BlackBerry AtHoc

Manage Users

7.15

Contents

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 Manage Operators and Administrators 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 Manage Operators and Administrators 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 the sponsor or sponsors have dependents, those dependents 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 Operators and Administrators 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 Operators and Administrators 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 User 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 next to the usernames you want to export.
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. Optionally, in the **Advanced** section, select **Include all Dependents of selected Sponsors** to export dependent users.
7. 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

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 for users 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	is	Yes	• Currently Online is Yes • CPR Certified is No
Date	equals, not equals, before, after	Date Panel (showing date value + Past & Next x days value)	• Joining Date equals 5/4/201 • CPR Expiration Date older than Sysdate - 30 days
Date	is empty, is not empty	Hide	• Expiration Date is empty
Date Time	before, after	Date Time Panel (showing date value + Past & Next x days value)	• Age is empty • Age is not empty
Date Time	is empty, is not empty	Hide	--
Geolocation	is inside, is outside	Map screen to show selections	• Home Location is inside shape on the map
Geolocation	is empty, is not empty	Hide	• Office Location is empty
Memo	—	—	—
Multi-select Picklist	equals, not equals, is empty, is not empty	Multi-value selection options	• • Emergency Community not equals Fire • Rank equals Commander, Captain

Attribute Type	Operator	Value	Examples
Number	equals, not equals, greater than, less than	Whole number without decimals	• Age equals 30 • Age greater than 18 • Age less than 65
Number	is empty, is not empty	Hide	• Age is empty • Age is not empty
Single-select Picklist	equals, not equals, is empty, is not empty	Single-value selection option	• Building is not empty
Status	equals, not equals, is empty, is not empty	—	—
Text(String)	equals, not equals, starts with, ends with, contains, does not contain	Alphanumeric text	• First Name equals John • First Name starts with A • First Name contains andy
Text(String)	is empty, is not empty	Hide	• First name is empty
Org Hierarchy	at, at or below, not at, not at or below	Multiselection of node in hierarchy	<Node name or names>

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 link below the search field and then select from the following options to filter search results by type.

- **Enabled Users**: Search results include enabled users only, excluding disabled users.
- **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.

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 new column to view all of the available user details 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

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 would not require the selection of users from the search results.

Sort search results

To sort search results, click once in any of the column headers to sort the results based on the data in the selected column. After you click the column header, a small ^ (**Up**) or v (**Down**) icon appears next to 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.

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 (Enabled, Operator), 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  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 dependents

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Users** > **Users**.
3. On the **Users** screen, search or scroll down to find the sponsor user whose dependents you want to view.
4. Click the row with the sponsor user's name.
5. On the user details screen, click **More Actions** > **View Dependents**. The Dependents screen opens.
6. Optionally, enter a name in the **Search by name** field to find a specific dependent.
7. Click the row for a dependent to view the dependent user's account details.

Edit or delete a dependent

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 to find the sponsor whose dependents you want to edit or delete.
4. Click the row with the sponsor user's name.
5. On the user details screen, click **More Actions** > **View Dependents**. The Dependents screen opens.
6. Optionally, enter a name in the **Search by name** field to find a specific dependent.
7. Click the row for a dependent.

8. On the **Edit Dependent** screen, edit the basic user information, contact information, or password as needed.
9. 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 you want to delete.
10. Optionally, click **Delete** to delete the dependent. Click **Delete** on the confirmation window that appears.
11. Click **Save**.

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 User 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.

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 Enterprise Planning and Management Guide*.

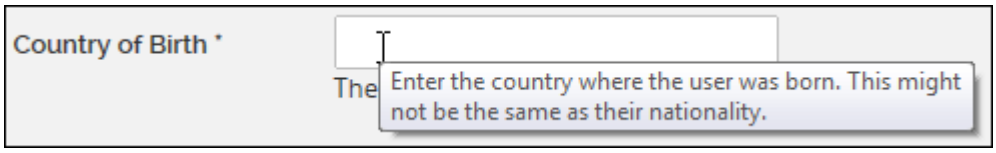
1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Attributes**.
3. On the **User Attributes** screen, click **New** and select one of the following attribute types:
   - Checkbox
   - Date
   - Date Time
   - Geolocation
   - Memo
   - Multi-select Picklist
   - Number
   - Single-select Picklist
   - Status
   - Text

The New Attribute screen displays all of 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.



6. Optionally, in the **Help Text** field, enter text that will appear under the field.

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 the user profile.
10. Optionally, select **Use as a Response Option**.

    Note: Only Single-select Picklist, Status, and Checkbox 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 that you selected, one of the following fields appears:

    - **Length**: For text attribute types, enter the minimum and maximum number of characters that end users must enter in the attribute field.
    - **Minimum Value** (number)/**Maximum Value** (number): Set the range for the field by entering the minimum and maximum number a user can enter.
    - **Minimum Value** (date)/**Maximum Value** (date): Set the date range for the field by entering the first and last dates it covers.
    - **Minimum Value** (date/time)/**Maximum Value** (date/time): Set the date-range and time-range for the field by entering the first and last dates and times it covers.
    - **Picklist values**: For single and multi-select picklist types, enter each of the values that a user can select in the attribute field. Specify the order the values appear in the list in.

      The sort order is the same anywhere the attribute is displayed. This is also the order users will be sorted when sending an alert that contains escalation rules.

      Note: User attributes that have a data type of single-select picklist appear in the Response Options list in the alert's Content section.
    - **Selected by Default**: For Checkbox type attributes, select Yes in this field if you want the attribute to be selected by default whenever it appears.
    - **Map Icon**: For Geolocation type attributes, you can select the icon that you want to display on maps to represent the attribute. Select the **Save Location History** option to track where the icon is located on the map over time.

12. Optionally, complete the **Page Layout** section:

    a. Select the pages and sections where you want the user attribute to appear.

b. 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, complete the **Personnel Reports** section:

a. For the following attribute types, select **Available for reporting**.

- Single and multi-select picklist
- Checkbox (Yes/No)

You can create a personnel report based on the attribute and its values.

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**, 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 Enterprise Planning and Management* 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.

Attributes with custom translations cannot be deleted. Before attempting to delete an attribute, verify that no custom translations are associated with it. Go to > **Translate Custom Attributes**. On the **Custom Attributes Translation** page, select the attribute from the pull-down list. Remove any text that appears in any **Attribute Name** or **Attribute Tooltip** field and then click **Save**. Text that is part of the system's primary language appears greyed out and cannot be deleted. This text does not prevent the attribute from being deleted.

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
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.

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 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 Administrator 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 Customer Support Portal

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

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

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

Documentation feedback

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

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

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

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada