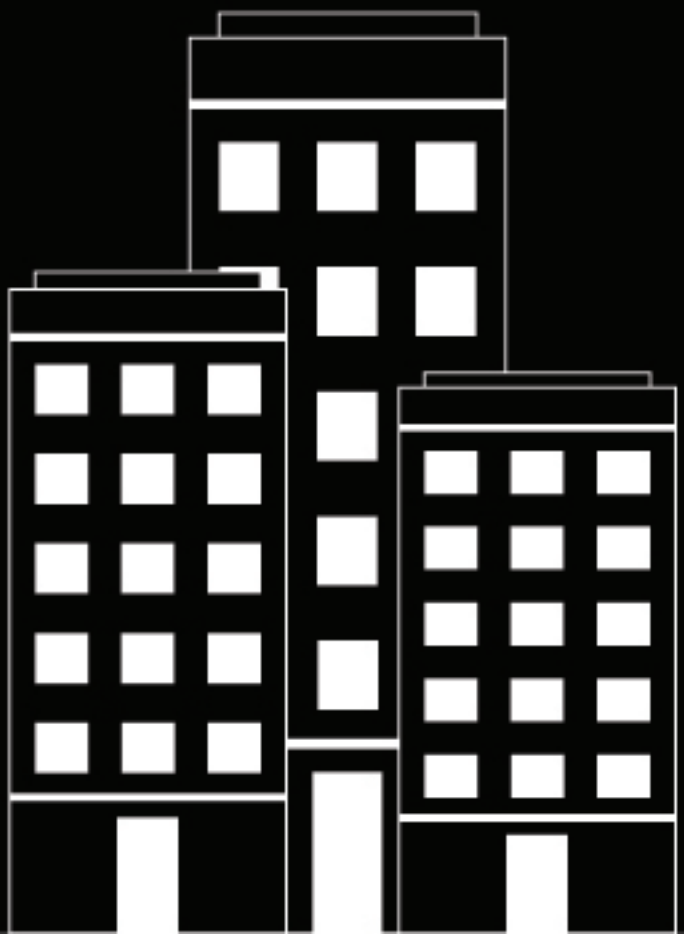

BlackBerry AtHoc

Operator Roles and Permissions

7.18

Contents

Operator roles and permissions

Only BlackBerry® AtHoc® System Administrators, Enterprise Administrators, and Organization Administrators can access the Edit Operator Permissions button on the user details page. The Edit Operator Permissions button displays the Operator Permissions page. The Operator Permissions page is used to grant or revoke a user's operator rights and assign operator roles. The Operator Permissions page also allows authorized users to define the user base of each operator. The user base is the subset of end users a publisher can target alerts to.

Operators cannot update their own roles and permissions. Administrators cannot assign or revoke permissions for a higher-level role than their role. For example, an Organization Administrator can grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

Enterprise and super enterprise organizations display users and operators in each sub enterprise and suborganization. Operators in a suborganization can be made an operator in the super enterprise or enterprise by using the Edit Operator Permissions button on the user details page in the super enterprise or enterprise organization. For more information, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

User base overview

A user base is a subset of end users that an operator can target alerts to and access through the Users and the Distribution Lists screens. Operators who have an unrestricted user base can target and access any user in the BlackBerry AtHoc system, while operators who have a restricted user base can target only the end users in their user base.

Operators who have a restricted user base cannot view information about users outside of their authorized user base, including in advanced reports, alert report summaries, delivery summary .csv files, or from the Details tab of a sent alert. A banner indicates how many users out of the total number are accessible for an operator with a restricted user base.

Note: If an operator with a restricted user base creates another operator, the new operator has the same user base restrictions. The parent operator can further restrict the user base of the new operator, but cannot assign them a less restricted user base.

The user base of an operator consists of end users from the following sources, which can be assigned using the User Base and Distribution Lists Permissions tabs of the operator:

- **Organizational nodes** (Optional. Not available on all systems): Users are selected based on membership in selected organizations.
- **Standard or customized user attributes assigned to end users**: Users are selected based on specific attributes such as department, job function, or location.
- **Distribution lists**: Users are selected based on their inclusion in selected distribution lists. Using distributions lists to identify users might result in the inclusion of people outside the designated user base of an operator.
- **Dependents**: Users are selected based on their relationship to a sponsor user.

The following table summarizes operator access privileges for features based on their user base.

User Base Restricted by....	Targeting Privileges	Distribution Lists Manager can...	End Users Managers can...
Custom or standard end user attributes	Operators can target only users who meet the specified attribute conditions	• Access the Distribution Lists screen • Assign users in their user base to static distribution lists	• View users in their user base • Edit custom and standard user attributes • Edit users device addresses and alert delivery schedules
Distribution lists (DLs)	Operators can target only the DLs they have Publishing privileges to. Static DLs can include users outside the user base. Dynamic DLs include only users in user base.	• Access the Distribution Lists screen • Access only the DLs they have View/ Manage privileges to	Edit user memberships in static DLs
Organizational nodes	Operators can target all members of a selected organization.	—	Assign user base to any organization to which operator has access privileges

User Base Restricted by....	Targeting Privileges	Distribution Lists Manager can...	End Users Managers can...
Dependents	Operators can target the dependent users of targeted sponsors.	—	View and Edit dependents

Switch a user base from unrestricted to restricted

If you have the necessary permissions, you can change the user base of an operator from unrestricted (the default) to restricted within BlackBerry AtHoc.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the name of the operator.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and then select the **Restricted** option.
5. Click **Save**.

Note: For complete details on how to set up restrictions on a user base, see Restrict a user base by attributes.

Note: You can also switch a user base from unrestricted to restricted with the Import Operators feature. For more information, see Importing and exporting operators.

Restrict a user base by attributes

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

If a parent operator has an unrestricted userbase, they can use either the AND or OR operators when assigning permissions to other operators. If a parent operator has a restricted userbase, they can only use the AND operator when assigning permissions to other operators. This prevents operators with a restricted userbase from assigning another operator permissions to access a less restricted userbase.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and select **Restricted**.
5. Click **Modify**.
6. Select the AND/OR operator. When AND is selected, the user attribute must meet all conditions to restrict the user base. When OR is selected, attributes that match any of the conditions are included. The default is AND.
7. On the **Create Conditions** screen, click **Select Attribute** and select the first attribute you want to use as restriction criteria.
8. In the **Select Operator** field, select the operator that you want to assign to the attribute.

   Note: The list of operators varies depending on the type of attribute selected.
9. In the next field that appears, enter or select a value for the attribute.
10. Optionally, click the **Add Condition** button and then repeat steps 7 through 9 for each additional attribute condition you want to add.

    Tip: You can restrict a user base using the User Last Updated Source attribute. For more information, see Restrict a user base with the User Last Updated Source attribute.
11. Optionally, if your organization is set up to display organizations, in the **Organization Hierarchy** section of the **User Attribute** drop-down list, select one or more options that the operator can select from as alert targets.

    Note: Users must belong to the selected organizational nodes and meet the other specified attribute conditions in order to be included in a user base.
12. When you are done creating restriction criteria, click **Apply**.
13. Optionally, on the **Operator Permissions** screen, view the list of end users who meet the criteria by clicking **View users** in the **User Base** section.
14. Click **Save**.

Restrict a user base with the User Last Updated Source attribute

Operators can restrict a user base with the User Last Updated Source attribute. The following table lists the possible sources and the search terms available to restrict a user base by source.

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

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the user details screen, scroll down to the **User Base** section and select **Restricted**.
5. Click **Modify**.
6. On the **Create Conditions** window, select the AND/OR operator. When AND is selected, users must meet all search conditions to be included in the search results. When OR is selected, users that match any of the search conditions are included. The default is AND.
7. Click **Select Attribute** and select **User Last Updated Source**.
8. Select an operation from the **Select Operation** list.
9. In the blank field that appears, enter the source to restrict the user's user base permissions by. The text you enter in this field must match one of the search terms listed in the table above. You can add more than one source, separated by a comma. For example, API, UserSyncClient.
10. Click **Apply**.
11. Click **Save**.

Restrict operator access to dependents

When an operator's access to dependents is restricted, the operator cannot view, edit, or delete a dependent user. The operator cannot target dependents in alerts or events, view them in reports, or export their data.

Operators have access to view, manage, and target dependents by default.

1. In the navigation bar, click **Users** > **Users**.
2. Click the row containing the operator name.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the **Operator Permissions** screen, scroll down to the **User Base** section and deselect the **Enabled** check box in the **Manage and Publish to Dependents** section.
5. Click **Save**.

Grant operator permissions to a user

When you grant operator permissions to a user, you select which roles the user has in BlackBerry AtHoc. The roles a user has determine the BlackBerry AtHoc features they can access. The roles that can be assigned to users are determined by the enabled features in an organization.

Only Organization Administrators, Enterprise Administrators, and System Administrators can grant operator permissions to users. Operators cannot update their own permissions. Operators cannot assign or revoke higher level operator permissions than their own permissions. For example, an operator with Organization Administrator permissions can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions

Only System Administrators and Enterprise Administrators can grant operator permissions to users in an enterprise or super enterprise organization.

User accounts that have the **Service Account** option selected do not have their operator permissions revoked in the following scenarios:

- Automatic revocation setting in the Security Policy settings.
- Operator role import.
- From the **More Actions** menu on the user profile.
- Manual removal of operator permissions by clicking **Edit Operator Permissions** on the profile page.

User accounts that have the **Service Account** option selected can have their operator permissions revoked through user move.

1. Create a user or select an existing user. After you create a new user and click **Save**, the user details screen appears.
2. Click **Grant Operator Permissions**.
3. On the **Operator Permissions** screen, in the **Operator Roles** section, click the **Operator Roles** list and select the roles you want to assign to the user.

   As you select roles, they appear on the screen under the Operator Roles drop-down list. If you select more than three roles, the first three are displayed, and the rest can be seen by clicking the scrollbar that appears in the field.

   Tip: Click **Operator Roles and Permissions Matrix** to view a complete mapping of BlackBerry AtHoc roles and their capabilities.
4. Optionally, in the **User** section, select the **Permissions Expire** option **Never** or **Choose a Date**. If you select the **Choose a Date** option, select a date from the calendar picker that appears.
5. Optionally, in the **User** section, select the **Service Account** check box. Select this option only for service accounts that are used to enable services such as SMS Opt-In, the User Sync Client, or API. Selecting this option prevents the user account from being automatically disabled or deleted, or having its operator permissions automatically revoked. If this option is selected, **Never** must be selected as the **Permissions Expire** option.
6. Optionally, in the **Password** section, enter and confirm a password that meets the specified requirements.
7. Optionally, in the **Password** section, select the check boxes to specify if the user must change their password at next login and whether the password expires.
8. Click **Save**.

Note: You can also grant operator permissions using the Import Operators feature. For more information, see Importing and exporting operators.

Edit operator permissions

Note: If you want to revoke all operator permissions for a user, see Revoke operator permissions.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the operator name in the list.
3. On the user details screen, click **Edit Operator Permissions**.
4. On the **Operator Permissions** screen, click the **Operator Roles** drop-down list and select the roles that you want to assign to the user.

   Note: Only operator roles that are at the same or lower-level than your role appear in the list. For example, if you are an Organization Administrator, you cannot assign the Enterprise Administrator role to another operator.
5. To remove an operator permission, click the **X** beside the name.
6. Click **Save**.

Note: You can also edit operator permissions with the Import Operators feature. For more information, see Importing and exporting operators.

Revoke operator permissions

You can only revoke the permissions of an operator whose permissions are at the same or lower level than your permissions.

If a user is logged in to the system when their operator permissions are revoked, they are logged out on their next page navigation and redirected to an error screen with the following message: "You do not have the required Operator Permissions to access this page. Contact your administrator."

Only System Administrators and Enterprise Administrators can revoke operator permissions from users in an enterprise or super enterprise organization.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the operator you want to revoke permissions for.
3. On the user details screen, click **More Actions** > **Revoke Operator Permissions**.

   A warning notification screen appears, asking "Are you sure you want to revoke Operator Permissions for this user?" and informing you that this action cannot be reversed. Revoking operator permissions cannot be undone, but you can later assign the permissions to the operator again using the Edit Operator Permissions button on the user details screen.
4. Click **Revoke**.

Note: You can also revoke operator permissions using the Import Operators feature. For more information, see Importing and exporting operators.

Revoke operator permissions from the External Operator Permissions screen

Use the External Operator Permissions settings page to revoke permissions for an operator who has permissions in another organization. You can only revoke the permissions of an operator whose permissions are at the same or lower level than your permissions. Only Organization Administrators, Enterprise Administrators, and System Administrators can revoke operator permissions.

Operator accounts that have the Service Account option selected cannot have their operator permissions revoked from the External Operator Permissions screen.

If a user is logged in to the system when their operator permissions are revoked, they are logged out on their next page navigation and redirected to an error screen with the following message: "You do not have the required Operator Permissions to access this page. Contact your administrator."

1. Log in to the management system as an administrator and change to the organization you want to assign roles in.
2. In the navigation bar, click .
3. In the **Users** section, click **External Operator Permissions**. A list displays the operators who have operator permissions in an organization that you also have operator permissions in.
4. On the **External Operator Permissions** screen, click the name of the operator. The user details screen opens, displaying the information for that user in the system.
5. Click **Revoke**. A warning screen appears, asking "Are you sure you want to revoke Operator Permissions for this user?" and informing you that this action cannot be reversed. Revoking operator permissions cannot be reversed, but you can later assign the permissions to the operator again using the **Edit Operator Permissions** button on the user details screen. If you want to remove only one or more operator permissions for a user, click the **X** in the pill for that role in the **Operator Roles** section.

Revoke operator permissions automatically

If you are an Organization Administrator, Enterprise Administrator, or System Administrator, you can configure your BlackBerry AtHoc system to automatically revoke operator permissions. When configured, operators who have not logged in to the system for the specified time have their permissions revoked. The operator's inactivity period is calculated using the Last Login Date attribute. If the operator has not logged in to the system, the inactivity period is calculated based on the date the operator was granted permissions on. When automatic revocation of operator permissions is enabled, a system job runs every 24 hours to revoke operator permissions based on the operator's last successful login.

Operator accounts that have the Service Account option selected cannot have their operator permissions automatically revoked.

Tip: Use the Last Login Date attribute to identify and notify operators whose permissions will be automatically revoked due to inactivity.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Revoke Operator Permissions** section, click **Add Condition**.
4. Select one or more roles from the **Operator Roles** list.

   Note: You can only revoke permissions for operators who have the same or lower-level permissions that you have. For example, if you are an Organization Administrator, you cannot revoke the permissions of Enterprise or System Administrators.
5. Select the number of days of inactivity from the **Auto Revoke Permissions after** list.
6. Optionally, click **Add Condition** to add an additional revocation rule. You can add up to three rules.
7. Optionally, click to remove a revocation rule.
8. Click **Save**.

Assign distribution list permissions

In each organization, someone is usually assigned the role of Distribution Lists Manager. The Distribution Lists Manager can create, edit, delete, and import distribution lists. This is a distinct and more powerful role than being able to edit a distribution list and use it to target alerts. Operators with the Advanced Alert Publisher or Draft Publisher role cannot manage distribution lists, but can select lists as recipients for an alert.

Note: You can assign distribution list permissions to an operator in another organization using the External Operator Permissions screen.

Note: You can only assign distribution list permissions to distribution lists that you have access to.

Assign distribution list permissions from the User Details screen

You can only assign distribution list permissions to distribution lists that you have access to.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click the name of the user to whom you want to assign distribution list permissions.
3. On the user details screen, click **Edit Operator Permissions**.
4. In the **Distribution Lists** section, do one of the following:
   - Keep the default settings of **Unrestricted** for the Publish and Manage fields to allow the user to manage and publish alerts to all existing distribution lists in the organization that the user is associated with.
   - Set one or both fields to **Restricted** if you want to limit the distribution lists that a user can manage or publish.
5. If you selected the first option in Step 4, go to Step 8. If you selected the second option in Step 4, continue to Step 6.
6. When you select the **Restricted** option next to the **Publish or Manage** field, a **Modify** link appears next to it.
7. Click **Modify** to open the **Distribution Lists** screen, which displays all distribution lists in the system.
   - To allow the operator to publish to a specific list, select the check box in the **Publish** column for that list.
   - To allow the operator to view and edit a specific list, select the check box in the **View/Manage** column for that list.
8. Click **OK**.

The distribution list permissions of the user are updated in the system.

Assign distribution list permissions from the External Operator Permissions screen

You can only assign distribution list permissions to distribution lists that you have access to.

1. In the navigation bar, click .
2. In the **Users** section, click **External Operator Permissions**.
3. On the **External Operator Permissions** screen, click the name of the operator you want to give distribution list permissions to. You can search by username to narrow the list of operators.
4. On the operator details screen, in the **Operator Roles** section, select **Dist. Lists Manager** from the **Operator Roles** list.
5. Optionally, to grant the operator access to publish to all distribution lists, select the **Publish Unrestricted** option in the **Distribution Lists** section. This is the default option.

6. Optionally, to grant the operator access to publish to specific distribution lists, in the **Distribution Lists** section, select the **Publish Restricted** option, and then click **Modify**. On the **Distribution Lists** screen, select the check box in the **Publish** column for each distribution list you want to give the operator permissions to publish to. Click **OK**. You are returned to the operator details screen.
7. Optionally, to grant the operator access to manage all distribution lists, in the **Distribution Lists** section, select the **Manage Unrestricted** option. This is the default option.
8. Optionally, to grant the operator access to manage specific distribution lists, in the **Distribution Lists** section, select the **Publish Restricted** option, and then click **Modify**. On the **Distribution Lists** screen, select the check box in the **View/Manage** column for each distribution list you want to give the operator permissions to publish to. Click **OK**. You are returned to the operator details screen.
9. Click **Save**.

Importing and exporting operators

The Operator Import and Export feature enables Enterprise Administrators and Organization Administrators to add a large number of operator accounts to their BlackBerry AtHoc organization by using a CSV file. Enterprise Administrators can also import and export operators for all suborganizations from an enterprise organization. Enterprise Administrators in a super enterprise organization can import and export operators for all sub enterprise and suborganizations in the super enterprise organization.

The Operators Import and Export feature is enabled for all organizations by default. This feature can be disabled for any organization, if needed. For more information, see "Enable and disable features" in the *BlackBerry AtHoc System Settings and Configuration* guide.

The Operator Import and Export feature enables administrators to perform the following actions for up to 500 operators in a single operation:

- Add operator roles to existing users
- Add restrictions to existing users
- Remove operator roles and restrictions from existing users
- Revoke all operator permissions
- Add or remove operator user base restrictions
- Add or remove operator access to static distribution lists, dynamic distribution lists, user bases, and folders
- Update password expiration settings
- Update the "User must change password at next login" setting
- Add or remove an operator's ability to manage dependents or publish alerts to dependents

Prerequisites and restrictions

- You must be an Enterprise Administrator or Organization Administrator. In a super enterprise, you must be an Enterprise Administrator.
- Operators cannot update their own permissions.
- Operator accounts that have the Service Account option selected cannot have their permissions revoked via operator import.
- Operators cannot assign or revoke higher level operator permissions than their own permissions. For example, an Organization Administrator can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.
- Only existing enabled users in the given organization can be imported as operators.
- If an import includes an Organization column and you are performing the import from an enterprise organization, operators are imported for both the enterprise and suborganizations. Only Enterprise Administrators can import or export operators across the enterprise and suborganizations.
- If an import includes an Organization column and you are performing the import from a super enterprise organization, operators are imported for both the sub enterprise organizations and suborganizations. Only Enterprise Administrators can import or export operators across the super enterprise, sub enterprise organizations, and suborganizations.
- If no Organization column is included in the import file, operators are imported only to the current organization.
- When updating a user base restriction for an operator, there is a limit of 10 conditions. You can use the OR or AND operators to update a user base restriction. You must enclose each condition and operand with double quotation marks (""). For example, `"username" "contains" "abc" OR "organizational hierarchy" "at or below" "xyz"`.
- All distribution lists, folders, and attributes being imported for an operator account must already exist in your organization.
- Only users with unique user names and mapping IDs in the system can be granted operator permissions.
- Operator import does not support these fields: Firstname, Lastname, Displayname, Password changed date, and Last login date. If the import file contains these columns, they are ignored and the import proceeds

without error. These columns may appear in your import file if you exported operator information and then modified the export file for import.
- Partial import is not supported. (If an attribute for an operator in the import CSV file is incorrect, the operator is not imported.)
- Up to 500 operators can be imported in a single import.
- Parallel imports are not supported. Only a single operator or user import can be processed at a time.

Import operators using a CSV file

Important: When you import operator details into BlackBerry AtHoc using a CSV file, the values that exist in the CSV file overwrite any existing values in the database. If the file contains blank fields, the current values in the database are replaced by empty values. You should make sure that all required fields are populated before you upload the file.

To import operators from a file, the file must be correctly formatted. If you do not know how to format the file, see Format an operator import file.

If duplicate operators (identified by username or mapping ID) are found in the CSV file, they are not imported and one of the following error messages is displayed:

```
[Username]: <username> already exists in the payload
```

```
[Mapping ID]: <mapping id> already exists in the payload
```

The remaining non-duplicate operators in the CSV file are imported.

If a username contains a space or one of the following characters, the user is not imported and an error message is displayed:

[ ] : : | = , + * ? < >

Leading or trailing spaces are ignored and trimmed during the import process. After the spaces are trimmed, the username is accepted and the operator is imported.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** screen, click **More Actions** > **Import** > **Operators**.
3. Optionally, to download a blank CSV file to use as a template for your import operator file, click the **Download a template CSV file**. Save the file to your computer and fill in the appropriate operator information.

   Note: Using the template ensures that all of the mandatory attribute columns are included in the import file.
4. Click **Browse**.
5. Navigate to the location of the import operator file on your computer.
6. Open the file to enter or modify the operators' data.

   Note: Microsoft Excel hides some characters from view. If you edit the file in Microsoft Excel, it might format your entries with extra characters. The incorrect format might cause the import operation to fail. If you are using anything other than a text editor to modify the CSV file, open the file in a text editor such as Microsoft Notepad, review the syntax for problems, then save the modified file as a .txt file. Edit the file name to change the extension from .txt to .csv. This method preserves the formatting in the text file.
7. Verify that columns with multiple values have the correct format to import correctly.
   - The entire entry must be enclosed within double-quotes. This rule is true even if a multi-select picklist has only a single entry.
   - Use a comma to separate each value. Do not include spaces before or after the comma.
   - If you are importing user base restrictions, you must enclose each value with double quotation marks ("").
8. After you have entered your data, save and close the file.

9. Click the filename, and click **Open** to upload the file into the system.

   The filename appears in the Operator CSV File field on the Import Operator screen. Each of the columns from the import file are listed in the **Select the columns to import** section.
10. Select the columns of data you want to import or click **Select All**.
11. Review the **Columns that cannot be imported** list to verify that it does not contain important data that you must be able to view within BlackBerry AtHoc. If the list contains important columns of information, contact BlackBerry AtHoc Customer Support for help.
12. Click **Import**. The Importing Operators window opens.

When the import completes, the Import Details: Import Completed screen displays the following information:

- Total number of operators in the import file
- Total number of operators who were processed
- Number of operators who were successfully processed
- Number of operators who failed to be processed
- Username of the person who imported the file
- Time the file import process started and ended

Tip: Click **Download Log** on the Import Details: Import Completed screen to download a CSV file that includes information about the sync status of the operator import.

Format an operator import file

Operator import does not support these fields: Firstname, Lastname, Displayname, Password changed date, and Last login date. If the import file contains these columns, they are ignored and the import proceeds without error. These columns may appear in your import file if you exported operator information and then modified the export file for import.

To import a CSV operator file, the following formatting standards are required:

Field Name	Description	Is Mandatory?
Username	The Username is a value that can be used to identify a user in the BlackBerry AtHoc system and the user repository (for example, LDAP or Microsoft Active Directory) within your organization. The Username column must contain a unique value. The username cannot contain spaces or any of the following characters: [ ] : ; | = + * ? < >. Leading or trailing spaces are trimmed during the import process. After the leading or trailing spaces are trimmed, the username is accepted and the operator is imported.	Yes

Field Name	Description	Is Mandatory?
Roles	Use the Roles column to assign roles and their associated permissions with an operator. To include multiple roles, use a comma-separated list with no spaces. The following roles can be included: • Accountability Manager • Accountability Officer • Activity Log Manager • Activity Log Viewer • Alert Manager • Advanced Alert Manager • Alert Publisher • Advanced Alert Publisher • Basic Administrator • Basic Operator • Connect Agreement Manager • Dist. Lists Manager • Draft Alert Creator • Enterprise Administrator • Organization Administrator • Report Manager • SDK User • User Manager **Note:** The roles that can be imported depend on the type of organization that you are importing operators in to (suborganization, enterprise organization, super enterprise organization, or system setup). For more information about BlackBerry AtHoc roles and permissions, see BlackBerry AtHoc roles.	Yes
Permission expiration date	Set a date in the format configured for your organization in General Settings, or leave the cell blank to have no expiration date. The date must be equal to or later than the current date.	No
Alert Folders manage/ publish	Enter the names of alert folders to give the operator permission to create, rename, delete, and publish alerts to them.	No

Field Name	Description	Is Mandatory?
User base manage/ publish	Enter the user attributes you want to restrict the operator's access to. Leave this column blank to import operators with an unrestricted user base. You must enclose each value with double quotation marks (""). To restrict an operator's user base by organization hierarchy, ensure that the nodes in the organizational hierarchy attribute do not contain commas (,). **Tip:** Open the user profile of a user in your organization that has a restricted user base and click in the **User Base** section to copy the attributes.	No
Dependents manage/ publish	Enter **Yes** to enable the operator to create, delete, edit, and publish alerts to dependent users. Enter **No** to restrict the operators permissions to manage and publish alerts to dependent users. If a value is not entered, it is treated as a **No** value.	No
Distribution List publish	Enter the names of static or dynamic distribution lists the operators will have permission to publish alerts to.	No
Distribution List manage	Enter the names of static or dynamic distribution lists the operators will have permission to manage.	No
Password never expires Yes/No	Enter **Yes** to configure the operators' passwords to never expire.	No
Change password next login Yes/No	Enter **Yes** to require operators to reset their password at next login.	No
Organization	Use the Organization column to assign operator roles to operators in organizations across a super enterprise or enterprise (including across the super enterprise, enterprise organization, sub enterprise organizations, and suborganizations.) **Note:** The Organization column does not assign users to organizations, it assigns operator roles in the specified organization.	No

Stop the import operators process

Important: When you import operator details into BlackBerry AtHoc using a .csv file, the values that exist in the .csv file overwrite any existing values in the database. If the .csv file contains blank fields, the current values in the database are replaced by empty values.

While the import operator process is underway, click **Cancel** or **Back** to stop the import.

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

Undo the import operators process

The import operators process cannot be undone after it runs. The only way to undo the import is to reimport the original data that was overwritten.

Export operators to a file

You must be an Enterprise Administrator or Organization Administrator to export operators. Only enabled users with operator roles can be exported. The export operator process exports all roles and permissions for the selected operators in the current organization. Enterprise Administrators can export operators from the enterprise organization for all operators in the enterprise and suborganizations. Enterprise Administrators in a super enterprise can export operators from the super enterprise organization for all operators in the super enterprise, sub enterprises, and suborganizations. The Export Operator feature must be enabled for the organization.

1. In the navigation bar, click **Users** > **Users**.
2. Select the check boxes beside the usernames that you want to export.
3. Click **More Actions** > **Export** > **Operators**. The Exporting Operators window opens while the export is in progress.

When the export is complete, a .csv file is downloaded. The .csv filename has the following format: AtHoc-{*provider-name*}ExportCSV_{*current-date-and-time*}.

The downloaded .csv file contains the following information for the exported operators:

- Username
- Firstname
- Lastname
- Displayname
- Roles
- Permission expiration date
- Alert Folders manage/publish
- User base manage/publish
- Dependents manage/publish Yes/No
- Distribution List publish
- Distribution List manage
- Password changed date
- Password never expires Yes/No
- Change password next login Yes/No
- Last login date
- Organization (for super enterprise and enterprise organizations only)

Change organizations

1. In the navigation bar, click your username.
2. Click **Change Organization**.

   Note: If your username is associated with only one organization, the Change Organization link does not appear.
3. Optionally, on the **Change Organization** screen, do any of the following:
   - Click the name of an organization in the **Name** column to view the organization hierarchy of that organization.
   - In the search field, enter an organization code, ID, or name, and then click or press **Enter** on your keyboard to filter the displayed organizations.
   - Click any column header to sort the list of available organizations.
   - From the **All Organizations** pull-down list, select **Super Enterprise**, **Enterprise**, **Sub Organizations**, or **Basic** to filter the list of organizations.
4. Click the row for the organization you want to switch to.
5. On the **Change Organization** confirmation window, click **OK**.

Subscribe users to organizations

This section describes how to subscribe users to suborganizations other than their home organization using the BlackBerry AtHoc management system or the CSV user import process. For instructions on how to subscribe to organizations from Self Service, see the *BlackBerry AtHoc Self Service User Guide*.

For more information about organization subscriptions, see "Manage organization subscriptions" in the *BlackBerry AtHoc Manage Users* guide.

Before you begin: Before users can be subscribed to organizations, the following conditions must be met:

- The Organization Subscriptions feature must be enabled on the enterprise organization.
- In a super enterprise organization, the Organization Subscriptions feature must be enabled on the super enterprise organization.
- The Enterprise Administrator must configure the subscription organizations.
- The Organization Subscription for End Users option must be selected in the Customization > Self Service section in General Settings in a suborganization for end users to be able to subscribe to that organization from Self Service.

Subscribe a single user

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select a user from the list.
4. On the user details screen, click **Edit User**.
5. On the user details screen, in the **Organization Subscriptions** section, click **Add Subscription**.
6. On the **Subscribe Organization** screen, select an organization from the list.
7. Click **Apply**.
8. In the **Organization Subscriptions** section, enter a date or click to select a start date for the subscription.
9. Optionally, click to set an end date for the subscription.
10. Optionally, repeat Steps 5 to 9 to subscribe the user to additional organizations. You can subscribe the user to a maximum of 10 available organizations.
11. Click **Save**.

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

Subscribe multiple users

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

1. Log in to the BlackBerry AtHoc management system.
2. Click **Users** > **Users**.
3. On the **Users** screen, select the users you want to subscribe to organizations.
4. Click **More Actions** > **Export** > **Users**.
5. On the **Export Users** screen, in the **All Columns** list, select **Subscribed Organizations** > **Add >**.
6. Click **Export CSV**.
7. Save the CSV file to your local system.

8. Open the CSV file.
9. Update the **Subscribed Organizations** column to add, remove, or modify the organizations for each user. You can subscribe each user to a maximum of 10 available organizations.
10. Optionally, in the **Subscribed Organizations** column, add start and end dates for the subscription. Separate the start and end dates with a pipe (|) character. Use the date format of your current organization. For example: `Sub-Org1: 4/5/2021|8/8/2021, Sub-Org3: 5/5/2021|, Sub-Org4|7/7/2021`.
11. Save the CSV file.
12. In the BlackBerry AtHoc management system, click **Back** to return to the Users screen.
13. Click **More Actions** > **Import** > **Users**.
14. On the **Import User File** screen, click **Browse** and select the CSV file on your local system.
15. Click **Open**.
16. In the **Select the columns to import** section, select **Subscribed Organizations**.
17. Click **Import**.
18. Optionally, on the **Import Details** window, click **Download Log** to view the results.

The updated users can now be targeted in alerts and events from their subscribed organizations.

Assign permissions for a different organization

If you have users that need to have access to multiple organizations, you grant access using the same account for each organization. You can create the user once and grant that user operator permissions in another organization, as long as the other organization is a sub enterprise or suborganization within the enterprise or super enterprise. This gives operators access to multiple organizations without the need to have multiple accounts.

Assign roles for a different enterprise

Use the External Operator Permissions settings page to give permissions to an operator who has permissions in another organization.

1. Log in to the BlackBerry AtHoc management system as an administrator and change to the organization you want to assign roles for.
2. In the navigation bar, click .
3. In the **Users** section, click **External Operator Permissions**.

   A list displays the operators who have operator permissions in an organization that you also have operator permission in.
4. Click **Add** to add existing operators from external organizations to the list. The Add Operator Permissions to External Operator window opens.
   a. Search for the operator in the **Search By Username** field and then select an operator. The user details page opens.

      The user account must be an operator in their home organization before they appear in this list. You must also be an administrator in the home organization of the user.
   b. Select the roles that you want the operator to have from the **Operator Roles** list. A full list of BlackBerry AtHoc roles is provided, including all administrator roles. If the user should be an administrator, use the following guidelines:

      - In System Setup, select the System Administrator role. With this role, the operator has administration privileges for settings privileges (no user management or alerting privileges) for all organizations in the system.
      - In an enterprise organization, select the Enterprise Administrator role. With this role, the operator has administration privileges for the enterprise organization and all suborganizations.
      - In a super enterprise organization, select the Enterprise Administrator role. With this role, the operator has administration privileges for the super enterprise organization, sub enterprise organizations, and all suborganizations.
      - In a suborganization, select the Organization Administrator role. With this role, the operator has administration privileges for the local suborganization.
      - In a Basic organization, select the Basic Administrator role. With this role, the operator has administration privileges for the local organization.

   c. Select the distribution lists the administrator can work with.

      - Publish: When selected for a distribution list name, the administrator can publish alerts to the members of the list.
      - Manage: When selected for a distribution list name, the administrator can view and manage the list.
5. Click **Save**.

Note: To change the roles for an existing administrator, click the user name and modify the details pages as described in Step 4.

Assign roles for the enterprise from a suborganization

If you have a super enterprise or enterprise organization, certain operators in sub enterprise organizations and suborganizations need access to the super enterprise or enterprise organization. This enables the operator to send alerts from the super enterprise or enterprise or manage the super enterprise or enterprise organization. For more information, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

If a user in a member organization needs access to the super enterprise or enterprise organization, you can edit their operator permissions at the super enterprise or enterprise level.

1. Log in to the BlackBerry AtHoc management system as an Enterprise Administrator and change to the super enterprise or enterprise organization.
2. In the navigation bar, click **Users** > **Users**.
3. On the **Users** screen, click the operator whose permissions you want to edit.
4. On the user details screen, click **Grant Operator Permissions**.
5. Click the **Operator Roles** list and then select the roles you want to assign to the user.

   Granting the Enterprise Administrator role gives this user full administrator permissions to all sub enterprise organizations or suborganizations.
6. To remove an operator permission, click **X** beside the name.
7. Click **Save**.

View operator roles in multiple organizations

If an operator has roles and permissions in multiple organizations, you can view the operator's roles in the organization you are currently logged in to from the Permissions section of the operator's profile page. You can also view the operator's roles in other organizations from the user manager page and from the operator's profile page.

1. In the navigation bar, click **Users** > **Users**.
2. On the **Users** page, do one of the following:
   - In the **Roles** column, click **Roles in {x} other organizations**.
   - Click the row for the operator you want to view. In the user profile page, in the **Permissions** section, click **This user has roles in {x} other organizations**.

The **Roles in other organizations** window opens and displays the roles the operator has in each additional organization.

Manage access to alert folders

The Alert Folders Manager centralizes alert folder configuration and management tasks. You can grant access to alert folders to operators in other organizations. You can only grant access to alert folders that you have access to.

1. In the navigation bar, click .
2. In the **Users** section, click **External Operator Permissions**.
3. On the **External Operator Permissions** screen, click the name of the operator you want to give access to alert folders to. You can search by username to narrow the list of operators.
4. On the operator details screen, in the **Operator Roles** section, select a role that has alert publishing permissions from the **Operator Roles** list.
5. Optionally, in the **Alert Folders** section, select the **Publish/Manage Unrestricted** option to grant access to all alert folders in the organization.
6. Optionally, in the **Alert Folders** section, select the **Publish/Manage Restricted** option to grant access to specific alert folders in the organization. The folders list appears. Select the folders you want to give the operator access to.
7. Click **Save**.

After you finish: You can also manage access to alert folders using the Import Operators feature. For more information, see Importing and exporting operators.

BlackBerry AtHoc roles

Enterprise Administrators, Organization Administrators, and System Administrators can grant operator permissions to any user who needs access to the BlackBerry AtHoc management system. Granting operator permissions includes selecting which roles the user has when they are logged in, as well as setting any restrictions. Roles are additive: you can assign multiple roles and they build on one another, such as End Users Manager and Advanced Alert Publisher.

Administrators cannot assign or revoke higher level operator permissions than their own permissions. For example, an Organization Administrator can revoke or grant Organization Administrator permissions to another operator, but cannot grant Enterprise Administrator or System Administrator permissions.

The role that a user is assigned to determines what BlackBerry AtHoc features they can access. Roles that are associated with specific features in BlackBerry AtHoc can only be assigned to users when that feature is enabled for that user's organization. The features in the following table are restricted to specific roles.

Feature	Roles
Account	• Accountability Manager • Accountability Officer
Activity Log	• Activity Log Manager • Activity Log Viewer
Connect **Note:** Connect is enabled and the Connect Agreement Manager role becomes available when organizations are connected.	Connect Agreement Manager
Situation Response	• Plan Manager • Plan Incident Manager
Collaborate	Collaboration Manager

The following sections describe the roles that are available in BlackBerry AtHoc.

For more information, see the *BlackBerry AtHoc Roles and Permissions Matrix*.

Accountability Manager

Account

- View, create, duplicate, search for, and delete accountability templates
- Create, delete, search for, and end accountability events
- Change the end time for accountability events
- Use the live map
- View accountability event dashboards
- Export accountability event reports
- Report status on behalf of others

Publisher map

- Export users list

Basic settings

- Manage accountability template settings

Accountability Officer

Account

- Search for accountability events
- Use the live map
- View accountability event dashboards
- Export accountability event reports
- Report status on behalf of others

Activity Log Manager

Alerts

- View, search, and export the activity log
- Create, modify, and edit the activity log

Activity Log Viewer

Alerts

- View, search, and export the activity log

Alert Manager

Give the Alert Manager role to an operator who needs to manage alerts and users, but should not have access to all settings. The Alert Manager role provides the maximum publishing privileges.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen

- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Manage distribution lists
- Mange user attributes
- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Reports

- View personnel, alerts usage, and user summary reports

Basic settings

- Configure alert template settings
- Configure alert folder settings

System setup settings

- Access the operator audit trail

User settings

- Configure user attribute settings
- Translate custom user attributes

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Advanced Alert Manager

Give the Advanced Alert Manager role to operators who need to manage alerts and users, but should not have access to all settings. The Advanced Alert Manager role provides the maximum publishing privileges as well as access to alert rules, delivery templates, audio files, placeholders, and user settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Manage alert rules
- Create and edit alert placeholders

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Manage distribution lists
- Mange user attributes

- Prioritize personal devices

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Reports

- View personnel, alerts usage, and user summary reports

Basic settings

- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rules

System setup settings

- Access the operator audit trail
- View geocoding summary and logs

User settings

- Configure user attribute settings
- Translate custom user attributes

Map settings

- Manage map settings
- Set default map view

- Add shape layer
- Add distribution list

Alert Publisher

Give the Alert Publisher role to operators who need to create and publish alerts but should not have access to all settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export the users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Advanced Alert Publisher

Give the Advanced Alert Publisher role to operators who need to create and publish alerts and configure alert settings.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders

Mobile publishing

- Publish alerts from the mobile app

Publisher map

- Export the users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Basic settings

- Configure alert template settings
- Configure alert folder settings

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings

Basic Administrator

The Basic Administrator role is available only in the BlackBerry AtHoc Basic edition.

Alerts

- Create and publish alerts
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates

Users

- Manage users
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View sent invitations
- Access All Organizations screen
- Access the Connect profile

Basic settings

- Configure alert placeholder settings
- Configure delivery template settings

- Configure audio file settings
- Configure alert rule settings

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Basic Operator

The Basic Operator role is available only in the BlackBerry AtHoc Basic edition.

Alerts

- Create and publish alerts
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts
- Create, edit, import, export, search for, delete, and duplicate alert templates

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- Publish a quick alert

Basic settings

- Configure accountability template settings

Collaboration Manager

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Connect Agreement Manager

Give the Connect Agreement Manager role to the people in your organization who need to manage AtHoc Connect.

Alerts

View, search for, and mark alerts as reviewed from the Inbox

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View sent invitations
- Access All Organizations screen
- Access the Connect profile

AtHoc Connect settings

Configure Connect profile settings

Distribution Lists Manager

Users

- Manage distribution lists

Reports

- View Personnel reports

Draft Alert Creator

Give the Draft Alert Creator role to operators who should write but not send alerts.

Alerts

- Create and save a draft alert
- Create, edit, duplicate, end, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

End Users Manager

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Manage dependents
- Manage subscriptions
- Move and subscribe users from their suborganization to other suborganizations
- Prioritize personal devices
- Create and import service accounts

Publisher map

Export users list

Reports

Access personnel reports

System Setup Settings

View geocoding summary and logs

Enterprise Administrator

The Enterprise Administrator role is used by customers who have multiple organizations to manage as part of an enterprise or super enterprise. Enterprise Administrator is the most powerful role in the super enterprise or enterprise and should be reserved for users who need to have access to everything in them. See the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide for more information about enterprise alerting.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Search for, view, and export alerts from suborganizations from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Reset system alert template to default values
- Create new alert folders, edit personal folders, search for folders
- Configure audio files

- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists
- Move and subscribe users from their suborganization to other suborganizations
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists
- Manage user attributes
- Prioritize personal devices
- Create and import service accounts

Mobile publishing

Publish alerts from the mobile app

Publisher map

Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Account

- View, create, search for, duplicate, and delete accountability templates
- Create, search for, delete, and end accountability events
- Change the end time for accountability events
- Use the live map

- View accountability event dashboards
- Export accountability event reports
- Report status on behalf of others

Reports

View personnel, alerts usage, and user summary reports

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View sent invitations
- Access All Organizations screen
- Access the Connect profile

Plan

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Plan Incidents

- Create an incident
- Edit an incident
- End an incident
- Publish an incident
- Export an incident
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Basic settings

- Configure general settings
- Configure dependent profile page layout

- Configure organization subscription
- Configure alert placeholder settings
- Configure accountability template settings
- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings
- Configure map settings
- Configure external events settings

AtHoc Connect settings

Configure AtHoc Connect profile settings

System setup settings

- Configure security policy settings
- Configure system health settings
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail
- View geocoding summary and logs

User settings

- Grant external operator permissions
- Disable and delete end users
- Configure distribution list folders

  Note: The Enterprise Administrator can access distribution list folder settings from a standalone enterprise organization with no suborganizations.
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication
- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings
- Configure mass device endpoints

- Configure desktop app settings
- Configure mobile app settings

Device Manager

- Access the device manager
- View device details
- Edit devices
- Enable and disable devices
- Set device delivery preference

Super enterprise

Manage all features and settings in a super enterprise organization.

Organization Administrator

The Organization Administrator role provides the maximum privileges in a single organization.

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Reset system alert template to default values
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Users

- Add, edit, or delete users
- Import and export users
- Enable and disable users
- Add and remove users from static distribution lists

- Move and subscribe users from their suborganization to other suborganizations
- Grant operator permissions
- Revoke operator permissions
- Manage distribution lists
- Manage user attributes
- Prioritize personal devices
- Create and import service accounts

Mobile publishing

Publish alerts from the mobile app

Publisher map

Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Account

Use the live map

Reports

View personnel, alerts usage, and user summary reports

Organizations (Connect)

- View Connected organizations
- Connect with organizations
- View sent invitations
- Access All Organizations screen
- Access the Connect profile

Plan

- Create a new plan
- Edit a plan
- Delete a plan

- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Plan Incidents

- Create an incident
- Edit an incident
- Edit a draft incident
- End an incident
- Publish an incident
- Export an incident
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Basic settings

- Configure general settings
- Configure dependent profile page layout
- Configure alert placeholder settings
- Configure alert template settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings
- Configure map settings
- Configure external events settings

AtHoc Connect settings

Configure AtHoc Connect profile settings

System setup settings

- Configure security policy settings
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail

- View geocoding summary and logs

User settings

- Grant external operator permissions
- Disable and delete end users
- Configure distribution list folders
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication
- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings
- Configure mass device endpoints
- Configure desktop app settings
- Configure mobile app settings

Device Manager

- Access the device manager
- View device details
- Enable and disable devices
- Edit devices
- Set device delivery preference

Plan Incident Manager

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders

- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Plan

- View Plans in read-only mode

Incidents

- Create an incident
- Edit a draft incident
- End an incident
- Publish an incident
- View activity
- Export activity log
- Add new entry in activity log
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Plan Manager

Alerts

- Create and publish alerts
- Create and save a draft alert
- View, search for, and mark alerts as reviewed from the Inbox
- Forward and reply to alerts from the Inbox
- Create, edit, duplicate, end, publish, and delete alerts, find alerts on the live map, and search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen
- Create, edit, import, export, search for, delete, and duplicate alert templates
- Create new alert folders, edit personal folders, search for folders
- Configure audio files
- Configure delivery templates
- Configure devices
- Configure mobile alert settings
- Configure alert rules
- Create and edit alert placeholders
- View, search, and export activity logs
- Create and edit activity logs
- Publish activity logs

Plan

- Create a new plan
- Edit a plan
- Delete a plan
- Duplicate a plan
- Disable a plan
- Enable a plan
- Approve a plan
- View active plans

Incidents

- Create an incident
- Edit a draft incident
- End an incident
- Publish an incident

- View activity
- Export the activity log
- Add new entry to activity log
- Activate plan steps

Collaborate

- Start a collaboration
- View and participate in all active collaborations in their organization
- View and participate in collaborations from the BlackBerry AtHoc mobile app
- End a collaboration
- Export ended collaborations

Publisher map

- Export users list

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Report Manager

Alerts

- Search for alerts from the Sent Alerts screen
- Export sent alerts from the Sent Alerts screen

Reports

- View Personnel reports

SDK User

The SDK User role is used by external applications to perform tasks such as sending alerts and creating users.

- This is the primary role needed to access all V1 APIs.
- This role performs all actions supported by the BlackBerry AtHoc SDK.

In the BlackBerry AtHoc management system, an SDK User can also perform the following actions:

Device settings

- Configure SDK settings
- Configure web API login settings

System Administrator

Designed for the people responsible for maintaining the entire system of servers, who are often IT staff. This role hides user information by default, but can increase its own roles if needed to accomplish more tasks. This role can only be given in the System Setup (3) organization.

Alerts

- Search for, view, and export alerts from suborganizations from the Sent Alerts screen
- Reset system alert template to default values

Users

- Grant operator permissions
- Revoke operator permissions

Live map

- Access the live map
- View layers
- View users
- View users in drawn shapes
- View incoming alerts
- View live alerts and events
- Publish a quick alert
- Export users

Basic settings

- Configure general settings
- Update the organization code in General Settings
- Enable dependents
- Configure dependent profile page layout
- Enable organization subscription

- Configure alert placeholder settings
- Configure alert folder settings
- Configure delivery template settings
- Configure audio file settings
- Configure mobile alert settings
- Configure alert rule settings
- Configure map settings
- Configure external events settings

System setup settings

- Configure security policy settings
- Configure global system health settings
- Configure system settings
- Configure system health settings
- Access and export the diagnostic log
- Clear the diagnostic log
- Access archive settings
- Access the organizations manager settings
- Configure feature enablement
- Configure integration manager settings
- Configure API application settings
- Access the operator audit trail
- View geocoding summary and logs
- Enable the SMS Opt-in service URL

User settings

- Grant external operator permissions
- Revoke operator permissions
- Configure distribution list folders
- Configure user attribute settings
- Translate custom user attributes
- Configure user authentication
- Configure SMS Opt-in

Map settings

- Manage map settings
- Set default map view
- Add shape layer
- Add distribution list

Device settings

- Configure device settings
- Configure mass device endpoints
- Configure desktop app settings

Device Manager

- Access the device manager
- View device details
- Enable and disable devices
- Edit devices
- Copy devices
- Delete devices
- Set device delivery preference
- Update device name

BlackBerry AtHoc Customer Support Portal

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

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

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

Documentation feedback

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

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

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

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada