When smart card authentication is enabled in addition to regular username/password authentication, users can log in to BlackBerry® AtHoc® by inserting their smart card into a card reader and then entering a PIN, or by selecting a valid certificate on the mobile app.

If you choose to require operators to log in using smart cards, the following changes occur in the administrative side of the BlackBerry AtHoc system:

- All sub organizations of the main organization inherit the smart card-only authentication method.
- The log in screen continues to display **Username** and **Password** fields because until a user attempts to log in, the system does not know what organization the user belongs to and what restrictions, if any, the user's organization has imposed on authentication.
- After the user attempts to log in with a username or password combination, the system returns an error message informing them that they must use their smart card for system authentication.

How smart card authentication works in BlackBerry AtHoc

When smart card authentication is enabled, the operator's mapping ID (MID) attribute is used to authenticate the operator at log in. The data in the mapping ID comes from one of the following sources:

- A sync with Active Directory's attribute (sAMAccountName, userprincipalname, or mail) when using the User Sync Client tool.
- A user import using the Import option in the End Users manager in BlackBerry AtHoc that includes the mapping ID column.
- A manual update of an operator's mapping ID in the End Users manager in BlackBerry AtHoc.

BlackBerry AtHoc uses a regular expression to extract the value for the mapping ID from one of the HTTP header fields that contains the certificate data. BlackBerry AtHoc then compares this mapping ID with the operator's mapping ID to determine their identity. The values for the HTTP header field and the regular expression are specified in the database and can be modified. However, the values apply system-wide and cannot be different for each organization.

The middle tier code attempts to use the primary HTTP_CAC_VARIABLE, if present, and validates the operator. If a valid operator is not found, the middle tier code then attempts to use ALT_HTTP_CAC_VARIABLE to validate the operator.

In BlackBerry AtHoc release 7.3 or later, if a valid operator is not found, the middle tier code then attempts to use the Subject Alternative Name to validate the operator.

Table 1: Login source code by BlackBerry AtHoc release

BlackBerry AtHoc release	File
6.1.8.85R3SP4CP1	wwwroot\client\dotnet\Controllers\AuthController.cs
7.0.0.2	wwwroot\client\dotnet\Controllers\SmartCardController.cs

Enable smart card authentication for operators

When smart card authentication is enabled, in addition to regular username/password authentication, users can log in to BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. On the mobile app, they can select a valid certificate. When smart card authentication is required, users must access BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN.

Note: In order to use this option, you must set up mapping IDs for each user through the users manager in the BlackBerry AtHoc management system.

BlackBerry AtHoc management system configuration

Use the BlackBerry AtHoc management system to enable smart card log in for operators.

1. Log in to the BlackBerry AtHoc management console as an administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Security Policy**.
5. In the **Smart Card Authentication** section, select **Enabled** beside **Smart Card Login**.
6. Optionally, to require smart card authentication, select **Require Smart Card**.
7. Click **Save**.

Note: This is a system-wide setting that applies to all organizations.

IIS configuration

Smart card authentication for operator log in requires the following settings in IIS. In the SSL Settings feature under the client web application, select the **Require SSL** check box and the **Require** option under “Client certificates.”

Table 2: SSL settings by BlackBerry AtHoc version

Version	Notes
All	Default web site > SSL Settings: Required + Ignore
6.1.8.87 CP1CHF2 and earlier	Default web site > Client > SSL Settings: Required + Accept
6.1.8.87 CP1CHF4 and later	Default Web Site > Client >SmartCard > SSL Settings: Required + Accept Default Web Site > SelfService > AuthCAC > SSL Settings: Required + Accept

Enable smart card authentication for the mobile app

When smart card authentication is enabled for the mobile app, when an operator starts the alert publishing, report summary, or accountability officer respond-on-behalf-of-others (ROBO) flows, a window appears for the operator to select a valid certificate. The certificate must already be present on the operator's device. When a valid certificate is selected, the operator can then complete the flow. If the selected certificate is not valid, the operator is redirected to the username and password login screen. When the operator selects a valid certificate, they are redirected to the mobile app to complete the flow. If the selected certificate is not valid, or the smart card authentication fails, the operator is redirected to authenticate using their username and password.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** screen, in the **Enabled Authentication Methods** section, select **Enable** beside **Smart Card**.
5. In the **Assign Authentication Methods to Applications** section, in the **Mobile App** section, select **Smart Card**.

   Note: This section appears only when the mobile app gateway is enabled and configured.
6. Click **Save**.

Note: The Username and Password authentication method is enabled by default and cannot be deselected. If smart card authentication is enabled, it is the primary authentication method.

Enable smart card authentication for the Desktop App

This section includes information about configuration updates in the BlackBerry AtHoc management system and IIS that are needed to enable smart card authentication for the BlackBerry AtHoc desktop app.

BlackBerry AtHoc management system configuration

You can enable smart card authentication for the desktop app in the BlackBerry AtHoc management system.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select **Enable** beside **Smart Card**.
5. In the **Assign Authentication Methods to Applications** section, in the **Desktop App** section, select **Smart Card** from the **Authentication Method** list.
6. Select the number of client certificates to collect from the list. The recommended value is 3.
7. Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=(?<edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.
8. Optionally, in the **Client Regular Expression** field, enter a client regular expression in the following format: `.*?(^)(?:(?!\s-[A||E||S]).)*`. This format extracts information from the client certificate subject name to find the identical certificates for authentication. The regular expression provided in the UI is a sample expression that may not be suitable for your environment. You can build you own regular expression or contact BlackBerry AtHoc customer support to configure this field.
9. Optionally, select **Create new user if an account is not found** to configure the desktop app to create a user at sign on if the user does not already exist
10. Click **Save**.

Note: This setting must be configured for each organization.

IIS configuration

Smart card authentication for the desktop app requires the following settings in IIS.

In the **SSL Settings** feature, under the client web application, select the **Require SSL** check box. Smart card authentication for the desktop app works with any of the options under Client certificates. However, to avoid end users receiving a PIN prompt every few minutes, select the **Ignore** option.

Enable smart card authentication for Self Service

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** screen, in the **Enabled Authentication Methods** section, select **Enable** beside **Smart Card**.
5. In the **Assign Authentication Methods to Applications** section, in the **Self Service** section, select **Smart Card** from the **Authentication Method** list.
6. Click **Save**.

Update the application server

The BlackBerry AtHoc application server is supported on Windows 2016 and later versions.

To enable smart card authentication, you must add the following new key in the registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL Value
name: ClientAuthTrustMode Value type: REG_DWORD Value data: 2.
```

Update the database server

Values in the database server that are used in smart card authentication are stored in the GLB_CONFIG_TAB in the ngaddata database. These values include the following items:

- The name of the HTTP header that contains the information.
- The regular expression that is used to extract the information.

Table 3: Version-specific notes

Version	Notes
6.1.8.84 CP9 and earlier	BlackBerry AtHoc version 6.1.8.84 CP9 and earlier do not have a value in the GLB_CONFIG_TAB for the default HTTP header variable. It is hard-coded as SubjectCN.
7.0.0.2 and later	A Require Smart Card option is available that appears when you select Smart Card Login.

Table 4: Smart card settings in PRV_SECURITY_POLICY_TAB

KEY_NAME	6.1.8.90 and earlier	7.0.0.2 and later
SMART_CARD_ENFORCED	Value is not present.	Value is present.

Y = value is present. N = value is not present.

Table 5: Smart card settings in GLB_CONFIG_TAB

KEY_NAME	6.1.8.84 CP9	6.1.8.85 R3SP4 CP1	6.1.8.85 R3SP4CP1 (and hot-fixes)	7.3
ALT_HTTP_CAC_REGEX	Y	Y	Y	Y
ALT_HTTP_CAC_VARIABLE	Y	Y	Y	Y
CAC_CHECK_PRESENT	N	N	Y	Y
CAC_CHECK_VALID	N	N	Y	Y
CAC_REGEX	Y	Y	Y	Y
CAC_SAN_REGEX	N	N	N	Y
HTTP_CAC_REGEX	N	Y	Y	Y
HTTP_CAC_VARIABLE	N	Y	Y	Y

Table 6: Definitions of smart card settings

KEY_NAME	Notes
ALT_HTTP_CAC_REGEX	(Operator log on) Alternate regular expression for extracting the mapping ID from the CAC certificate.
ALT_HTTP_CAC_VARIABLE	(Operator log on) Alternate HTTP header variable that contains the mapping ID from the CAC certificate.
CAC_CHECK_PRESENT	(Operator log on) Specifies if the system should check that the CAC certificate is present.
CAC_CHECK_VALID	(Operator log on) Specifies if the system should check that the CAC certificate is valid.
CAC_REGEX	Primary regular expression for extracting the mapping ID from the certificate data passed by the BlackBerry AtHoc desktop app during sign on.
CAC_SAN_REGEX	(Operator log on) Alternate regular expression to extract the email address from the Subject Alternative Name in the certificate.
HTTP_CAC_REGEX	Primary regular expression for extracting the mapping ID from the certificate during operator log on.
HTTP_CAC_VARIABLE	Primary HTTP header variable to search for mapping ID during Operator log on.

Table 7: Correlation of smart card settings between the database and user interface

KEY_NAME	Visible in management system
ALT_HTTP_CAC_REGEX	No
ALT_HTTP_CAC_VARIABLE	No
CAC_CHECK_PRESENT	No
CAC_CHECK_VALID	No
CAC_REGEX	No
CAC_SAN_REGEX	No
HTTP_CAC_REGEX	No
HTTP_CAC_VARIABLE	No

Determine the regular expression

The following three regular expression values are provided to extract the user's Mapping ID:

1. HTTP_CAC_REGEX: The primary regex in BlackBerry AtHoc for operator login.
2. ALT_HTTP_CAC_REGEX: The first alternate regex in BlackBerry AtHoc for operator login.
3. CAC_SAN_REGEX: The second alternate regex in BlackBerry AtHoc for operator login.

The BlackBerry AtHoc server tries HTTP_CAC_REGEX first. If ALT_HTTP_CAC_REGEX results in an empty string, the server tries to use CAC_SAN_REGEX. If none of these regular expressions extracts a value or retrieves incorrect information, smart card log in fails.

To determine what the issue is, check the certificate and verify that at least one of the regular expressions extracts the value. For more information, see Appendix A: Retrieve certificate information.

Regular expression test tool

You can use an online regular expression test tool to test regular expressions. Enter the data and adjust the regular expression until the mapping ID is extracted from the data.

The SQL to retrieve the current regular expression from the database is:

```
SELECT value FROM GLB_CONFIG_TAB where KEY_NAME = 'ALT_HTTP_CAC_REGEX'
```

When the preconfigured regular expression values do not extract the correct information, modify the regular expression stored in ALT_HTTP_CAC_REGEX. The default value is:

```
(?<MID>\d{8,10})(?!.*\d)
```

Where:

- ?<MID> is the named group MID that the middle tier code requires. The remaining regex inside the parenthesis with ?<MID> is the sub expression: \d{8,10}.
- \d matches any decimal digit, and \d{8,10} matches any number between 8 and 10 digits.
- (?!.*\d) matches a dot 0 or more times, a decimal digit once, and that expression is used by (?<MID>\d{8,10}) to extract numbers with 8 to 10 digits. For example:
  - 0069651550.CBP evaluates to 0069651550 (Good—Extracts between 8 and 10 digits to the left of the decimal.)
  - FIRST.LAST.MI.1233837489 evaluates to 1233837489 (Good—Extracts between 8 and 10 digits to the right of last decimal.)
  - 1234567890.CBP.11223344 evaluates to 11223344 (Good—Extracts between 8 and 10 digits of the last number.)
  - 1234567890.CBP.112233445566 evaluates to 2233445566 (Bad—Truncates digits when there are more than 10. You need to update the regex: (?<MID>\d{8,12}) will work.)

For information on .Net regular expression syntax see:

https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference

If changes are required to accommodate a different format, you have two options:

1. Send the data found above to BlackBerry AtHoc customer support with a request to have engineering determine the new regular expression.
2. Determine the regular expression yourself.

Update the database

Once you have a good regular expression, update the database with it. Use the following SQL to update the database with the new regular expression. Replace 'new_expression' with the new regular expression:

```
UPDATE GLB_CONFIG_TAB SET VALUE = 'new_expression' WHERE KEY_NAME =
'ALT_HTTP_CAC_REGEX'
```

Troubleshooting smart card authentication

If smart card authentication fails after it has been configured, it could be due to the format of the CN string in the certificate. BlackBerry AtHoc has three regular expressions for validating the mapping ID:

- HTTP_CAC_REGEX
- ALT_HTTP_CAC_REGEX
- CAC_SAN_REGEX

These regular expressions are in the `ngaddata.glb_config_tab`. BlackBerry AtHoc attempts to parse the MID using HTTP_CAC_REGEX. If that fails, it attempts to parse the MID using ALT_HTTP_CAC_REGEX. If that also fails, it attempts to parse the MID using CAC_SAN_REGEX.

Sometimes the certificate can be stripped from the header by a proxy server, which causes the validation to fail. In other cases, the regular expression could not parse the data. As a first step, verify that the certificate details are making it through to BlackBerry AtHoc. Use the Test Page described in Appendix A: Retrieve certificate information.

See the sample verbose log entry below, and note that the subject is missing.

If you are getting a 403 error that prevents the login page from displaying, deselect Require SSL in IIS. Otherwise, the call to GetCACMID is not made.

If the certificate information does not appear, it may be due to SSL settings in IIS, or due to a proxy removing the information from the request.

It is possible that the information from the certificate is available, but the certificate is not. Version 6.1.8.87 CP1 with CHF3 and later BlackBerry AtHoc releases have a new property, CAC_CHECK_PRESENT, which can be set to N to work around this issue. This setting is not exposed in the user interface.

Sample verbose log entry

```
<event>
<eventId>12445</eventId>
<type>VERBOSE</type>
<time>02/03/2015 15:36:53.350</time>
<server>D1ASEPRIC090</server>
<categorySource>Management System</categorySource>
<assembly>MSDotNetClient.dll</assembly>
<module>AuthController</module>>
<member>GetCACMID</member>
<shortMessage> CAC: Issuer: SerialNumber: Subject: Valid From: 2/3/2015 3:36:53 PM
 Valid Until: 2/3/2015 3:36:53 PM IsValid: True CertEncoding: 0 Cookie: Present:
 False </shortMessage>
. . . .
```

Appendix A: Retrieve certificate information

You can retrieve certificate information using the following two methods:

- Use the test page in the management system
- Use a sample certificate

Use the test page in the management system

For BlackBerry AtHoc release 6.1.8.88 and later releases, the test page is located at:

https://<server>/client/smartcard/info

For BlackBerry AtHoc release 6.1.8.87 and earlier releases, the test page is located at:

https://<server>/client/auth/ccd

If this test URL does not work, enable verbose logging and search the BlackBerry AtHoc event log for the certificate details. Search for the AuthController module, or the GetCACMID member. Turn off verbose logging after finding the certificate details.

For BlackBerry AtHoc release 6.1.8.84 and earlier releases, check the `servervars.asp` file at:

https://<server>servervars.asp

Use a sample certificate

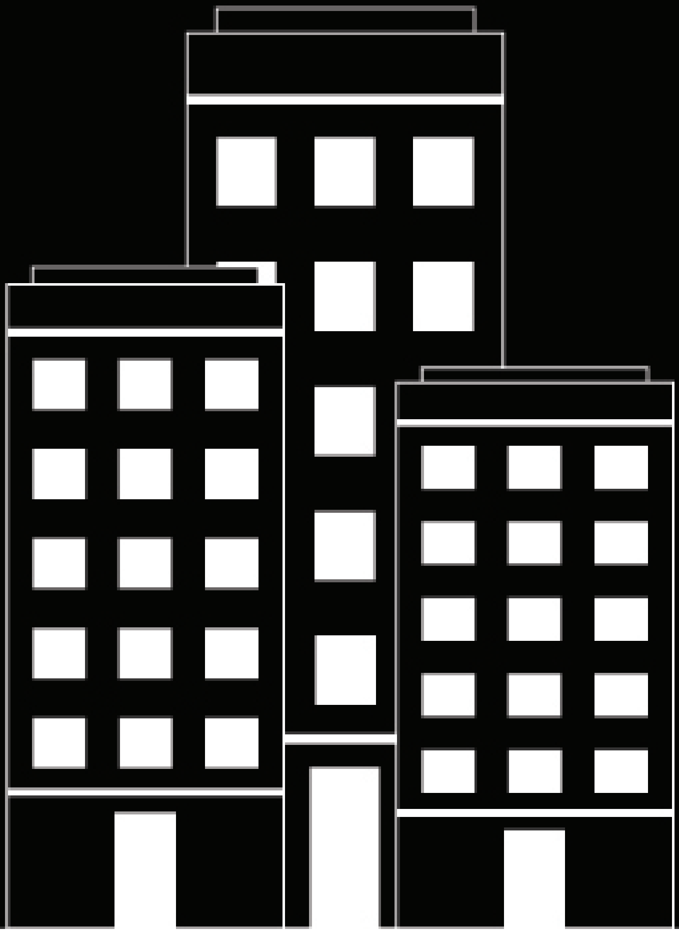
Have the customer provide a sample of the certificate to determine if the regular expression can parse the MID. You may need to request several samples for comparison.

To open a customer's certificate, complete the following steps:

1. From the **Start Menu**, type **MMC** in the search area and press **Enter**.
2. Once the MMC is open, click **FILE** and select **Add / Remove Snap-in**.
3. Select the Certificates Snap-in on the left hand side and click **Add**.
4. When prompted, select **My user account**.
5. Click **Finish**.
6. Click **OK** to close the menu and return to the main console page.
7. Find the user's certificate and open it.
8. On the **Certificate** window, click the **Details** tab.
9. Ensure **Show:** is set to **<All>**.
10. Scroll down and select **Subject**. The MID is displayed in the field below. It is displayed beside the value for CN.
11. Copy the details or click **Copy to File...**. The information in CN is used to determine the proper regular expression to use, which will overwrite the existing value in glb_config_tab.

Some customers with OnPrem systems use more than one type of smart card and will already use one of the regular expressions successfully. In this case, it is necessary to coordinate with the customer on which regex to update (CAC_REGEX or ALT_HTTP_CAC_REGEX) when you have a solution for the CAC/PIV with the issue.

Try to obtain three or four user certificates and compare them.



BlackBerry AtHoc

Localization

7.16

Contents

Overview

A locale is a specific dialect of a language spoken in a region such as Canadian French, Mexican Spanish, and US English. Localization is the process of customizing an application for a given language and region. This document describes how BlackBerry® AtHoc® has been localized to accommodate users with locales beyond US English.

Within the BlackBerry AtHoc system, *Organization* locales define the way the user interface appears to operators, while *Delivery* locales define the way BlackBerry AtHoc alerts appear to alert recipients. Although an organization can be associated with only one organization locale, it can be associated with multiple delivery locales. For more information, see Set delivery locales for an organization.

This document lists the organization locales supported by the BlackBerry AtHoc system and explains the process by which the system determines a user's locale and the impact of localization on the operator user interface. This document describes how to set delivery locales for an organization and how to specify a delivery locale when creating an alert. The characters supported in the system and a list of the localized and non-localized pages in the BlackBerry AtHoc system is also included.

Organization locales

Organization locales define the way the user interface appears to operators. In addition to determining the language to be displayed on BlackBerry AtHoc screens, the organization locale determines the language of the default templates available to operators. These templates include the default date, time, and phone number formats displayed in the user interface.

Supported organization locales

Each organization created within the BlackBerry AtHoc system is associated with *one* of the following language/locale combinations. This combination cannot be changed after it has been set.

- Dutch (Netherlands)
- English (UK)
- English (US)
- French (Canada)
- French (France)
- German (Germany)
- Italian (Italy)
- Spanish (Mexico)
- Spanish (Spain)

Organizations created at the enterprise level within the same system can have different language/locale combinations associated with them. For example, an organization set to Spanish (Spain) can exist in the same system as an organization set to French (Canada), as long as neither one is a suborganization of the other.

All organizations created as suborganizations of an enterprise organization are automatically assigned to the same language/locale combination as the enterprise organization. For example, if an enterprise is set to the Spanish (Spain) language/locale, then its suborganizations are also set to Spanish (Spain.)

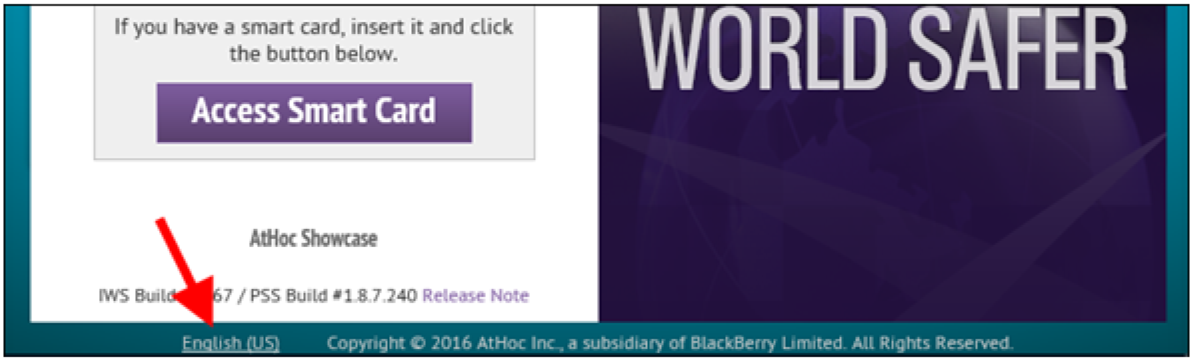
All text in the operator user interface is locked to the selected locale, so all operators within the same organization see the same language displayed throughout the BlackBerry AtHoc system.

Identify an organization locale/language

When you access the BlackBerry AtHoc system login screen for the first time, the system does not know what organization you belong to or what language you will be viewing the system in. The system decides which language to display on the Log In screen by running through the following series of checks:

1. The system searches for any language-related cookies in your browser from past log ins. If you have never logged in before, the system cannot make a determination about the language to display, so it proceeds to the next check.
2. The system tries to use the browser’s preferred locale information to determine the language to display. If the preferred language is not supported within BlackBerry AtHoc or if there is no browser preferred locale information, the system proceeds to the next check.
3. In the absence of any language preference indicators, the system displays US English by default.

The bottom of the Log In page contains a language selection link that enables you to switch the language displayed on the Log In, Forgot Username, and Forgot Password screens.



If you have a smart card, insert it and click the button below.

IWS Build 67 / PSS Build #1.8.7.240 Release Note

Copyright © 2016 AtHoc Inc., a subsidiary of BlackBerry Limited. All Rights Reserved.

Regardless of the language that you select from the drop-down menu, when you successfully log in to the system, the language that is displayed will match the language associated with your organization. If you set the Log In screen to display UK English, but your organization is associated with US English, you will see UK English before you log in and US English after you log in.

Change the default organization locale settings

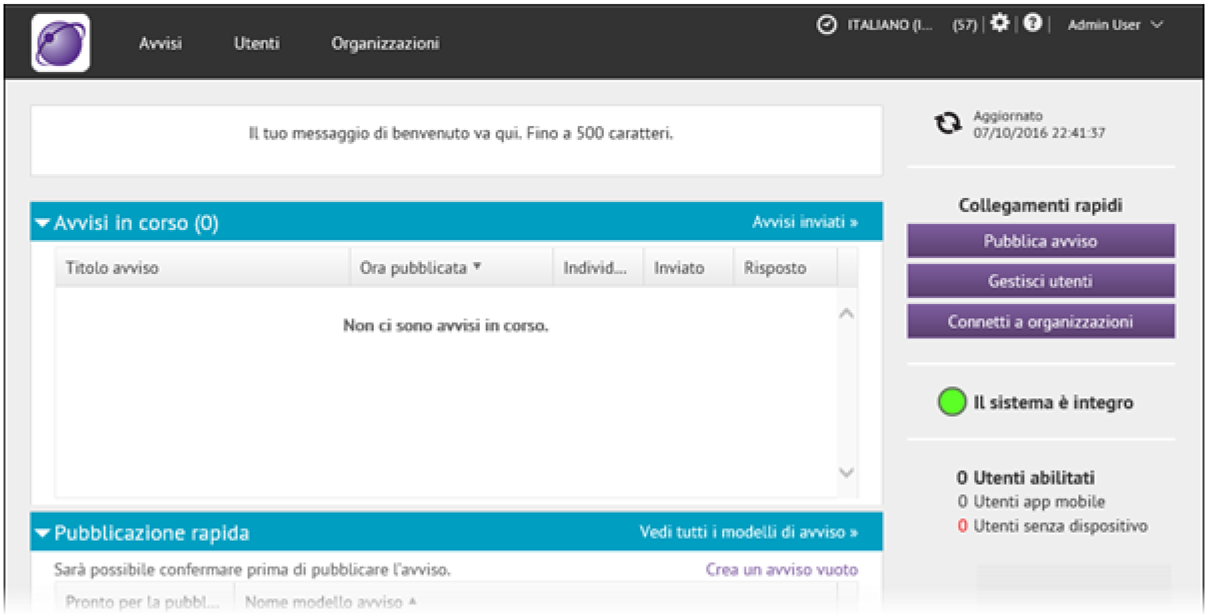
Operators with the necessary permissions can change the default organization locale settings for their organization.

1. Log in to the BlackBerry AtHoc system.
2. In the top navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, scroll down to the **Locale Setting** section.
5. Select the default value for the following lists:
   - **Date Format**
   - **Time Format**
   - **Delivery Locales**
   - **Time Zone**
6. Optionally, in the **Phone Call Setting** section, change the value in the **Default Country Code** field.
7. Click **Save**.

Impact of localization on the operator user interface

The language/locale that is selected affects the following features and components of the operator user interface:

- Operator facing pages, excluding some administrative pages. The image below shows the BlackBerry AtHoc Homepage localized for the Italian (Italy) locale.



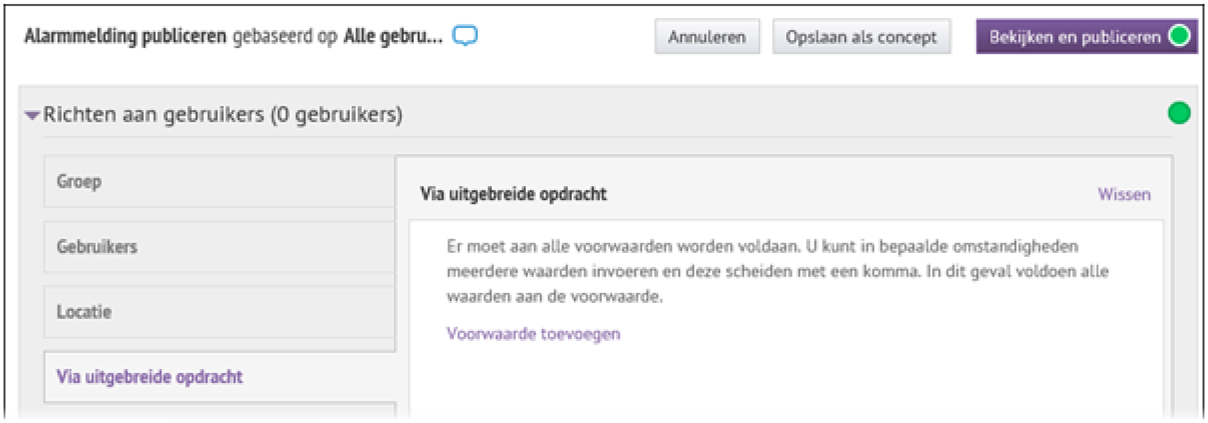
Il tuo messaggio di benvenuto va qui. Fino a 500 caratteri.

Non ci sono avvisi in corso.

Sarà possibile confermare prima di pubblicare l'avviso.

For a list of the screens that are localized, see Localized and non-localized pages in BlackBerry AtHoc.

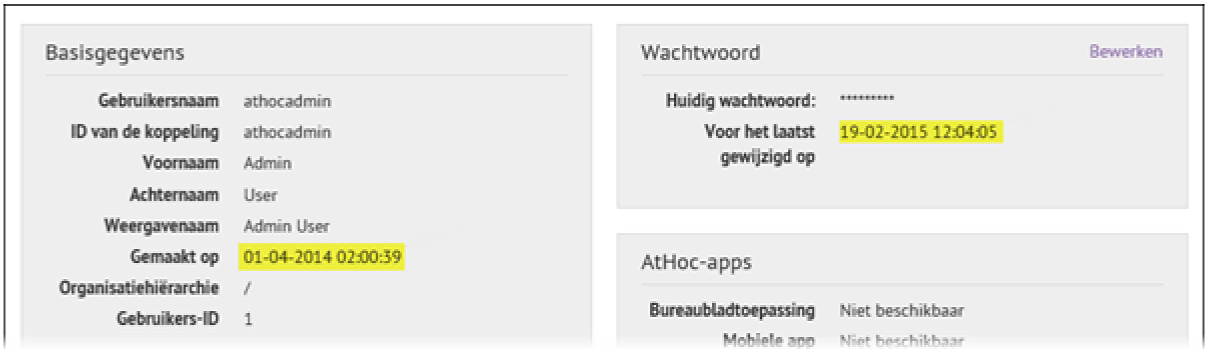
- Out of the box default content, including alert templates, distribution lists, user attributes, and delivery templates. The following image shows the Target Users section of an out-of-the-box alert template localized for the Dutch (Netherlands) locale.



Er moet aan alle voorwaarden worden voldaan. U kunt in bepaalde omstandigheden meerdere waarden invoeren en deze scheiden met een komma. In dit geval voldoen alle waarden aan de voorwaarde.

Note: Custom user attributes are not translated by default. Operators with administrator permissions can provide translations for custom attributes in **Settings** > **Translate Custom Attributes**.

- Date/time default formats. The following image shows the User Details screen localized for the Dutch (Netherlands) locale, with the date and time information presented in the format most commonly used in the Netherlands.



Basisgegevens

Gebruikersnaam athocadmin
ID van de koppeling athocadmin
Voornaam Admin
Achternaam User
Weergavenaam Admin User
Gemaakt op 01-04-2014 02:00:39
Organisatiehiërarchie /
Gebruikers-ID 1

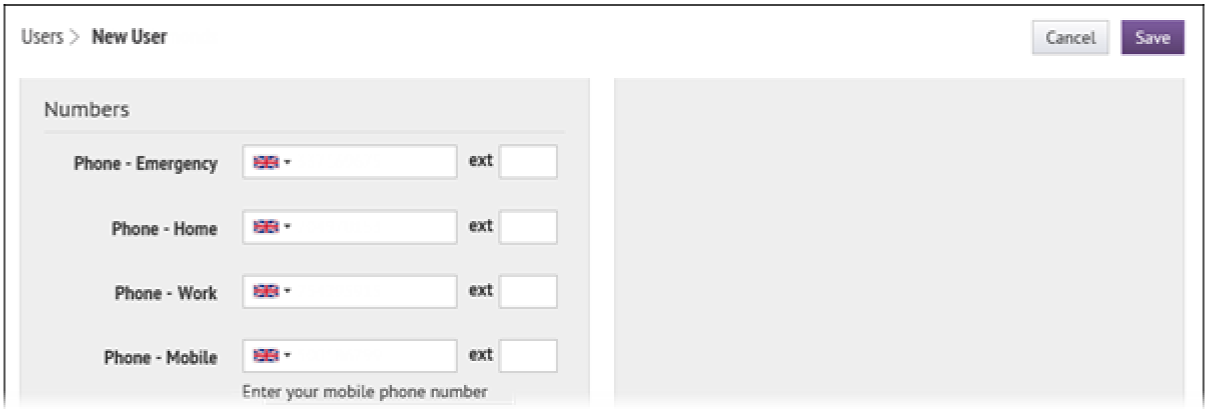
Wachtwoord

Huidig wachtwoord: *********
Voor het laatst gewijzigd op 19-02-2015 12:04:05

AtHoc-apps

Bureaubladtoepassing Niet beschikbaar
Mobiele app Niet beschikbaar

- The default Date, Time, and Time Zone values for a locale can be overwritten by modifying the corresponding fields on the Settings screen. See Change the default organization locale settings for more information.
- Phone default formats. The following image shows the out-of-the-box settings for phone numbers on the New User screen, localized for UK English. The British flag icons in each field indicate that all numbers will be automatically prefaced with the British country code 44.

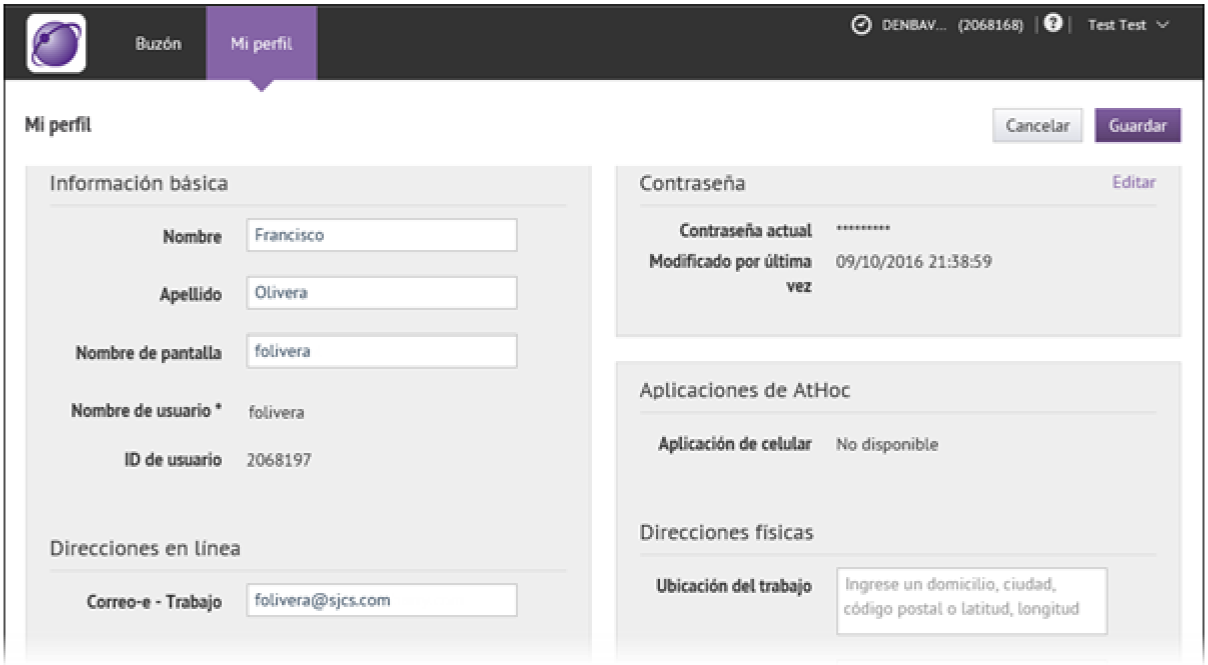


Numbers

Phone - Emergency ext
Phone - Home ext
Phone - Work ext
Phone - Mobile ext
Enter your mobile phone number

The default country code for a locale can be overwritten by modifying the corresponding field on the Settings screen. See Change the default organization locale settings for more information.

- The Self Service experience. The following image shows the User Profile screen in Self Service, localized for the Spanish (Mexico) locale.



Mi perfil

Información básica

Nombre	Francisco
Apellido	Olivera
Nombre de pantalla	folivera
Nombre de usuario *	folivera
ID de usuario	2068197

Direcciones en línea

Correo-e - Trabajo	folivera@sjcs.com

Contraseña

Contraseña actual	**********
Modificado por última vez	09/10/2016 21:38:59

Aplicaciones de AtHoc

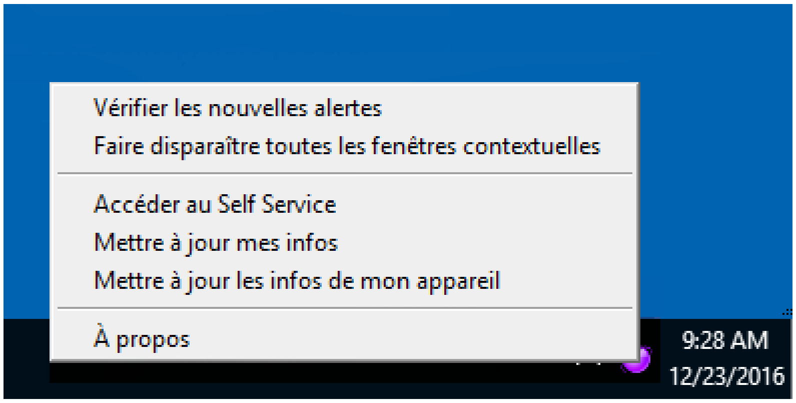
Aplicación de celular	No disponible

Direcciones físicas

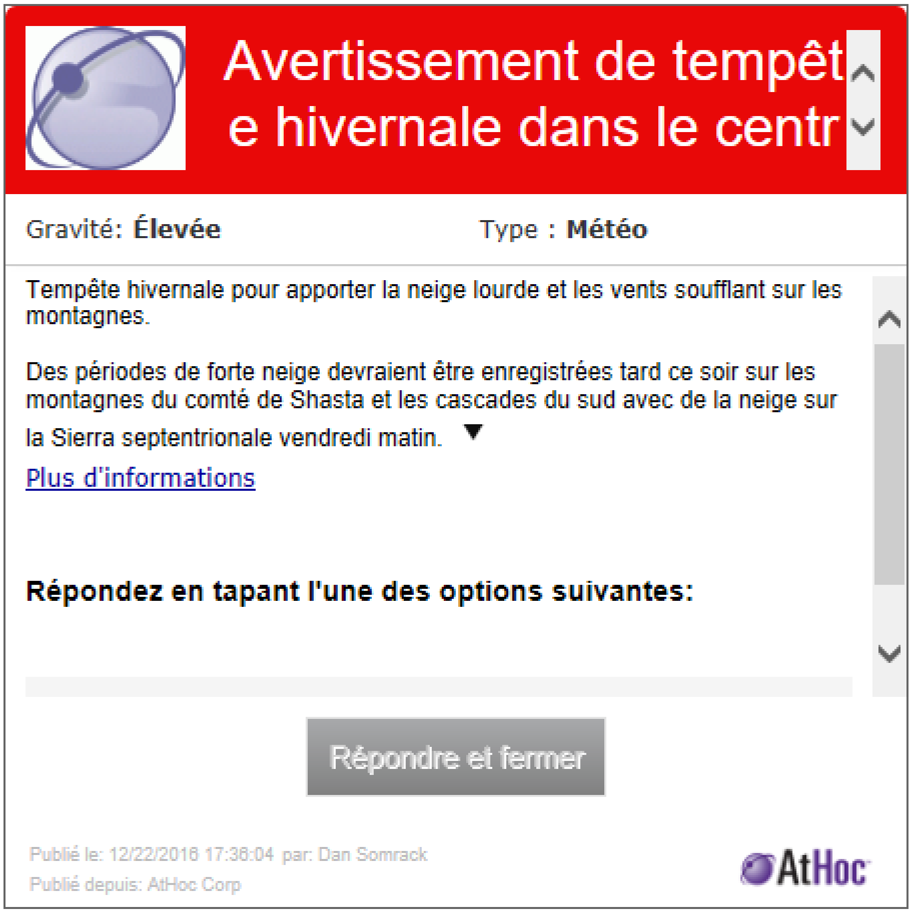
Ubicación del trabajo	Ingrese un domicilio, ciudad, código postal o latitud, longitud

Note: The locale that the user selects can be different than the default locale of their organization.

- The system tray menu for connected desktop applications. The following image shows the menu localized for the French (France) locale.


Vérifier les nouvelles alertes
Faire disparaître toutes les fenêtres contextuelles
Accéder au Self Service
Mettre à jour mes infos
Mettre à jour les infos de mon appareil
À propos
9:28 AM
12/23/2016

- Desktop alerts. The following image shows a desktop alert localized for the French (France) locale.



Avertissement de tempête hivernale dans le centr

Gravité: **Élevée** Type : **Météo**

Tempête hivernale pour apporter la neige lourde et les vents soufflant sur les montagnes.

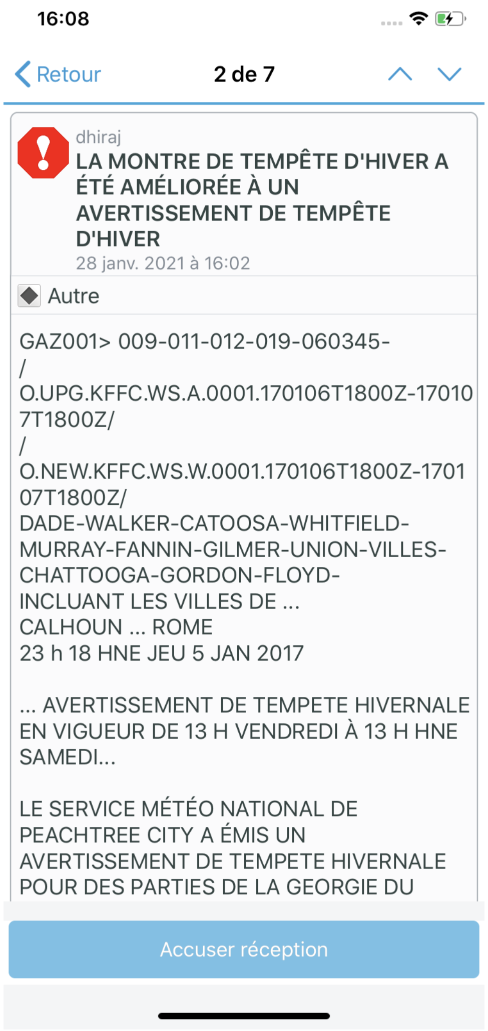
Des périodes de forte neige devraient être enregistrées tard ce soir sur les montagnes du comté de Shasta et les cascades du sud avec de la neige sur la Sierra septentrionale vendredi matin. ▼

Plus d'informations

Répondez en tapant l'une des options suivantes:

Publié le: 12/22/2016 17:36:04 par: Dan Somrack
Publié depuis: AtHoc Corp

- Mobile alerts. For the mobile phone app, the app locale is based on the operating system settings of the phone. If you change your operating system settings, the app displays in the language of your phone, regardless of the delivery locale of a single alert or your organization’s settings. The following image shows the same alert as the desktop alert above, but displayed on a mobile phone with its operating system set to French (Canada).



dhiraj

LA MONTRE DE TEMPÊTE D'HIVER A ÉTÉ AMÉLIORÉE À UN AVERTISSEMENT DE TEMPÊTE D'HIVER

28 janv. 2021 à 16:02

◆ Autre

GAZ001> 009-011-012-019-060345-
/
O.UPG.KFFC.WS.A.0001.170106T1800Z-170107T1800Z/
/
O.NEW.KFFC.WS.W.0001.170106T1800Z-170107T1800Z/
DADE-WALKER-CATOOSA-WHITFIELD-MURRAY-FANNIN-GILMER-UNION-VILLES-CHATTOOGA-GORDON-FLOYD-
INCLUANT LES VILLES DE ...
CALHOUN ... ROME
23 h 18 HNE JEU 5 JAN 2017

... AVERTISSEMENT DE TEMPETE HIVERNALE EN VIGUEUR DE 13 H VENDREDI À 13 H HNE SAMEDI...

LE SERVICE MÉTÉO NATIONAL DE PEACHTREE CITY A ÉMIS UN AVERTISSEMENT DE TEMPETE HIVERNALE POUR DES PARTIES DE LA GEORGIE DU

Delivery locales

Delivery locales define the way alerts appear to alert recipients. In addition to localizing the delivery envelope of an alert—the hard-coded text in the alert, such as the Severity, Type, Response Options titles, and the Copyright information—the delivery locale is used by the text-to-speech engine to determine how to pronounce the alert content when it is read aloud by the system.

For the mobile phone app, the app locale is based on the operating system settings of the phone. If you change your operating system settings, the app will display in the language of your phone, regardless of the delivery locale of a single alert or your organization's settings.

If the Bilingual Alerts feature is enabled, the enabled delivery locales can be used to send an alert in a second, translated language. When an operator selects a second language to send an alert in, users who have selected that language as their preferred language receive the alert in that language. For more information, see Bilingual alerts.

Supported delivery locales

The BlackBerry AtHoc system supports the following delivery locales:

- Arabic (ىبرع)
- Chinese (中國語)
- Deutsch (Deutschland)
- English (UK)
- English (US)
- Español (España)
- Español (México)
- Français (Canada)
- Français (France)
- Greek (Ελληνικά)
- Italiano (Italia)
- Japanese (日本語)
- Korean (한국어)
- Nederlands (Nederland)
- Polish (Polskie)
- Portugues (Brasil)
- Russian (Русский)
- Swedish (Svenska)
- Turkish (Türkçe)

Set delivery locales for an organization

Administrators with the necessary permissions can set the delivery locales for their organization.

1. Log in to the BlackBerry AtHoc management system.
2. In the top navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, scroll down to the **Locale Setting** section.

5. In the **Delivery Locales** field, select the delivery locales from the list that you want to make available to alert creators within your organization.

   Note: Once enabled, support for a delivery locale cannot be disabled.
6. Click **Save**.

Select a delivery locale for an alert

During the creation of an alert, an operator can specify a delivery locale that is different from the organization locale. Only one delivery locale can be associated with an alert, so if you need to send an alert in multiple languages, you must create separate alerts for each language.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Alerts** > **New Alert**.
3. On the **Select from Alert Templates** screen, select an alert template or click **Create a Blank Alert**.
4. On the **New Alert** screen, in the **Content** section, click the language button and select the delivery locale that you want to use for the alert.

   Note: Changing the delivery locale of an alert has no impact on the language displayed in the user interface. The organization locale, which cannot be changed, controls the display language of the fields within the BlackBerry AtHoc system.
5. Create the alert, entering text written in the language that matches the delivery locale.
6. Publish the alert.

   Alert recipients then receive an alert that is fully localized. The operator-provided content and the delivery template—the field names and preset, unchangeable content—match the delivery locale. If a text-to-speech engine is used to listen to the alert, all preset and operator-provided content is read aloud in the language of the delivery locale.

Bilingual alerts

The Bilingual Alerts feature enables operators to select a second language to send an alert to end users. End users can choose their preferred language to receive alerts in from the BlackBerry AtHoc management system, Self Service, or from the mobile app.

A System Administrator must enable the IsBilingualAlertSupport feature in **Settings** > **System Setup** > **Feature Enablement**. Delivery locales must be selected in **Settings** > **General Settings**.

The alert template used to send a bilingual alert must have the Add Bilingual option enabled in the alert template settings.

The bilingual alert can be enabled and a second language selected by an administrator when creating an alert template, or by an operator when sending an alert. The Add Bilingual option is available in the Content section of the alert. The quick edit feature is available for the translation on the Review and Publish page when publishing an alert.

Supported characters

The BlackBerry AtHoc system supports Windows-1252, a set of characters that includes all of the characters that are required for the languages currently supported in the system.

Some of the key fields for alerting support the Unicode character set, which is much larger than Windows-1252. This is important because it enables users to create alerts that have delivery locales that are different from the organization locale. For more information, see Select a delivery locale for an alert.

The following table defines which fields in BlackBerry AtHoc allow which characters.

Text fields or components	Allowed characters	Notes
	User profile fields	
Username	Supported alpha-numeric characters	Avoid spaces and these characters [ ] : ; | = , + * ? < >
All fields on General Settings page: Name, Organization Code, Name on User Pages, Homepage Welcome Message, Footer Text	Supported alpha-numeric characters	Avoid special characters in general. ` ! $ % ^ ( ) = { } , ; : ? " < > |
Friendly Name for User Attributes	Supported alpha-numeric characters	Avoid special characters such as `!$%^()={}.,;\:?"<>|[] &. Although the UX supports Unicode, it will break other flows like import, and API user sync.
Friendly Name for Device	Supported alpha-numeric characters	Avoid special characters such as `! $%^()={},;\:?”<>|
Common Name: Devices, User Attributes, User Attribute Values	Supported alpha-numeric characters	Avoid special characters such as `! $%^()={}.,;\:?"<>|[]&
Values: Device Values, User Attribute Values, Organization Hierarchy	Supported alpha-numeric characters	Keep the values for attributes to supported characters. Special characters create problems when searching for or targeting users. The "&" special character is supported.
XML Layouts: Self Service, User Detailed Layout including Section names, Page Details, help sections	Supported alpha-numeric characters	Use XML escaping for characters for < > & ' and ". The system will show error messages if these are typed in directly.
Import and Export Users with .csv	Supported alpha-numeric characters	
	Alerting	
Alert Title, Alert Body	Unicode support	—

Text fields or components	Allowed characters	Notes
Response Options	Unicode support	—

The following alphanumeric characters are supported:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
ÀÁÂÃÄÅÆÇÈÉÊËÌÍĨÏÐÑÒÓÔÕÖØÙÚÛÜÝÞß àáâãäåæçèéêëìíĩïðñòóôõöøùúûüýþÿŒœŠšŸŽžƒ

Localized and non-localized pages in BlackBerry AtHoc

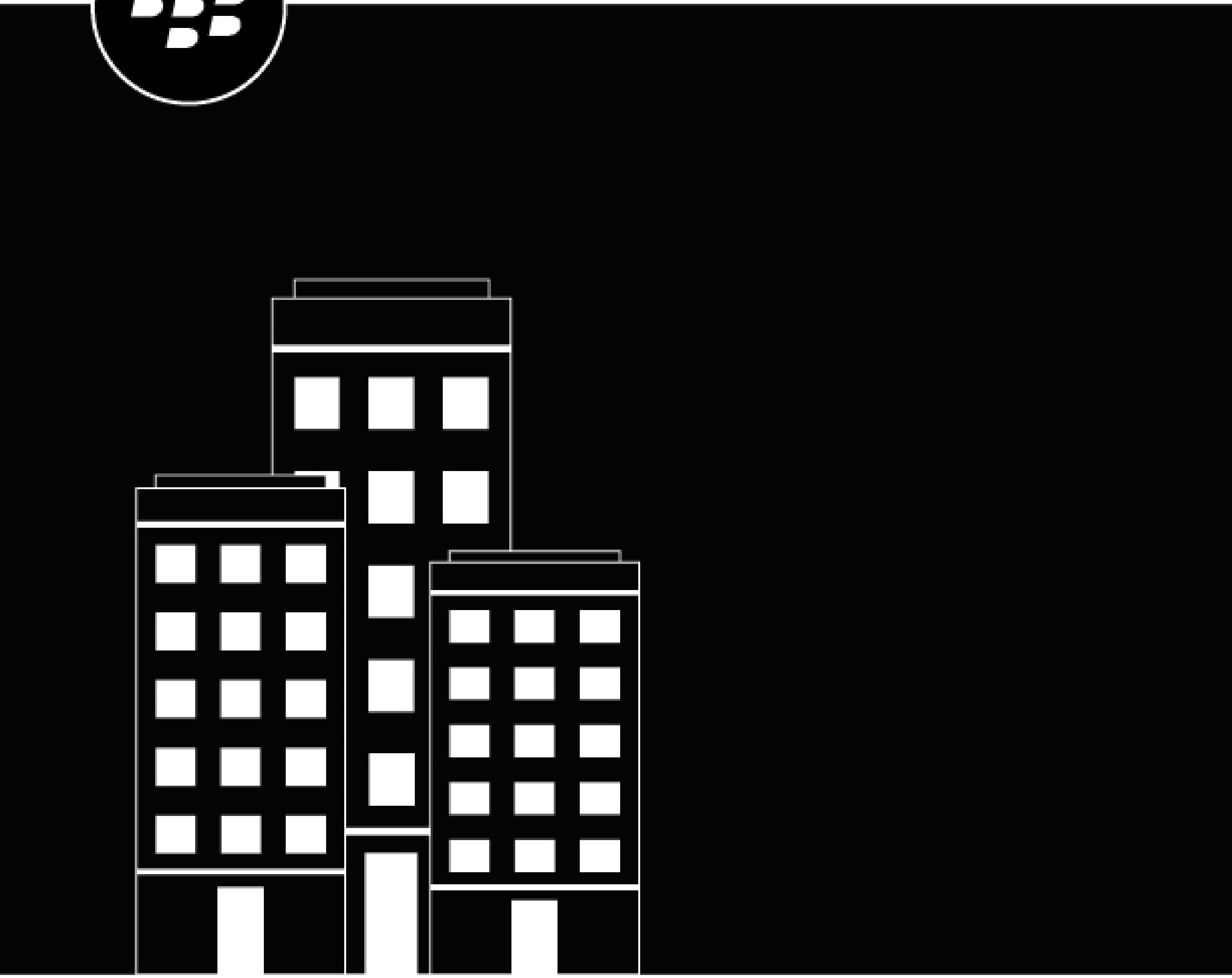
Localized

- Home page
- New Alert page
- Alert templates
- Delivery templates
- Audio files
- Incoming alert rules
- Connect profile
- Security policy
- Invite organization to Connect
- Invitations
- Inbox
- Sent alerts and alert reports
- User manager
- External operator manager
- Distribution list manager
- Connected organizations
- User attributes
- Alert folders
- General settings
- Alert placeholders
- Change organization
- My Details
- Disable and Delete End Users
- Operator audit trail
- Organizations manager
- Organization settings
- Activity log
- Desktop App menu

Not localized

- Mobile alert settings
- Map and layers
- Global system health
- System health
- Diagnostic log
- Archive
- Device manager
- Alert Usage Summary report
- User Summary report
- Personnel reports
- Help & Support page
- Integration manager

- Mass devices manager
- AtHoc Cloud Delivery gateway
- AtHoc Connect gateway
- Other gateways
- Advanced Alert reports
- Online help



BlackBerry AtHoc

Alert Tracking and Reporting

7.16

Contents

Manage alert tracking and reporting

This guide describes how to generate, view, export, and print reports that are available within BlackBerry® AtHoc®.

Run and view personnel reports

Personnel reports are used to determine specific information that could be important to know about groups of people during an emergency. Although the exact list of reports varies depending on the organization, examples of personnel reports include Duty Status, Building Number, Transport Needs, Commanders, Police and Fire Teams, and Work Availability.

Note: When a user is deleted, all of their details are removed from the report. Only the status and responses are retained. The display name for the deleted user is replaced by Del_[GUID].

When you run reports, you can view the output data in any of the following formats:

- **Summary**: Provides a high-level overview of all of the data that has been collected for the report.
- **By organizational hierarchy**: Provides the same information as the Summary report, broken down into each of the organizational groups that exist within the organization.

Create a personnel report based on a user attribute

Personnel reports track the use of user attribute values. For example, a user attribute called *MedicalTraining* might have two single-select picklist values (Yes and No) and be used as response options for an alert. As each user selects a response, the information is added to their user record. At the end of the alert, you can use the personnel report to track the responses.

Note: You must be an Organization Administrator or Enterprise Administrator to create user attributes.

1. From the navigation bar, click **Users** > **User Attributes** and create one of the following types of user attributes:
   - Single-select Picklist
   - Multi-select Picklist
   - Check box
2. Optionally, for a picklist attribute, add new values.
3. In the **Personnel Reports** section, beside **Enabled**, select **Yes**.
4. In the **Personnel Reports** section, enter a name, such as "RO-Accountability". RO indicates that it will be used as a custom response option. This name appears on the Personnel Reports screen.
5. Optionally, add a description for the user attribute.
6. Click **Save**.
7. In the navigation bar, click **Reports** > **Personnel Reports**.
8. On the **Personnel Reports** screen, click **Summary** or **By Organizational Hierarchy**.

View a summary report

Summary reports provide a high-level overview of the data in a report without breaking it down into its component parts. Summary reports are useful when it is necessary to make quick assessments about data and the specific details are not as important at the moment.

1. In the navigation bar, click **Reports** > **Personnel Reports**.
2. On the **Personnel Reports** screen, find the report that you want to create.
3. Click the corresponding **Summary** link.

   The screen refreshes and displays a summary of the relevant data.

   Note: Authorized users can configure the list of categories that appears on the screen.

4. Optionally, on the Summary screen, do any of the following:
    - Click **Print** to print a copy of the report.
    - Click **Export** to export either a summary or the complete report to a .csv file.
    - Click **Show Selection Summary** to view the criteria used to select which users to include in the report.
    - Click **View list** to open a screen that displays the relevant details for each user included in the report.
    - In the **Other Views** section, click **By Organizational Hierarchy** to view the report based on the organizational hierarchies of each user.
    - In the **Other Reports** field, click ⌄ to select a different report. Click **Run report** to view it.

View an organizational hierarchy report

Organizational hierarchy reports present the data you request broken down by increasingly granular levels of detail revealed as you drill further down into the hierarchy.

1. In the navigation bar, click **Reports** > **Personnel Reports**.
2. On the **Personnel Reports** screen, find the report that you want to create and click the corresponding **By Organizational Hierarchy** link.

    The screen refreshes and displays the same data as found in the Summary report, but with the data broken down by both category and hierarchy.
3. On the **By Organizational Hierarchy** screen, do any combination of the following:
    - Click **Print** to print a copy of the report.
    - Click **Export** to export either a summary or the complete report to a .csv file.
    - Click **Show Selection Summary** to view the criteria used to select which users to include in the report.
    - Click **View list** to open a screen that displays details for the users included in the report.
    - In the **Other Views** section, click **Summary** to view the report without the data broken out into individual distribution lists.
    - In the **Other Reports** field, click ⌄ to select a different report. Click **Run report** to view it.

Create and view an alerts usage summary report

Use Alerts Usage Summary reports to determine how many reports or messages were sent out within a designated amount of time.

The Alert Usage Summary report includes data from the organization you are logged in to. If you are logged in to an enterprise organization, data for each suborganization is also displayed.

If you are a System Administrator, you can log in to the System Setup (3) organization to view an alerts usage summary report with data for all organizations in the system.

1. In the navigation bar, click **Reports** > **Alerts Usage**. The Alert Usage Summary Report screen opens, displaying by default the Total Number of Alerts Over Time report generated with a default time range.
2. Optionally, click **Report Type** to create the Total Number of Messages Sent Over Time report.
3. Click 📅 to set the start and end dates for data to be included in the report.

   Note: The date range must be between 1 and 12 months.
4. Optionally, if you want the report to include or exclude specific alert headers, select either **contains** or **does not contain** in the **Alert Header** field and then enter a word or phrase in the text entry field at the end of that row.
5. Click **Generate Report**.

The report appears at the bottom of the screen, replacing the previous report.

View a summary of all organizations

Note: If you are an authorized user, you can click the User Summary link on the Settings screen to view, download, or print a summary of the number of enabled users in each organization.

1. In the navigation bar, click **Reports** > **User Summary**.

   The **End User Summary** screen opens, displaying a list of each organization you have permissions to view, the number of enabled users in each system, and the total number of enabled users in all systems.
2. Optionally, do any of the following:

   - If the report has more than one page, click › to go to the next page or ›| to go to the last page.
   - To export the report, click **Export to the selected format**, make a selection, then click **Export**.
   - To refresh the page , click 🔄.
   - To print the list, click 🖨.

Export and print reports

BlackBerry AtHoc gives you the ability to print or export any generated report to an external location. Depending on the type of report that is generated, you might be able to export a report in any of the following formats:

- **CSV**: Available for all report types.
- **Excel**: Available for all report types.
- **Acrobat PDF**: Available for alert usage summary reports.
- **Rich Text Format (RTF)**: Available for alert usage summary reports.
- **TIFF**: Available for alert usage summary reports.
- **Web Archive**: Available for alert usage summary reports.

Export a personnel report

1. In the navigation bar, click **Reports Personnel Reports**.
2. Follow the instructions in Run and View Personnel Reports to create the report you want to export.
3. In the report, from the **Export to the selected format** list, select a file type.
4. Click **Export**.
5. On the **Export** window, choose to download the report or open it directly.

Export an alerts usage summary report

1. In the navigation bar, click **Reports** > **Alerts Usage**.

   The Alert Usage Summary Report screen opens, displaying the Total Number of Alerts Over Time report generated with a default time range.
2. Optionally, follow the instructions in Create and view an alerts usage summary report to customize the report to a specific timeframe or report type.
3. In a report that you generated, or the default report, in the **Export to the selected format** field click ⌄.
4. Select the type of file to download.
5. Click **Export**.

Print a personnel report

1. In the navigation bar, click **Reports** > **Personnel Reports**.
2. Follow the instructions in Run and view personnel reports to create the report that you want to print.
3. When the report is generated and appears on the screen, click **Print**.
4. Follow the instructions on the screen to print the report.

Print an alerts usage summary report

1. In the navigation bar, click **Reports** > **Alerts Usage**.

   The Alert Usage Summary Report screen opens, displaying by default the Total Number of Alerts Over Time report generated with a default time range.

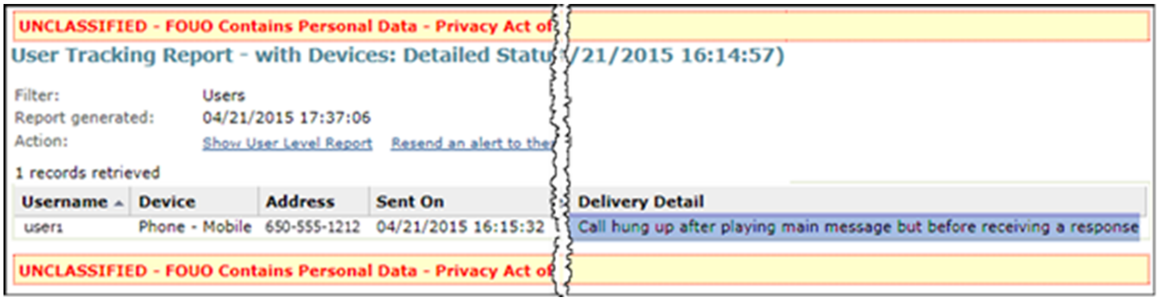
2. Optionally, follow the instructions in Create and view an alerts usage summary report to customize the report to a specific timeframe or report type before you print it.
3. When the report is generated and appears on the screen, click 🖨.
4. Follow the instructions on the screen to print the report.

Unified telephony tracking codes

BlackBerry AtHoc uses unified tracking codes to track the progress of alerts that are sent to telephony devices, such as mobile phones and work phones. Each call has a code assigned to it. The code then maps to a status message for the call.

View reports with the codes and messages

The status message for a call appears in the Device Delivery report for a sent alert.



UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of

User Tracking Report - with Devices: Detailed Statu /21/2015 16:14:57)

Filter: Users
Report generated: 04/21/2015 17:37:06
Action: Show User Level Report Resend an alert to the

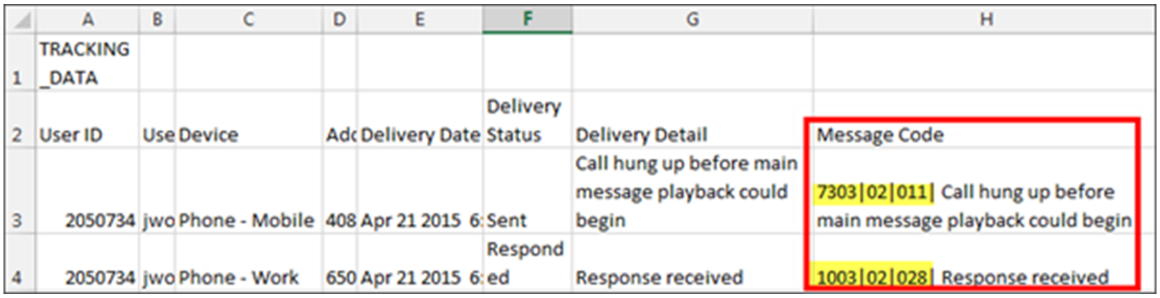
1 records retrieved

Username	Device	Address	Sent On	Delivery Detail
user1	Phone - Mobile	650-555-1212	04/21/2015 16:15:32	Call hung up after playing main message but before receiving a response

UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of

The code and mapped message appear in the full tracking report. Export the full report to view these codes.

1. Send an alert.
2. Click **Alert Summary** from the completed alert or double-click to open the alert from the **Sent Alerts** screen.
3. On the **Alert Summary** screen, click **Advanced Reports**.
4. Hover over the **Export** link in the top corner of the report and then select **Export Full Report** from the drop-down list.
5. The report is exported to a .csv file. You can see the status and duration of each call.

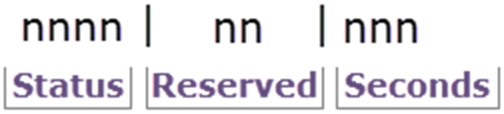


	A	B	C	D	E	F	G	H
1	TRACKING _DATA							
2	User ID	Use	Device	Adc	Delivery Date	Delivery Status	Delivery Detail	Message Code
3	2050734	jwo	Phone - Mobile	408	Apr 21 2015 6:	Sent	Call hung up before main message playback could begin	7303|02|011| Call hung up before main message playback could begin
4	2050734	jwo	Phone - Work	650	Apr 21 2015 6:	Respond ed	Response received	1003|02|028| Response received

In the example above, the mobile and work phones of the user were targeted. The user listened to the alert and responded to the call from his or her work phone. When the user heard the start of the alert on their mobile phone, they hung up before listening to the main message because they had already responded to it using their work phone.

Code format and message descriptions

The unified code has the following format:



Status: A 4-digit number indicating the success or failure of the call or voice mail.

- 1XXX: Success
- 7XXX: Incomplete
- 9XXX: System Error

Reserved: For BlackBerry AtHoc use.

Seconds: The number of seconds the call lasted. The number “022” means the call took 22 seconds from pick up to hang up.

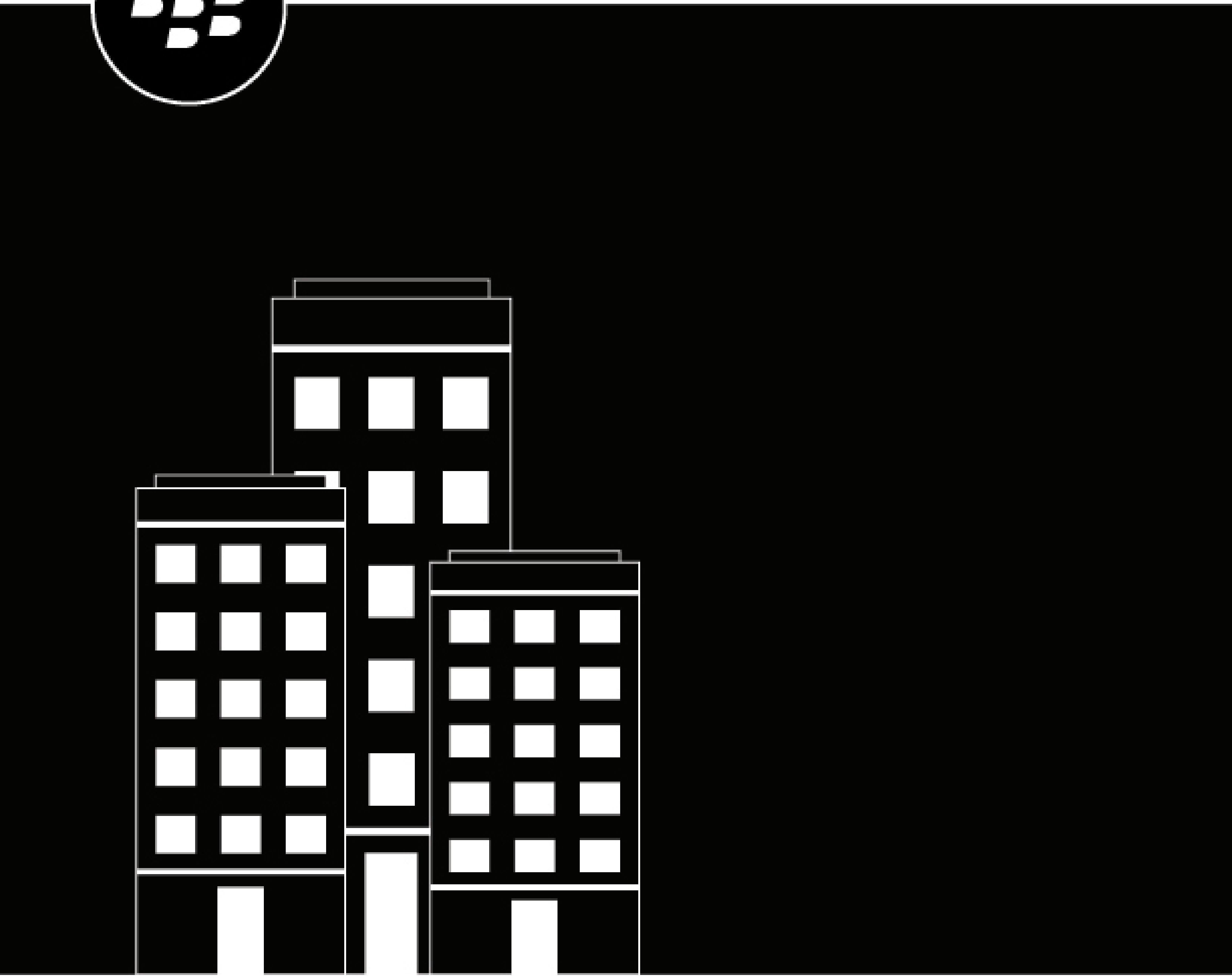
For example, the following code means that the voice mail was delivered successfully and it took 27 seconds:

```
1002|03|027
```

The following table lists each of the status codes:

Status	Description
1001	Call completed successfully
1002	Voice mail delivered successfully
1003, 1004	Response received
7001-7050	Cannot process call based on configuration
7037	Call flow has no ID
7051	The target user has no PIN defined for retrieving secure messages
7052	No callback number has been defined to use when leaving voice mail
7053	Phone number has an invalid format
7200-7102	Failed to prepare call for sending
7230-7235, 7240	Failed to make call
7250	Provider timeout received
7251	Failed to connect call (voice error)
7252	Failed to connect call (voice error.) Error might be temporary. Retry later.
7253	Failed to connect call (voice error.) Do not retry.

Status	Description
7254	Failed to connect because of a voice error message, such as “Your call cannot be completed at this time.”
7257	Failed to dial number
7258	No answer received
7259	Line was busy
7261	Failed to connect call
7301	Call hung up before playback could begin
7302	Call dropped before playback could begin
7303	Call hung up before main message playback could begin
7304	Call dropped before main message playback could begin
7305	Call hung up in middle of main message playback
7306	Call dropped middle of main message playback
7314	Voice mail delivered successfully
7315	Failed to leave voice mail
7316	Voice mail detected, but not ready after waiting for an excessive time period
7317	Voice mail dropped in middle of message playback
7318	Voice mail dropped in middle of message playback
7319	Voice mail ready, but leaving voice mail is not a call option
7401	Call hung up after playing main message but before receiving a response
7402	Call dropped after playing main message but before receiving a response
7411	Call terminated after waiting too long for a response
7412	Call terminated after too many invalid key presses
9001-9090	Failed to send message to TAS



BlackBerry AtHoc

External Events

7.16

Contents

What are external events?

BlackBerry® AtHoc® improves emergency managers' situational awareness by providing alerts for external events that impact their organization and employees. External event categories include Earthquake, Fire, Hurricane, and Flood. To see the full list of supported external event types, see Supported external event types.

BlackBerry AtHoc monitors external feeds and creates events that appear in the Inbox and on the live map. System Administrators can enable the External Events feature in **Settings** > **Feature Enablement** in the BlackBerry AtHoc management system. For more information, see Enable external events.

When external events are enabled, operators can select the locations and external events they want to monitor. When an event occurs that impacts a selected location, it appears in the Inbox in the BlackBerry AtHoc management system and on the live map. Operators can also receive notifications on their chosen devices (email, SMS, and mobile app) when events that impact their selected locations appear in the Inbox. These notification events include a link to the event in the Inbox. In addition, when an external layer is enabled, the notification includes a link to the live map. For more information, see Set up external events for your organization.

External events that appear in the Inbox and on the live map include the event title, description, event start time, expiration time, severity, map, and feed source (name and URL.) External events include the event geolocation and the number of impacted users. Click the **View the Live Map...** link in the event details to open the live map. The live map opens with the triggering event type selected in the External Layers panel. After evaluating the external event and its impact, the operator can forward the event as an alert to impacted employees.

Enable external events

External Events settings do not appear on the Settings page in the BlackBerry AtHoc management system until the External Events feature is enabled.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Feature Enablement**.
4. On the **Feature Enablement** screen, click **IsExternalEventSupported**.
5. On the **Edit Feature Enablement** dialog, select **True** from the **Enabled** pull-down menu.
6. Click **Save**.

Set up external events for your organization

When external events are enabled, Organization Administrators can define the locations and external events they want to monitor. When an external event occurs that impacts a selected location, it appears in the Inbox in the BlackBerry AtHoc management system and on the live map. Operators can also receive notifications on their chosen devices (email, SMS, and mobile app) when events that impact their selected locations appear in the Inbox.

Before you begin:

- IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement**.

1. In the navigation bar, click ⚙.
2. In the **Basic** section, click **External Events**.
3. On the **External Events** screen, in the **Your Organizational Area** section, click ✎.
4. On the map, do any of the following:

    - Click **Create Custom Locations**, and then select a shape. Click and drag on the map to draw a shape.
    - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

    You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
5. Click **Apply**.
6. In the **External Event Types** section, select the types of external events to receive in the Inbox.
7. Optionally, in the **Setup Admin Notifications** section, click **Select Targets**.
8. On the **Users** dialog, select the operators to notify when an external event occurs in the selected organizational areas. All external events that impact the organizational area appear in the Inbox in the BlackBerry AtHoc management system. The operators you select will receive an alert about the event on the selected devices.
9. Click **Apply**.
10. From the **Devices** pull-down menu, select the devices (email, SMS, and mobile app) that the targeted operators will receive notifications on. You can select more than one device.
11. From the **Frequency** pull-down menu, select the interval to send the event notifications at. Choose **24 Hrs** or **48 Hrs**. One notification is sent for each event category. For example, Earthquake.
12. Click **Save**.

Forward an external event as an alert

You can forward external events from the Inbox in the BlackBerry AtHoc management system to users in the targeted event location.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Alerts** > **Inbox**.

   Tip: External events are marked with **Feed Service** in the Inbox.
3. In the left pane, select the external event you want to forward as an alert.
4. Review the details of the external event alert in the details pane.
5. Click **Forward Alert**. The following feed content is mapped to the forwarded alert: Severity, Title, Body, and Map. The Type is always Other.
6. On the **Forward Alert** page, review the alert details and make changes as needed.
7. In the **Target Users** section, click **By Advanced Query**. By default, if the forwarded alert has a selected location, all users in that location and users with a Last Known Location updated in the past 4 hours are targeted.
8. Optionally, enter a number and select **Hour(s)**, **Minute(s)**, or **Day(s)** to change the timeframe for targeting users with a Last Known Location attribute.
9. Click **Select Personal Devices**, and select the personal devices to use to contact the targeted users.
10. Click **Review and Publish**.
11. On the **Review and Publish** screen, review the details of the alert.
12. Optionally, click **Preview and Publish** to preview how the forwarded alert will appear to end users.
13. Click **Publish**.

View external layers on the live map

External layers are layers from public sources such as FEMA, weather maps, or ArcGIS.

The External Layers section in the External Layers panel on the live map displays the external layers that are configured in Map Settings. For more information, see External layers.

Note: The data displayed for external layers are obtained from external sources. BlackBerry AtHoc does not modify or validate this data. If a selected external layer has no data from the external feed, no icons or shapes appear on the live map.

1. Log in to the BlackBerry AtHoc management system.
2. Click **View Live Map**. The live map opens in a new browser tab.
3. Click ▣ in the top navigation bar to open the External Layers panel.
4. On the **External Layers** panel, click ⌄ to expand the **External Layers** section.
5. Select the check box beside a layer to display it on the map.
6. Optionally, click ▾ > ◒ **Transparency** to open the Layer Transparency slider and change the transparency of the layer.
7. Optionally, click ▾ > 🗀 **Source** to view the feed source. For KML layer types, a feed source file downloads to your computer. For other types of feeds, the feed source opens in a new tab on your browser.
8. Optionally, in the middle pane, click ≡ to display a legend that provides graphical information about the layer. The displayed legend information is obtained from the source of the layer. If a layer has no legend information, clicking the ≡ opens the Legend panel, but no data is displayed. You can display multiple legends. If multiple legends are selected, click ●○○ to switch between them on the Legend panel. Click « to close the Legend panel. Legends are supported only for Feature and Image layer types. KML type layers do not support displaying a legend.
9. Optionally, click the name of a selected external layer to zoom the map to display it.
10. Optionally, click the icon or shape for an external layer item on the map to open a details pop-up.
11. Optionally, on an external layer shape details pop-up, click **Zoom to** to move the map focus to the external layer shape location.
12. Optionally, click ◫ to dock the external layer shape pop-up to the right side of the map.

View external events on the live map

The External Events section of the External Layers panel on the live map displays the external events that are configured in the External Events settings. For more information, see Set up external events for your organization.

Note: IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement** for external events to be visible on the live map.

1. Log in to the BlackBerry AtHoc management system.
2. Click **View Live Map**. The live map opens in a new browser tab.
3. Click ◈ in the top navigation bar to open the External Layers panel.
4. On the **External Layers** panel, click ⌄ to expand the **External Events** section.
5. In the **Event Types** section, select the event types to display from the pull-down list.
6. Optionally, in the **Time Filter** section, from the pull-down list, select the time period to display on the map. You can select from 30 minutes to 72 hours. The default is 2 hours. External events that occur in the selected time period are displayed under the Time Filter pull-down list and appear on the map. The severity and the time elapsed since the event occurred are displayed.
7. Optionally, in the **External Events** section, do any of the following:

   - Click an external event to highlight it in the panel. The shape associated with the event is highlighted on the map.
   - Click 👁 to hide an event on the map.
   - Click ⊘ to display a hidden event.
   - Click 🔍 to zoom the map to an event.
   - Select or deselect the **Show All** option to display or hide all events on the map. All events are displayed on the map by default.
8. Optionally, click an event on the map to display a pop-up with details about the event. The details pop-up includes the following information about the event:

   - Title
   - Source
   - Severity
   - Event Type
   - The date and time the event was published.
   - Description. This description is from the original feed source and is not modified by BlackBerry AtHoc.
   - The number of users who are impacted by the event, based on their geolocation.
9. Optionally, click ▣ to dock the external event pop-up to the right side of the map.

External events data are refreshed on the live map every 5 minutes. Click ↻ to refresh external events data manually.

Supported external event types

The following external event types are supported:

Earthquake

- Earthquake

Fire

- Extreme Fire Danger
- Fire Warning
- Fire Weather Watch
- Red Flag Warning
- Wildfire

Flood

- Flash Flood
- Flood Advisory
- Flood Statement
- Flood Warning
- Flood Watch

Freeze

- Amber Warning Ice
- Amber Warning Snow
- Blizzard Warning
- Freeze Warning
- Freeze Watch
- Freezing Fog Advisory
- Frost Advisory
- Heavy Freezing Spray Warning
- Red Warning Ice
- Red Warning Snow
- Snow Squall Warning
- Winter Storm Watch
- Winter Weather Advisory
- Yellow Warning Ice
- Yellow Warning Snow

Heat

- Amber Warning Extreme Heat
- Excessive Heat Warning
- Excessive Heat Watch
- Heat Advisory
- Red Warning Extreme Heat
- Yellow Warning Extreme Heat

Hurricane

- Hurricane Force Wind Warning
- Hurricane Warning

- Hurricane Watch

Storm

- Amber Warning Lightning
- Amber Warning Rain
- Amber Warning Thunderstorms
- Red Warning Lightning
- Red Warning Rain
- Severe Thunderstorm Watch
- Severe Weather Warning
- Snow Squall Warning
- Storm Surge Warning
- Storm Surge Watch
- Storm Warning
- Storm Watch
- Tornado Warning
- Tornado Watch
- Tropical Cyclone Statement
- Tropical Storm Warning
- Tropical Storm Watch
- Winter Weather Advisory
- Yellow Warning Lightning
- Yellow Warning Rain
- Yellow Warning Thunderstorms

Wind

- Amber Warning Wind
- Gale Warning
- Gale Watch
- High Wind Warning
- High Wind Watch
- Red Warning Rain
- Wind Advisory
- Wind Chill Advisory
- Wind Chill Warning
- Wind Chill Watch
- Yellow Warning Wind

Request a new external event type

If the external event type you need is not listed on the External Events settings page, you can submit a request to add it. Go to the BlackBerry AtHoc support portal at: https://www.blackberry.com/us/en/support/enterpriseapps/athoc/support-request.

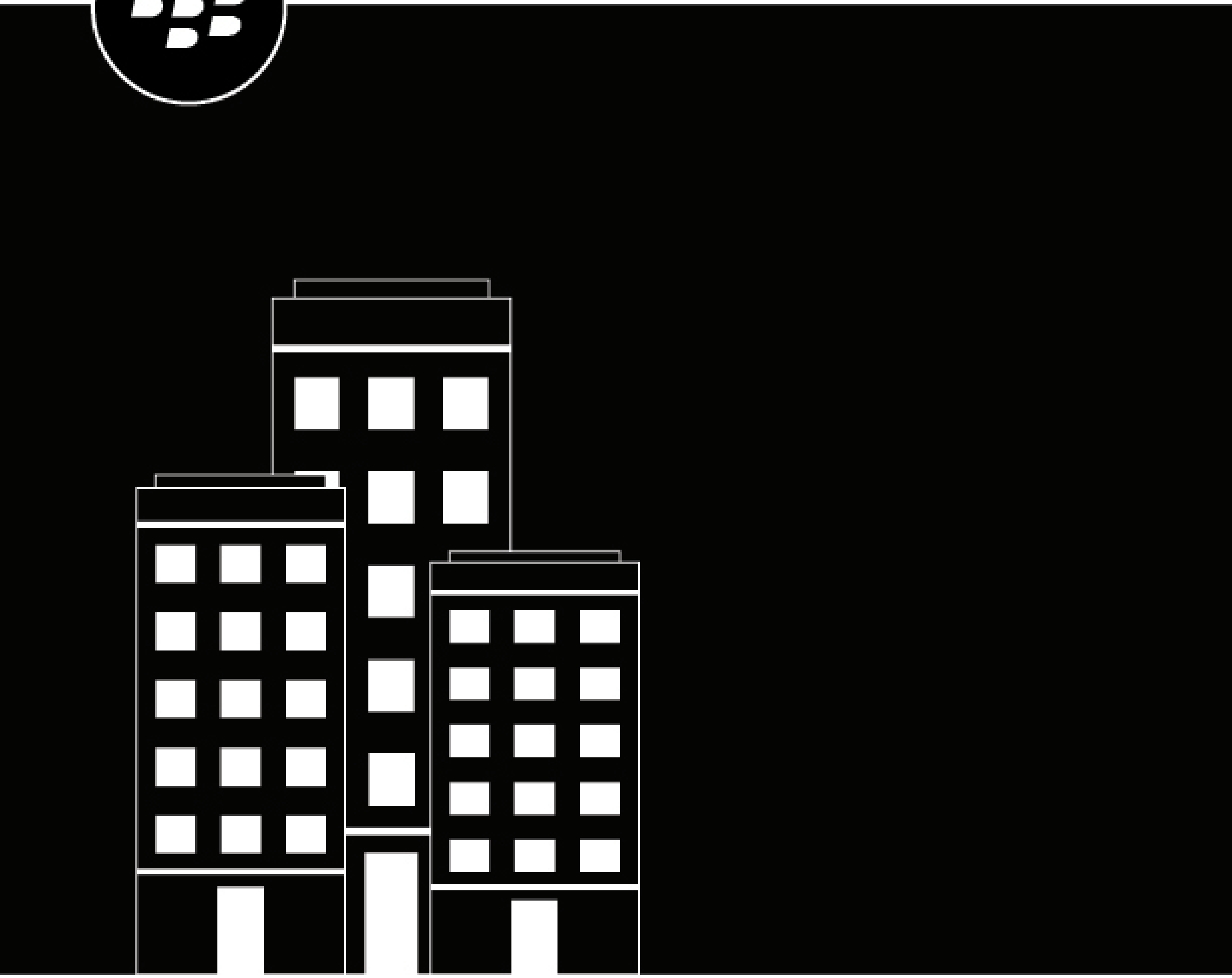
RSS, Geo-JSON, CAP, and ATOM formats are supported.

The requested feed should:

- Include geolocation information for events. For example, earthquakes in San Jose, California, or winter storms in Toronto, Canada.
- Provide consistent location data and event type information.
- Be applicable to a regional (for example U.S. West Coast), national, or international area.

Include the following information in the support request form:

- Event Type keyword. For example, Weather, Fire, Geological, Protest, civil unrest, or bomb threat.
- Region. For example, United States (Country), UK, or Global.
- Feed source URL. For example, https://tools.cdc.gov/api/v2/resources/media/404952.rss
- Customer details, including name and contact information.
- Justification for the use case.



BlackBerry AtHoc

SMS Opt-In

7.16

Contents

What is SMS Opt-In?

SMS Opt-In enables operators to allow community members, visitors, event participants, or other users outside of their organization to subscribe to receive alerts by SMS. These outside users can subscribe to receive alerts by sending a text event code via SMS.

Organization Administrators create event codes, and then share the event code and the short code with users. When a user opts-in by sending an SMS with the event code, they are added to the BlackBerry® AtHoc® management system. Administrators can then target them in alerts.

Activate SMS Opt-In

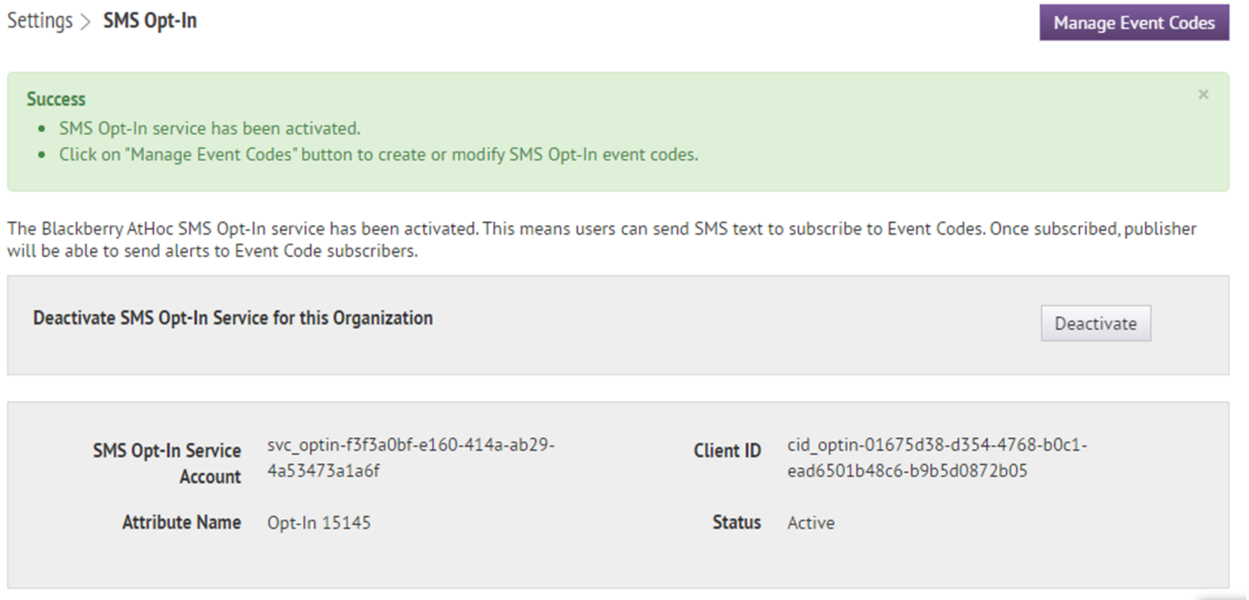
Before you begin:

- You must be an Organization Administrator, Enterprise Administrator, or System Administrator to enable and activate SMS Opt-In.
- SMS Opt-In is disabled by default. To enable it, log in as a System Administrator and go to **Settings** > **System Setup** > **Feature Enablement** and set the IsSMSOptInEnabled feature to True.

Entries are added to the operator audit log when SMS Opt-in is enabled or disabled.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **Users** section, click **SMS Opt-In**.
4. On the **SMS Opt-In** page, click **Activate**.

- A success message and details about the SMS Opt-In service are displayed on the **SMS Opt-In** page.
- A multi-select picklist attribute is automatically created that can be used to target users in alerts.



Success

- SMS Opt-In service has been activated.
- Click on "Manage Event Codes" button to create or modify SMS Opt-In event codes.

The Blackberry AtHoc SMS Opt-In service has been activated. This means users can send SMS text to subscribe to Event Codes. Once subscribed, publisher will be able to send alerts to Event Code subscribers.

Deactivate SMS Opt-In Service for this Organization

SMS Opt-In Service Account	svc_optin-f3f3a0bf-e160-414a-ab29-4a53473a1a6f	Client ID	cid_optin-01675d38-d354-4768-b0c1-ead6501b48c6-b9b5d0872b05
Attribute Name	Opt-In 15145	Status	Active

Make the Opt-In user attribute available for targeting and user management

When you enable SMS Opt-In, an Opt-In user attribute is automatically created. In order to target users in alerts and events using this SMS opt-in user attribute, you must make it available for targeting.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, in the **Layouts** section, click **View/Edit** beside **Targeting Settings** .
5. On the **Group Targeting Definition** window, in the **Available Fields** column, click the **Opt-In** *<opt-in-number>* attribute.
6. Click **Add**.
7. Optionally, use the control buttons on the right to move the Opt-In attribute higher or lower in the **Selected Fields** list.
8. Click **Save**.
9. On the **General Settings** screen, click **Save**.
10. In the navigation bar, click **Users** > **User Attributes**.
11. On the **User Attributes** screen, click the **Opt-In** *<opt-in-number>* attribute.
12. On the user attribute details page, in the **Page Layout** section, select a value from the **User Details - Full Page** pull-down menu. Do not leave this option set to **Do Not show**.
13. Click **Save**.

Create an event code

Create an event code so that you can target users outside your organization with SMS alerts.

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event Codes**.
4. On the **Manage Event Codes** page that opens in a new tab on your browser, click **New**.
5. On the **Create New Event code** window, enter an event code name. Spaces and the following characters are not allowed: `` ` ``!$%&^()={},;\:?"<>|\
6. In the **Event Code** field, enter an event code. This is the code that you will provide to your end users. They send this event code in an SMS to subscribe to alerts.
7. Optionally, in the **Expiration** field, select a date for the event code to expire. When an event code expires, users can no longer use the event code.
8. Click **Save**.

After you finish: When you promote your event code, include the following text: `Text [event-code] to [sms-number]`. If you do not know the SMS number, see SMS numbers for U.S. hosted systems and SMS numbers for European hosted systems.

SMS numbers for U.S. hosted systems

Country	Primary SMS number	Backup SMS number
Canada	73101	73102
Japan	81502	80447
New Zealand	2316	2575
United Arab Emirates	3775	6991
United States	28462	73101

SMS numbers for European hosted systems

Country	Primary SMS number	Backup SMS number
Canada	555666	333666
Croatia	815517	815518
Japan	85136	80447
New Zealand	4840	8434

Country	Primary SMS number	Backup SMS number
United Arab Emirates	1727	2496
United Kingdom	65165	65465
United States	333666	444666

Edit an event code

Event codes can be edited until they expire. Event codes cannot be deleted.

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event codes**.
4. Optionally, on the **Manage Event Codes** window, enter an event code in the **Search** field and click 🔍 to narrow the list of event codes.
5. On the **Manage Event Codes** window, click ✎ on the row for the event code you want to edit.
6. Optionally, update the **Event Description**, **Event Code**, and **Expiration** fields.
7. Click **Save**.

Deactivate SMS Opt-In

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. Click **Deactivate**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada