



BlackBerry AtHoc

Manage Users Guide

7.9

Contents

- Manage users..... 5**

- Create a user..... 6**
 - Create dependents for a user..... 7

- Import users from a file..... 8**
 - Import dependent users..... 9
 - Format a user import file..... 10
 - Stop the import users process..... 11
 - Undo the import users process..... 12
 - Troubleshooting tips for user import..... 12

- Export users to a file..... 14**

- Search for users..... 15**
 - Search engine overview..... 15
 - Run a basic search for a user..... 15
 - Include groups as search criteria..... 16
 - Run an advanced search for a user..... 16
 - Advanced search attribute types..... 17
 - Filter search results by user type..... 18
 - Customize search results columns..... 18
 - Select search results..... 18
 - Sort search results..... 19
 - Reset the search field..... 19

- View user details..... 20**

- View user activity..... 21**
 - Export user activity details..... 21

- View dependents..... 22**

- Edit user details..... 23**

- Make mass changes to user details..... 24**
 - Export the user details..... 24

Modify the export file.....	24
Import the modified user details.....	24
Enable users.....	25
Disable users.....	26
Delete users.....	27
Edit or delete a dependent.....	28
Managing organization subscriptions.....	29
Subscribe users to organizations.....	29
Subscribe a single user.....	29
Subscribe multiple users.....	30
View subscribed users.....	30
Manage user settings.....	31
Manage user attributes.....	31
View a list of user attributes.....	31
Create a user attribute.....	31
Edit a user attribute.....	33
Delete a user attribute.....	33
Automatically disable users based on attributes.....	34
Automatically delete users based on attributes.....	34
Configure an Organization Hierarchy attribute.....	35
Manage advanced settings for operators.....	35
Manage user authentication.....	36
Enable authentication methods.....	36
Assigning authentication methods to applications.....	36
Configure SDK access security.....	38
Enable two-factor authentication.....	38
Enable single sign-on.....	39
BlackBerry AtHoc Customer Support Portal.....	45
Legal notice.....	46

Manage users

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](#)

This document describes how to manage users within 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 detailed information about operator roles and permissions, see the [BlackBerry AtHoc Manage Operators and Administrators Guide](#) or the [BlackBerry AtHoc Roles and Permissions Matrix](#).

Create a user

Note: You must have End User Manager permissions 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**.
2. Click **Users**.
3. At the top of the **Users** screen, click **New**.

Note: Fields marked with an asterisk (*) on the New User screen are required.

4. 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 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, click the forward slash (/) link. On the pop-up screen, navigate to the specific organization the user belongs to. Click **Apply** to add the organization information to their record in the system.
 - Any custom fields added by the administrators, including details such as CPR certification status, Emergency Community membership, or special skills.
 - Enter a work location and (if applicable) temporary work location.
5. In the **Numbers** section, enter the work number, mobile number, pager numbers, and any other numbers that could be used to contact the user.

Note: International numbers and numbers with extensions are supported.

BlackBerry AtHoc then 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.

6. In the **Online Addresses** section, enter work and home email addresses.
7. In the **Physical Addresses** section, enter work and home addresses.
8. In the **Distribution List Membership** section, specify the distribution lists in which the user is a member.

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.

9. In the **Advanced Information** section, which is configurable for each system, complete any required fields plus any of the non-required fields you want to include in the account details for the user.
10. Provide a password that meets the displayed rules, if required.
11. 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.

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 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**. The users screen opens.
3. 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. Repeat Steps 6 to 11 to add additional dependents for the sponsor user.

Import users from a 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. You should make sure 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 the "Importing and Exporting Operators" section 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 non-duplicate users in the .csv file are imported.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Click **More Actions > Import > Users**.
4. Select the **Import** option.
5. If you want to download a blank .csv file to use as a template for your import user file, click the **Download a template CSV file** link. 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.

6. Click **Browse**.
7. Navigate to the location of the import user file on your computer.
8. Open the file to enter or modify the user data.
9. 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 a single 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 (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"
```


10. Optionally, make sure that any geolocation attributes in the .csv file are in the correct "Latitude,Longitude" format. The value for the geolocation must be enclosed in quotes. For example, "37.538226,-122.32726".
11. (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.
12. After you have entered your data, save and close the file.

Note: Microsoft Excel hides some characters from view. If you edit the file in 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 for the above steps, complete steps 13 through 15. Otherwise, skip to Step 16.
13. Optionally, save and close the file.
14. Optionally, 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.
15. Optionally, edit the file name and manually change the extension from .txt to .csv.

The import function requires a .csv file type. This method preserves the formatting in the text file.
16. 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.
17. Optionally, select the **Partial User Import Enabled** check box 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.
18. Select each of the columns of data you want to import or click **Select All**.
19. Review the **Columns that cannot be imported** list to make sure it does not contain important data that you must be able to view within BlackBerry AtHoc. If the list contains important columns of information, contact BlackBerry AtHoc Customer Support for help.
20. Click **Import**. The Importing Users window opens. The import happens in batches of 5000 users.
21. 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 appears, listing the 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 the *BlackBerry AtHoc Operators and Administrators Guide*.

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.

Format a user import file

In order to import a .csv user file, the following formatting standards are required:

Field Name	Description	Is Mandatory?
Username	The Username is a value that can be used to identify a user within 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.	Yes
Status	Use the Status column to enable, disable, or delete a user. The following attribute values can be used: <ul style="list-style-type: none"> • Enabled—Enable the user • Disabled—Disable the user • Deleted—Delete the user <p>The import file must contain a Status column, but the column can be empty. Note that 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.</p>	Yes
HRCHY: Hierarchy Name	Use the prefix "HRCHY:" to specify the location in your User Base Hierarchy where the user is a member. You can view your organizational hierarchy by going to Users > Users and clicking on  .	No

Field Name	Description	Is Mandatory?
SDL: Static Distribution List Name	Use the prefix "SDL:" to specify the name of the static distribution list to which users will be added. You can view your distribution list hierarchy by going to Users > Users and clicking on  . 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, this option can be used 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 user attribute as column heading to update user attribute value.	No
Device: Device Name	Use prefix "Device:" for specifying any device name in the import file. For pager addresses, specify 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 <i>BlackBerry AtHoc Create and Publish Alerts</i> 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

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 and 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.

The Stop Import button stops the import, but does not undo it. Records that have already been added are not removed and records that have been updated are not restored to previous values. To download a .csv file that contains information about the users that were imported before the import was stopped, on the **Import Details: Stopped** window, click **Download Log**.

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 a single 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 (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 "Latitude,Longitude" format. The value for the geolocation must be enclosed in quotes. For example, "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.
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.

Export users to a file

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check boxes next to the usernames you want to export.
4. Click **More Actions > Export > Users**.
5. On the **Export Users** window, 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.

6. Optionally, use the **Move Up** and **Move Down** buttons next to the **Selected Columns** field to change the order in which the information appears in the export file.

Note: At any time during this process, you can reset the Selected Columns field to its default values by clicking the **Reset to columns displayed in User List** link that appears at the bottom of the field.

7. Optionally, in the **Advanced** section, select **Include all Dependents of selected Sponsors** to export dependent users.
8. When you are finished selecting columns, click **Export PDF** or **Export CSV**.

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.

Search for users

This section describes how to search for users.

Search engine overview

By default, the Users search engine uses a Boolean AND operator between search criteria that appear in the search field. All search results will contain both criteria. For example, entering `max ssa` returns all users containing `max` and `ssa`.

To use a Boolean OR operator, separate the search criteria by a comma in the search field. For example, entering `max, ssa` returns all users containing `max` or `ssa` or both.

In addition, each criteria pill under the Search field is treated as having an AND relationship to other criteria. As a result, if you have two existing pills, `Madhu` and `mnye` and then enter the search string `Nye` in the Search field and click the Search icon, all search results will contain `Madhu`, `mnye`, and `Nye` in at least one of the following fields: display name, first name, last name, or username.


However, in Advanced Searches, when multiple attributes are included within the same search criteria, the search engine uses a Boolean AND operator within that criteria. So, for example, if you create an advanced search criteria `Last Name starts with smi` and `First name contains bar`, both of those criteria would need to be satisfied in order for a username to appear in the results list.

Another feature of the search engine is that it matches any set of letters or numbers anywhere in a word or ID. So a search for `man` would return values such as `Manager`, `Germany`, and `John Hilman`, while a search for `134` would return `134506`, `721349`, and `863134`. Note that the search is not case-sensitive, so whether you search for `Man` or `man`, the same results appear on the screen.

Wildcards are not supported in searches.

Run a basic search for a user

Note: Before you run a search, see [Search engine overview](#) for important information on how the search engine works.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Optionally, in the **Search** field, type or paste into the text box all or part of any of the following user-related search criteria: display name, first name, last name, username.
4. Optionally, in the **Search** field, type or paste into the text box all or part of any of the following group-related search criteria: hierarchy node name, distribution list name.
5. Click  to view the results.

The criteria you used so far appear within a pill beneath the Search field. Each time you add new criteria and click the Search button, a new pill appears next to the previous pills under the Search field.

Note: If the search criteria is too long to fit within the pill, the pill will display ellipses.

Each time a new pill is added, the total count of matching results is updated in the field below the Search field.

6. To remove a pill, click the **X** icon in it. The search results update to display all users that match the remaining search criteria.

Include groups as search criteria

The groups button launches the groups dialog, which enables users to include distribution lists, organization hierarchy nodes, or targetable groups as additional search criteria.


Key features of the "Select groups" screen

The following are important features to know about the "Select Groups" screen:

- Most group names display with a check box next to them, which allows you to select the group and all of its sublevels (if any exist) at the same time. If a group contains a Yes or No selection in its sublevel, no check box appears next to its name because you cannot select all values listed in the sublevel. As an example, a group called CPR Certified would have no check box next to it because you are required to select either Yes or No in the sublevel.
- Groups that have sublevels contain a clickable > icon next to their names. Clicking the > icon opens a list of sublevels in the panel next to it.
- Groups that were selected previously display with a dark background.
- If at least one of the subgroups has been selected previously, the group name displays with a lighter background.

Include groups as search criteria

To include groups as criteria in a search, complete the following steps:

1. On the **Search** screen, click .
2. On the **Select Groups** screen, select the group or groups you want to include in the search.
3. After selecting all of the groups, subgroups, distribution lists, and organizational hierarchy nodes you want to include in the search, click **Apply**.

Each of the groups, lists, or nodes you selected then appears as a separate pill beneath the search field.

Run an advanced search for a user

Note: Before running an advanced search, see [Search engine overview](#) for important information on how the search engine works and [Advanced search attribute types](#) for a complete list of user attributes you can use to create advanced searches.

To run an advanced search for a user using user attributes and organizational hierarchies as search criteria, complete the following steps:

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. To view the advanced search fields, click **Advanced**.
4. Click **Select Attribute** and select the first 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 next to the attribute field. Select an operation.
6. After you make an operation selection in Step 5, a third field appears on the screen. Depending on the attribute type selected in Step 3, the third field can be a text-entry field, a drop-down list, a date field, or any of the other field types listed in [Advanced search attribute types](#). Enter or select a value in the field.
7. Optionally, click **Add Condition** to add another attribute condition to the search, then repeat steps 4 through 6.
8. After you have finished adding conditions to the search, click **Apply**.

The search results field displays all users who match all of the attribute conditions you created.

Advanced search attribute types

The following table lists the different attribute types, operators, and values you can use to construct advanced search criteria. 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	<ul style="list-style-type: none"> Currently Online is Yes CPR Certified is No
Number	equals, not equals, great than, less than	Whole number without decimals	<ul style="list-style-type: none"> Age equals 30 Age greater than 18 Age less than 65
Number	is empty, is not empty	Hide	<ul style="list-style-type: none"> Age is empty Age is not empty
Text(String)	equals, not equals, starts with, ends with, contains, does not contain	Alphanumeric text	<ul style="list-style-type: none"> First Name equals John First Name starts with A First Name contains andy
Text(String)	is empty, is not empty	Hide	<ul style="list-style-type: none"> First name is empty
Date	equals, not equals, before, after	Date Panel (showing date value + Past & Next x days value)	<ul style="list-style-type: none"> Joining Date equals 5/4/2011 CPR Expiration Date older than Sysdate - 30 days
Date	is empty, is not empty	Hide	<ul style="list-style-type: none"> Expiration Date is empty
Date Time	before, after	Date Time Panel (showing date value + Past & Next x days value)	<ul style="list-style-type: none"> Created On older than 5/4/2011 Created On later than Sysdate - 90 days
Date Time	is empty, is not empty	Hide	--
Picklist	equals, not equals	Multi-value selection combo box	<ul style="list-style-type: none"> Rank equals Commander, Captain Emergency Community not equals Fire

Attribute Type	Operator	Value	Examples
Picklist	is empty, is not empty	Hide	• Building is not empty
Geo	is inside, is outside	Map screen to show selections	• Home Location is inside shape on the map
Geo	is empty, is not empty	Hide	• Office Location 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

Either before running a search or after generating search results, you can limit the types of users you want to include in the search results. By default the search screen is set to display enabled users in search results.

The following other user combinations are available and can be selected by clicking the users link below the search field and then selecting the option you want on the drop-down list that appears.

- **Enabled Users:** Search results include enabled users only, exclude 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 users individually or all at the same time 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 for the first column.



As soon as the users are selected, you can perform any of the following actions on them using the More Actions drop-down list above the Search field.

- 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. Note that after you click the column header, a small  (**Up**) or  (**Down**) icon appears next to the name, letting you tell at a glance which column the data is being sorted by and which direction the sort is going.

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 this button does not remove any filtering you have set up 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 have End User Manager privileges to view detailed information about users in the system, including contact address, memberships, login information, and location information.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Click the 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
- Distribution list membership
- Permissions
- Login and location
- User activity
- Any user attributes defined by administrators

View user activity

The Activity List screen enables authorized users to view all activities for individual users in the system. Clicking on a specific user activity opens an activity details screen that provides information about the activity and any response the user made.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Click the user name.

The user details screen opens, displaying information for the user in the system.

4. Select **More Actions > View Activities**.
5. Click a specific activity to view more details.

The details of that activity appear to the right of the activities list.

For each activity, the following details are displayed:

- The title of the activity
- The content of the activity
- The date and time the activity was initiated or created.
- The publisher of the activity
- The timeline for the activity, listing all of the devices to which the activity has been sent along with 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**.
2. Click **Users**.
3. Click the user name.
4. Click **More Actions > View Activities**.
5. Choose which activities to export:
 - To export all of the activities, click **Export PDF**.
 - To export a specific activity:
 - a. Click the specific activity that you want to export. The details of that activity appear next to the activities list.
 - b. Click the  in the corner of the activity details field.

View dependents

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click **Users > Users**. The users screen opens.
3. Search or scroll down the users list to find the sponsor user whose dependents you want to view.
4. Click the row with the sponsor user's name. The user details screen opens.
5. 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 dependent user's account details.

Edit user details

The following instructions explain how to make changes to the details of an individual in the system. To make a global change to all users, such as changing the work address of all users to display a new address, see [Make mass changes to user details](#).

Note: You must have End User Manager privileges to edit user details.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Click next to the name of the user whose details you want to edit.
4. Make changes to any of the user fields in the following sections:
 - Basic Information
 - Numbers
 - Online Addresses
 - Physical Addresses
 - Distribution List Membership
 - Login and Location
 - 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.

5. Click **Save**.

Make mass changes to user details

Note: The following instructions explain how to make global changes to details about users in the system. If you want 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**.
2. Click **Users**.
3. If the users already appear in the results table, select the check boxes next to their names. Otherwise, use the **Search** field to locate them, and then select the corresponding check boxes.
4. Click **More Actions > Export > Users**.
5. In the **All Columns** field, select the columns you want to modify outside of the system, and then click **Add >** to move them to the **Selected** field. To include all columns, click **Add All** at the top of the **All Columns** field.
6. When you are finished selecting columns, click **Export CSV**.
7. 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**.
2. Click **Users**.
3. Click **More Actions > Import > Users**.
4. Click **Browse**.
5. Navigate to the location of the file you modified on your computer.
6. Click **Open**.

Enable users

You can enable a user if the following conditions are true:

- You have End User Manager permissions for the organization.
- You have End User Manager permissions for the user. In some cases, the user may be outside of your userbase and appears as read-only.

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. If the **Status** column is not visible in the user list, click **Add** in the header row to add a column.
4. Click the  in the new column heading, and then select **Status**.
5. Select the check box or check boxes next to the user or users whose status you want to change.
6. Click **More Actions**.
7. Select **Enable**.

The user or users are then enabled and the Status column updates for each of the affected users.

Note: If the sponsor or sponsors have dependents, those dependents are also enabled.

Note: If you have selected users that you do not have permission 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 have End Users Manager permissions for the organization.
- The user is in your userbase. Your userbase 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**.
2. Click **Users**.
3. Select the check box or check boxes next to the user or users whose status you want to change from Enabled to Disabled.
4. Click **More Actions**.
5. Select **Disable**. A confirmation dialog appears.
6. Click **Disable**. The user or users are then 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 have End Users Manager permissions for the organization.
- The user is in your userbase. Your userbase may be restricted to exclude the user and the user is hidden from view.

Note: It might be more efficient for you to identify the users you want to delete based on a specific user attribute or set of attributes they have in common. For more information, see [Automatically delete users based on attributes](#).

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check box or check boxes next to the user or users you want to delete.
4. Click **More Actions**.
5. Select **Delete**.

A confirmation screen opens.

6. Click **Delete** to permanently remove the users from the system.

The screen refreshes and the User list no longer displays the user or 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, an advisory 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."

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**. The users screen opens.
3. Search or scroll down the users list to find the sponsor user whose dependents you want to edit or delete.
4. Click the row with the sponsor user's name. The user details screen opens.
5. 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. The Edit Dependent screen opens.
8. Edit the basic user information, contact information, or password as needed.
9. Click **Save**.
10. Optionally, click **Delete** to delete the dependent. Click **Delete** on the confirmation window that appears.

Managing 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 three 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.

Once organization subscriptions are enabled, operators can subscribe users from the BlackBerry AtHoc management console or by using the .csv user import process. Users in suborganizations can subscribe themselves to enabled suborganizations from Self Service. If the organization subscription feature is disabled, any existing subscriptions are cancelled. Administrators or users can cancel their subscriptions at any time, or set an expiration time for the subscription.

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 console 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.

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. Optionally, click  to set an end date for the subscription.
9. Optionally, repeat Steps 5 to 8 to subscribe the user to additional organizations.
10. Click **Save**.

The user can now be targeted in alerts and events from the subscribed organizations.

Subscribe multiple users

You can also use the .csv user import process to delete or modify organization subscriptions for multiple users.

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users > Users**.
3. On the **Users** screen, select the users you want to subscribe to organizations.
4. Click **More Actions > Users > Export**.
5. On the **Export Users** window, in the **All Columns** list, select **Subscribed Organizations**.
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.
10. Save the .csv file.
11. In the BlackBerry AtHoc management system, on the **Users** screen click **More Actions > Users > Import**.
12. Select the .csv file you updated.
13. In the BlackBerry AtHoc management system, click **Back** to return to the Users screen.
14. Click **More Actions > Users > Import**.
15. On the **Import User File** screen, click **Browse** and select the .csv file on your local system.
16. Click **Open**.
17. In the **Select the columns to import** section, select **Subscribed Organizations**.
18. Click **Import**.

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 to the user manager window.

Manage user settings

The following sections describe tools for managing users, whether they are administrators, operators, or end users.


- Create or edit user attributes that are used to filter, sort, or target users.
- Disable or delete users by user attributes, such as by status or last login date; and then specify when users targeted for deleted are actually purged from the system.
- External Operator Permissions provides a way to add an operator from outside an enterprise.
- Organize distribution lists into folders with Distribution List Folders. You can specify the order in which folders are seen in alert publishing.

Manage user attributes

User attributes provide powerful ways to organize, filter, and manage users, and the majority of this section describes how to configure these attributes. 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, and edit user attributes.

View a list of user attributes

1. In the navigation bar, click .
2. In the Users section, click **User Attributes** link.
3. The **User Attributes** screen opens, displaying all user attributes in the system.

For each attribute, the following information is displayed:


- **Name:** The name that is displayed when the attribute appears in lists or on fields within the 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 in which organization the attribute was created.
- **Updated On:** Specifies the date on which the attribute was last modified.

You can sort the by any of the columns.

4. Click on the name of an attribute to view the details.

Create a user attribute

Note: User attributes can be managed at the system, Enterprise, or organizational 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 Guide*.

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 **New** and select a **type** for the attribute.

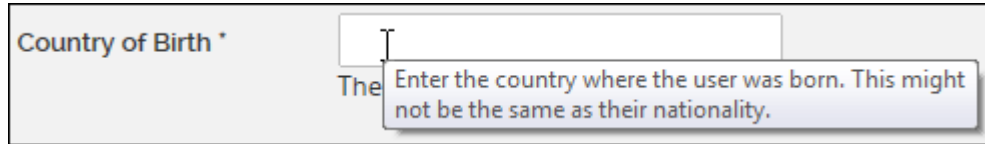
You can select one of the following types: multi-select picklist, single-select picklist, checkbox, text, number, memo, date, date/time, status, or geolocation.

The New Attribute screen displays all of the fields required to create a user attribute.

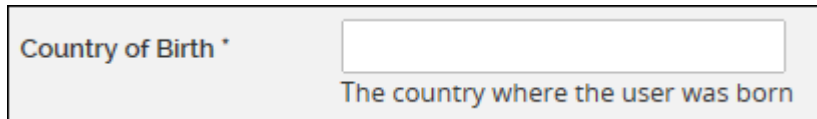
- In the **Name** field, enter the name that will be displayed when the attribute appears in lists or on fields within the system. The attribute name has a 128 character limit.

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.

- Optionally, in the **Tooltip** field, enter a hint that will pop up when users hover their cursor over the attribute field.



- Optionally, in the **Help Text** field, enter text that will appear under the corresponding field within the application.



- Optionally, modify the **Common Name** value.

Note: The value of the Common Name field is by default the same as the Attribute Name value. You can change it, but typically it is not changed. The common name has a 128 character limit.

- Select **Users Can Update** if users need to modify the value.
- Select **Mandatory** if the attribute is a required field in the user profile.
- Complete the **Values** section.

Depending on the attribute type that you selected, one of the following fields appears below the Data Type screen:

- Length:** For text attribute types, enter the minimum and maximum number of characters that end users will have to 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 may 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 will be able to select in the attribute field. Specify the order in which the values appear in the list.

The sort order will be 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. For this option, an additional optional field, called Save History, appears above the Data Type field. Select it if you want to keep track of where the icon is located on the map over time.

- Optionally, complete the **Page Layout** section:

- Select the pages and sections on which you want the user attribute to appear.
- 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.

- 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**.

13. 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: If the list of attributes is extensive, you can filter it by searching by attribute name and further filter it by opting to display only the attributes that are defined within the organization. This will cut out all Enterprise and system attributes that are inherited.

4. Make whatever changes you want on the **Basic, Values, Page Layout, and Personnel Reports** sections.

Note: The **Info** tab 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**.

Delete a user attribute

Note: User attributes use inheritance. To delete the attribute, it must be in the organization from which 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 the "Manage Common Content with Inheritance" section of the *BlackBerry AtHoc Enterprise Planning Guide*.

If a user attribute becomes obsolete, you have the ability to 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 popup box appears, listing all locations where the attribute appears. Removing an attribute in a user query can have unintended consequences, such as changing the target audience of an alert. To avoid these effects, you must remove the attribute from each of the dependencies manually before you can delete the attribute itself.

1. In the navigation bar, click .
2. In the **Users** section, click **User Attributes**.

The **User Attributes** screen opens, displaying all of the attributes available to users in the organization.

3. In the **Attribute Name** column, click the name of the attribute that is defined in the organization.
4. Click **Delete**.
5. On the confirmation screen, click **OK**.

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.


After you click OK, the value is removed from the system and no longer appears in the User Attributes list.

Automatically disable users based on attributes

In organizations where changes to the userbase occur frequently, it is often more efficient to automatically disable users based on one or more user attributes. This helps ensure the userbase 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**. The Disable and Delete Users screen opens.
3. In the **Disable Users** section, click the drop-down list in the **Select Attribute** column and select the first attribute you want to use as a means of identifying users to be disabled.
4. As soon as you make a selection in the **User Attribute** drop-down list, the **Select Operator** drop-down list appears. Select an option from the list.
5. In the field that appears to the right of the **Select Operator** field, enter or select a value.
6. Optionally, to include another condition to the list of criteria that must be met in order for a user to be disabled, click **Add Condition** below the **Disable Users** section, and then repeat steps 3 through 5.


Note: If more than one condition appears in the Disable Users section, *all* of the conditions must be met in order for a user to be disabled.

7. 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 will have to navigate to this screen and click the **Disable Now** button each time you want to disable users
8. If you are unsure how many current users will be impacted by the criteria you set in steps 3 through 6, click **Calculate** to see the total number.
9. Consult the **Last Run** field to see the date and time the most recent disable action was carried out.
10. Click **Download Log** in the **Last Run Result** field to download a list of all of the users who were disabled during the last disable action.
11. Click **Save**.
12. Optionally, click **Disable Now** if you want to disable the list of users immediately.

Automatically delete users based on attributes

In organizations where changes to the userbase 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**. The Disable and Delete Users screen opens.
3. In the **Delete Users** section, click the drop-down list in the **Select Attribute** column and select the first attribute you want to use as a means of identifying users to be deleted.
4. As soon as you make a selection in the **User Attribute** drop-down list, the **Select Operator** drop-down list appears. Select an option from that list.
5. In the field that appears to the right of the **Select Operator** field, enter or select a value.
6. Optionally, click **Add Condition** below the **Delete Users** section, then repeat steps 3 through 5 to include another condition to the list of criteria that must be met in order for a user to be deleted.

Note: If more than one condition appears in the Deleted Users section, *all* of the conditions must be met in order for a user to be deleted.

7. 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 will have to navigate to this screen and click the Delete Now button each time you want to delete users.

8. If you are unsure how many current users will be impacted by the criteria you set in steps 3 through 6, click **Calculate** to get the total number.
9. Consult the **Last Run** field to see the date and time the most recent delete action was carried out.
10. Click **Download Log** in the **Last Run Result** field to download a list of all of the users who were deleted during the last delete action.
11. Click **Save**.
12. Optionally, click **Delete Now** if you want to delete the list of users immediately.
13. Optionally, in the **Purge Deleted Users** section, select **Purge deleted users after** and then select a timeframe. Selecting this option helps ensure that the userbase is kept current and database performance is maximized by reducing the number of active users. If your organization has a data retention requirement, leave this option unchecked.


Note: After a purge occurs, it cannot be undone.

Configure an Organization 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.

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 sub organizations or stand alone organizations.

1. In the navigation bar, click .
2. In the **Users** section, click **User Attributes**.
3. Select **Organizational Hierarchy**. The Organizational Hierarchy Attribute 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. 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.

Manage advanced settings for operators


For information on how to manage advanced settings for operators, see the *BlackBerry AtHoc Manage Operators and Administrators* guide.

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 next to 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**
- **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.

Assigning authentication methods to applications

You can specify the authentication method to use for the BlackBerry AtHoc management system, Desktop App, and Self Service.

Desktop App

1. In the navigation bar, click .
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods 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=(?<edi>\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 your 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 user 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 SmartCard, 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

Select the authentication method to use for the BlackBerry AtHoc management system, Desktop App, and Self Service.

1. In the navigation bar, click .
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods 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](#).
4. Optionally, if you selected Username and Password as the authentication method, select the check box to enable the option to save user names on the user's computer.
5. Optionally, if you selected Username and Password as the authentication method, select the check box to enable self-registration for new users.
6. Optionally, if you selected Username and Password as the authentication method, select the check box to enable two-factor authentication. When selected, the Delivery Methods for Sending Verification Code list appears. Select the delivery methods users can select to receive a verification code from the list. Click **Calculate** to view the number of users who do not have one of the selected delivery methods.
7. 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** window, 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 changed.
 - **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](#).
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 SDK User permissions to define the username and password for an API request.


1. In the navigation bar, click .
2. In the **Users** section, click **User Authentication**. The User Authentication window opens.
3. 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**. The User Authentication window opens.
4. In the **Enabled Authentication Methods** section, select the Username and Password **Enable** check box.

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. Next to **Users Unable to Log In**, click **Calculate** to see the number of users who do not have any of the 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 your the BlackBerry AtHoc system.
9. Click **Save**.


Enable single sign-on

Single sign-on 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 can access the BlackBerry AtHoc management system or Self Service without the need to sign in again.

If a user is not signed in, when they attempt to sign in, they are redirected to their organization's customer IDP login. 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.


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 formats: `<server>/selfservice/organization-code` if an organization code is available and `<server>/selfservice/provider-id` if no organization code is available. This URL is used when users attempt to access Self Service using SSO authentication.
5. Click **Configuration**.
6. On the **Self Service SSO configuration** window, configure [Identity Provider](#) and [Service Provider](#) settings.

Note: You can also [Export SP and IDP settings](#).
7. Click **Apply**.
8. 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 formats: `<server>/client/organization-code` if an organization code is available and `<server>/client/provider-id` if no organization code is available. This URL is used when a user attempts to access the BlackBerry AtHoc management system using SSO authentication.
5. Click **Configuration**.
6. On the **Management system SSO configuration** window, configure [Identity Provider](#) and [Service Provider](#) settings.
Note: You can also [Export SP and IDP settings](#).
7. Click **Apply**.
8. Click **Save**.

Configure SSO certificates on the application server

If you are installing a new SSO configuration, you must install and configure the SSO certificates on each application server.

1. Open **mmc** as an administrator.
2. For **Computer Account**, add the certificates snap-in.
3. On the **mmc console** window, in the left pane, expand **Certificates (Local Computer)**.
4. Right-click **Personal** and select **All Tasks > Import...**
5. On the **Certificate Import Wizard**, click **Next**.
6. On the **File to import** window, click **Browse** and navigate to select the certificate file on your local computer.
7. Click **Next**.
8. On the **Certificate Store** window, select **Place all certificates in the following store**.
9. In the **Certificate store:** field, click **Browse...** and select **Personal**.
10. Click **Next**.
11. Click **Finish**.
12. In the **mmc console**, right-click the installed certificate file and select **All Tasks > Manage Private Keys...**
13. On the **Permissions** dialog, on the **Security** tab, select the **IUSR** and **IIS_IUSRS** users.
14. Click **OK**.
15. Restart the **IIS**.

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.

If you are configuring a new SSO installation, complete the [Configure SSO certificates on the application server](#) before you configure the IDP settings.

1. On the **Management system SSO configuration** or **Self Service SSO configuration** window, 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 service provider 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.
2. Configure the following **Security Settings**:
 - a. **SAML Response 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 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. Select a **Signature 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. If **SAML Response Signature** is set to **Signed**, **Assertion Signature** is set to **Signed**, or **Assertion Encryption** is set to **Encrypted**, select a **Certificate Identifier**: Select **Serial Number** or **Subject Name**.
 1. **Certificate Value**: Specify the serial number or subject name of the X.509 certificate to be used to verify SAML signature assertions.
3. 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**
4. Click **Apply**.
 5. Click **Save**.

Configure Service Provider settings

1. In the **Management system SSO configuration** or **Self Service SSO configuration** window, 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. **Self Service Assertion Consumer Service URL** or **Management Assertion Consumer Service URL:** Enter the URL of the location of the service provider's ACS where SAML responses are sent as part of SSO.
 - c. **Logout Service URL:** Optionally, enter the URL of the service provider's endpoint that receives SAML log out messages. If SAML log out is not supported, leave this field blank. For more information, see [SSO logout service](#).
 - d. **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**.
2. Configure the following **Security Settings**:
 - a. **SAML Response Signature:** Select **Signed** or **Unsigned**. When **Signed** is selected, SAML authentication requests received from the partner IDP must be signed. Receiving signed authentication requests is optional but highly recommended.

Note: You must have a valid certificate installed for your organization.
 - b. If **SAML Request Signature** is set to **Signed**, select a **Signature Algorithm**. The default setting is **RSA-SHA256**.
 - c. **Certificate Identifier:** Select **Serial Number** or **Subject Name**.
 1. **Certificate Value:** Specify the serial number or subject name of the X.509 certificate whose private key will be used to generate signatures. If SAML messages are signed, a certificate PFX is required.
3. Click **Apply**.
4. 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 configured 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.)

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**. 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:

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 a 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://support.athoc.com/customer-support-portal.html>

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

Legal notice

©2019 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada