



BlackBerry AtHoc

Enterprise Planning and Management Guide

7.9

Contents

- Getting Started..... 5**

- Enterprise management overview..... 6**
 - What is an enterprise configuration?..... 6
 - Single organization configuration..... 6
 - Enterprise configuration..... 7
 - Does enterprise solve my problems?..... 8
 - When should I use an enterprise configuration?..... 9
 - What can I do in the enterprise?..... 10
 - Enterprise user management..... 10
 - Enterprise publishing..... 10
 - AtHoc Connect for peer-to-peer organization alerts..... 11
 - Manage common content with inheritance..... 11

- Create an enterprise hierarchy..... 13**
 - Best practices for creating an enterprise hierarchy..... 13
 - Create and configure the enterprise..... 14
 - Create an enterprise organization..... 14
 - Create a suborganization..... 14

- Migrate existing organizations to an enterprise..... 15**
 - Best practices for migrating to an enterprise organization..... 15
 - Prepare to migrate..... 15
 - Run the Enterprise Migrator tool..... 16
 - Migrate organizations to the enterprise..... 16
 - Promote user attributes and alert folders..... 17

- Manage users in the enterprise..... 18**
 - Enable enterprise features..... 18
 - Enable user uniqueness..... 18
 - Move users in an enterprise organization..... 19
 - Move users from the management console..... 19
 - Move users with a .csv file..... 20
 - View and manage user accounts..... 20
 - Create enterprise distribution lists..... 21

- Manage roles and permissions..... 23**
 - Create the enterprise administrator..... 23
 - Assign operator permissions for the enterprise..... 24
 - Restrict the operator user base..... 24
 - BlackBerry AtHoc roles..... 24

Manage alerts..... 26
 Publish to the entire enterprise.....26
 Publish alerts to a subset of the enterprise..... 26
 Target by advanced query.....27
 Target by distribution list..... 27

Inherited content and settings in the enterprise..... 29
 Available reports in the enterprise.....29

BlackBerry AtHoc Customer Support Portal..... 31

Legal notice..... 32

Getting Started

This *BlackBerry AtHoc Enterprise Planning and Management Guide* contains information about enterprise concepts, uses, planning, and implementation. It assumes you have detailed knowledge of the BlackBerry AtHoc management system, including implementation, user management, and alert management for stand-alone organization configurations.

To learn about the BlackBerry AtHoc management system, see the BlackBerry AtHoc user guides available at: <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc>.

Enterprise management overview

You can use the enterprise configuration in BlackBerry AtHoc to manage alerts for a large, complex group of users. Using the enterprise configuration, you can delegate alerting to the organizations, while you maintain critical, unified alerting policies and processes for the enterprise and its members.

This document discusses the basics of BlackBerry AtHoc enterprise configuration and explains how to plan and implement one.

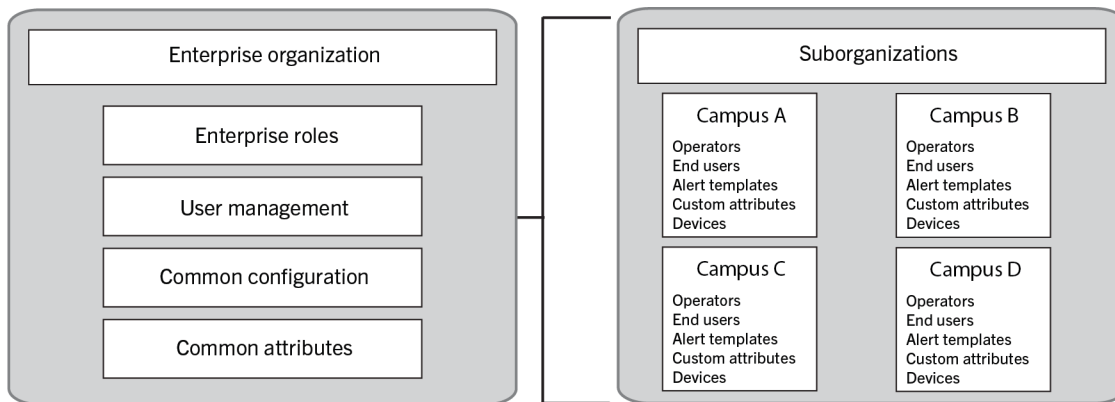
The following topics are covered:

- Enterprise concepts and benefits
- The differences between using an enterprise or stand-alone configuration
- Integration of AtHoc Connect to improve communication between organizations inside or outside the enterprise
- Tips for migrating your existing organizations to an enterprise configuration or creating an enterprise from scratch
- Enterprise role and permissions management
- User management for enterprise configurations
- Alert publishing in the enterprise

What is an enterprise configuration?

An enterprise configuration is a set of BlackBerry AtHoc organizations in one system that are managed by a single parent organization called the enterprise organization.

The enterprise organization centralizes the user, content, and policy management of its suborganizations.



User accounts are created in suborganizations, but the enterprise provides a higher-level view. The enterprise also manages common content such as user attributes, alert folders, audio files, and delivery templates.

The enterprise configuration uses a hierarchy to control the flow of information and centralize management tasks for organizations in the same system. The enterprise organization has one or more suborganizations that are defined by location or purpose. The suborganizations inherit certain configuration settings from the enterprise organization, while the enterprise manages users and provides a way to send alerts to multiple organizations across the enterprise.

Single organization configuration

Many BlackBerry AtHoc customers have found that their configurations are becoming too complex.

A single organization configuration can become unwieldy, with distribution lists and user accounts that are difficult to manage and synchronize as users come and go or business units change. Users suffer from too many alerts or fail to get any at all. Additionally, operators can find it difficult to use the Connect network effectively, especially if they are separated geographically. While each location would like to connect with certain neighboring agencies or companies, local alerts from these neighbors show up in everyone's inbox, at times creating an information overload.

Example A

A federal agency has developed one very large organization. Thousands of end users are targeted for various alerts ranging from daily status, emergency drills, or live emergencies. Despite having a flexible system, complex configurations make it difficult to ensure that operators have the correct permission to target only the people they should.

This agency can use the enterprise configuration to better organize personnel into smaller organizations with local administrators to manage user permissions and contact information.

Multiple organizations are great for many sites or regions, can have unique configurations for a location, delegate user management to organization administrators, and can separate distinct functions. However, using multiple organizations loses the benefit of a consolidated view of your operations. It is more difficult to have consistent and centralized communication across all organizations. Independent organizations are harder to maintain, require duplicate configuration effort, and do not have a good way to communicate with each other. Additionally, maintaining consistent user attributes, templates, and distribution lists is impossible because too much customization is occurring in each organization. Finally, individual organizations can communicate using Connect, but there is no easy way to communicate across all organizations, or with subsets of an organization.

Example B

A military organization has many bases around the world. The organization has created one organization for each base, which has thousands of personnel with rotating assignments and changing permissions (best managed by local administrators). However, with over 50 bases and hundreds of thousands of personnel, the senior leadership cannot effectively alert all bases in a consistent way or alert just the required subset of each base (such as by function). They can not determine, from a single view, who is available and where they are located.

During a major emergency, this military branch cannot account for personnel, send alerts to multiple bases at once, or effectively manage distribution lists that need to span organizations. They need a consistent way to target personnel across all organizations in the system and for those personnel to provide their location and status.

Enterprise configuration

To help large organizations, BlackBerry AtHoc provides the enterprise configuration. Enterprise configuration centralizes communication for multiple organizations, while using inheritance to provide consistent policies and procedures. Alerts can be sent from the enterprise organization to all organizations or subsets of suborganizations.

The enterprise configuration works with AtHoc Connect, allowing suborganizations to communicate with each other and outside organizations, such as vendors or community agencies.

Customers that have a standalone organization with too many users and distribution lists can create multiple suborganizations based on common alerting needs. The enterprise configuration allows you to delegate user management to local organizations, while maintaining the centralized control and communication that the single organization provided.

Example A

A federal agency with an unwieldy single organization can migrate to an enterprise configuration by breaking the large organization into small organizations that represent each geographical location. With multiple locations, the federal agency creates an organization for each alerting region, while retaining the ability to alert all users.

The federal agency also has manageable user bases that operators can maintain locally. The smaller suborganizations makes it easier to manage user contact information and distributions lists. Each suborganization can use AtHoc Connect to communicate with each other or to invite local vendors and community agencies to join AtHoc Connect without impacting the larger enterprise with connect requests and incoming alerts.

With an enterprise configuration, customers that have multiple organizations can have a virtual view of all personnel and consolidate and centralize communication and alert consistency. Enterprises can keep the benefit of multiple organizations, such as user management at the local suborganization.

Example B

A military branch has over 50 organizations, one for each base. To migrate to an enterprise configuration, they implement the following changes:

- They migrate to a configuration that uses three enterprise organizations, one for each continent on which they have bases. They use three enterprises because the emergency alerting for each continent is managed by a different team of people and each continent has different configuration needs.
- All enterprises are in the same system, so that any common content in System Setup can be inherited by the enterprise organizations.
- For each enterprise, they have about five enterprise administrators (EA) and 10 enterprise operators (EO) who can publish alerts to all or parts of the enterprise. At least one EO can access each of the three enterprises.
- Each enterprise organization has suborganizations for each base on that continent.
- Operators can create customized common content for bases on each continent (such as content in additional languages) at the enterprise level. Suborganizations inherit the common content.

Alerts can be sent from the enterprise organization, while personnel in the system can be accounted for by tracking responses to alerts.

The consolidated view provides the leadership with useful personnel accountability information for each continent from their respective enterprise.

Each suborganization can use AtHoc Connect to communicate with their peer suborganizations and affiliates of the organization such as vendors and local governments.

If there is a hurricane on the East coast of the U.S., they can publish alerts to only the appropriate North American alerting regions and ask for responses to check on personnel location, safety status, and availability to assist with recovery. Each base can then alert their Connect affiliates and assess their status.

Does enterprise solve my problems?

The hierarchy enables the enterprise to delegate user management, while maintaining critical unified alerting policies and processes. The enterprise configuration answers the following questions for many customers:

Question	Answer
Can I have a single user interface for managing all of my users?	<p>Yes you can perform the following types of management from the enterprise organization:</p> <ul style="list-style-type: none"> • Manage user accounts • Filter and search • Create enterprise distribution lists • Create reports

Question	Answer
Can I manage operators across my entire system efficiently?	Yes, you can create enterprise operators that have permission to publish alerts to all or parts of the enterprise. You can also limit the ability of operators to publish to only their local organization.
Can I overcome cumbersome cascading configurations for communicating with other organization or outside affiliates?	Yes, you can use AtHoc Connect at the suborganization level for peer-to-peer alerting or for connecting with outside affiliates.
Can my users in one suborganization move to another organization efficiently?	Yes, you can set the "Enterprise Features" flag in the General Settings of the enterprise organization to enforce uniqueness of users in the enterprise and suborganizations. This enables users to move between suborganizations using the same Self Service URL, login credentials, and the same organization code in the BlackBerry AtHoc Desktop App.

When should I use an enterprise configuration?

Planning your configuration is essential whether you are a small or large organization. You must consider which user roles, security policies, user base size, and content are common to all organizations and whether they need to be centralized by using enterprise alerting, user, and content management.

Enterprise configurations are generally for large, complex implementations with multiple locations that need to segment end users. Small groups find it easier to manage user bases with one or more standalone organizations. The following table compares the use of a standalone organization, multiple standalone organizations, and enterprises with suborganizations.

Setup	Standalone organization	Multiple standalone organizations	Enterprise with suborganizations
Advantages	<ul style="list-style-type: none"> • Best for one geographic site • Lowest up-front cost • One-time configuration of common content and settings • Import users once 	<ul style="list-style-type: none"> • Best for multiple sites or regions • Delegate user management to administrators • Unique configurations by location • Distinct operations per site • Works with AtHoc Connect 	<ul style="list-style-type: none"> • Shared configuration between organizations • Centralized user views • Alerting of enterprise users • All the benefits of multiple organizations • Works with AtHoc Connect

Setup	Standalone organization	Multiple standalone organizations	Enterprise with suborganizations
Disadvantages	<ul style="list-style-type: none"> • Difficult to manage operator permissions • Hard to separate team operations • Harder to implement AtHoc Connect effectively 	<ul style="list-style-type: none"> • Hard to maintain multiple configurations and consistency • Requires duplicate effort for entity configuration and security policies • No central user management or alerting between peer organizations • Users that move between sites have to re-enter profile information • Hard to manage personnel accountability 	<ul style="list-style-type: none"> • Migration can be complex • Device configuration is not inherited • Some stand-alone features not available on the enterprise

What can I do in the enterprise?

Now that you've seen the primary pros and cons for standalone and enterprise organizations, let's delve more deeply into how things work in the enterprise organization.

Enterprise user management

The enterprise organization provides a central view of all users in the organization. The enterprise administrator manages users at the enterprise level, and is able to grant or revoke operator permissions to the enterprise, as well as create or modify any user account.

You can view all users on the Users screen when you are logged in to the enterprise organization. To identify which organization the user account was created in, you can add the Organization column. This column is based on the Enterprise attribute of the same name and exists only in the enterprise organization. To learn more about enterprise user management, see [Manage users in the enterprise](#) and [Manage roles and permissions](#).

Enterprise publishing

To help with consistency across organizations, users with any alert publishing roles for the enterprise organization can create and publish enterprise alert templates. When they are logged in to the enterprise organizations, users with alert publishing roles create the templates. Enterprise alert templates are most effective for targeting users in multiple suborganizations. Alert templates are not inherited by suborganizations.

Using enterprise attributes, the operator can create common dynamic distribution lists, custom alert responses, and reports. Creating the user attributes from the enterprise organization makes them available for publishing enterprise-wide alerts and ensures that operators in each suborganizations can also use them.

While logged into the enterprise organization, operators can [publish alerts](#) that target users from multiple suborganizations. Targeting works very similarly to stand-alone organizations, except that operators can see users in all suborganizations to which they have access. When filling out the user targeting section of the alert, the operator can select any user or group to which they have access through their user base. Use the "Organization" attribute for targeting users in suborganizations.

AtHoc Connect for peer-to-peer organization alerts

Enterprise is great for targeting users within the enterprise. However, AtHoc Connect is best for communication between suborganizations or outside entities, without targeting individuals. For example, if a site in the federal agency has an IT outage, they can alert other organizations and ask if they have been affected.

You might already be using AtHoc Connect to communicate with outside agencies. You can also enable alerting between organizations in the enterprise with AtHoc Connect. Each suborganization registers for AtHoc Connect and then invites the other organizations in the enterprise to join their network. Operators can then send alerts to their peer organizations, just like they would for outside agencies.

Note: You do not target individuals in another organization through AtHoc Connect. The other organization would need to set up incoming alert rules that publish an alert targeting an individual.

Manage common content with inheritance

One of the main advantages of an enterprise configuration is the ability to create common content or configuration settings in one place and push them down to subordinate organizations. This is known as "inheritance".

There are three levels of inheritance.

- **System:** This is the top level that is used for the entire BlackBerry AtHoc system, where a system is defined as a single installation of BlackBerry AtHoc accessed by a single URL. An example of a system user attribute is First Name. All users have the First Name attribute, no matter what organization or enterprise they belong to. System configuration is set in the System Setup (3) organization.
- **Enterprise:** This is the second level of inheritance, primarily used for content and settings that need to be the same across all suborganizations. An example is a user attribute called employeeID. By setting it at the enterprise level, the content is part of all user profiles that are in the organization managed by the enterprise.
- For Cloud configurations, content and settings are set in the enterprise, which allows the cloud to use multitenancy.
- **Suborganization:** This is the third level, primarily used for content that is specific to a single base or location. An example is the user attribute OptIn4Birthdays, which is used by only one organization.

Security policies are also frequently handled as common content, allowing them to be inherited so that consistent policies, procedures, and communication methods can be established across a system.

Example

The following example focuses on attributes, but it could apply equally well to any type of common content.

A federal agency has three organizations managed by a single enterprise. There are three tiers, including one called System Setup at the system level. The enterprise organization is named Fed_Agency_Enterprise and it has three suborganizations: East Coast, Mid-West, and West Coast.

The organizations have the following user attributes:

- *System Setup* has three user attributes that are available for the system, which includes all enterprise and suborganizations: `UserName`, `ID`, and `LastName`.
- *Fed_Agency_Enterprise* has three user attributes that are available for the enterprise and its suborganization: `Department`, `Location`, and `CPR-Trained`.
- The *East Coast* organization has a team that wants to track birthdays, so they have added an attribute called `OptIn4Birthdays`.

An operator in the suborganization can edit the value of an attribute for a user if the operator has access to the organization in which the user attribute was created.

- The system administrators on System Setup can access and edit user attributes created at the System level. In this example, they can target users through the `UserName`, `ID`, and `LastName` attributes. However, they cannot see any attributes defined at lower levels.
- The enterprise operators have more options. They can view and use all of the attributes inherited from the System level, plus publish, search, create reports, and edit the attributes created at that enterprise organization (`Department`, `Location`, and `CPR-Trained`).
- Operators in the suborganizations can use but not edit user attributes inherited from system and enterprise levels. These operators can also create, edit, and use user attributes for publishing to the local organization, but the operators do not have access to attributes from peer organizations. As a result, operators in the *East Coast* org can access and edit the `OptIn4Birthdays` user attribute, while none of the other suborganization operators or enterprise or system administrators can use the attribute.

For a list of entities that are inherited, [Inherited content and settings in the enterprise](#).

Create an enterprise hierarchy

Before starting to plan and implement your organization, make sure you read the following section on [Best Practices](#).

Important: For cloud configurations, BlackBerry AtHoc operations must create the enterprise hierarchy.

Best practices for creating an enterprise hierarchy

Consider the following recommendations when planning your implementation:


- Plan the number of suborganizations and how they will be organized.
 - Think about which operators need to send alerts to a group of users. An organization is a group of people that need to be alerted by a specific team of operators and is not always a reflection of the corporate organization structure.
 - Create an organization for each alerting region, such as military base, a campus or a hospital. The alerting regions are often organized by geography, but can also be organized by purpose such as Weather, Security, or Disaster Relief alerts.
 - Do not make the suborganizations too granular. For example, in a large corporation, create organizations by a site, a region, or a division. Do not create an organization for each department or team.
- Create end users and operators at the suborganization level, not the enterprise level. No user accounts should exist in the enterprise organization because it prevents sending alerts to user accounts in the enterprise unless they are enterprise alerts. If they are in a suborganization, they can get alerts from their location as well as any enterprise alerts. You can see all users from suborganizations from the enterprise organization so there is no reason to create any users at this level.
- Plan the user attributes and alert folders that should be created in the enterprise organization:
 - Using enterprise attributes and alert folders is a good way to enforce consistency for all suborganizations.
 - Think about situations in which you need to alert the entire enterprise. What attributes do you need to target all users in an alert? These attributes should be created at the enterprise level.
 - Attributes that are for only one suborganization should be created at the suborganization level.
 - Do not name a user attribute with the string "Organization." BlackBerry AtHoc provides an enterprise user attribute with this name that is used to identify the suborganization in which a user account is created.
- If you plan to create an organization for "headquarters", make it a suborganization. The enterprise organization should be used for managing the suborganizations only and should not have user accounts for headquarters personnel.
- Maintain unique email addresses for users across your suborganizations in order to provide end users with a single enterprise-wide organization code.
- Enable user uniqueness in the General Settings of the enterprise organization to enforce uniqueness in usernames and mapping IDs across the enterprise organization and all suborganizations. Having unique users allows you to:
 - Deploy a single desktop app for the enterprise that determines a user's suborganization based on their unique mapping ID.
 - Provide end users with a single Self Service URL that can be used at the suborganization or enterprise level.
 - Provide end users with a single enterprise-wide organization code that they can use to sign in to their suborganization client.

Create and configure the enterprise

1. Plan your configuration. See [Enterprise management overview](#) and [Best practices for creating an enterprise](#).
2. Log in to System Setup using the login values provided by BlackBerry AtHoc customer support.
3. Create an enterprise organization and suborganization.

Important: For cloud configurations, BlackBerry AtHoc operations must perform this step.


Create an enterprise organization

1. In the navigation bar, click .
2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click **New**.
4. Enter the name of the new enterprise organization.
5. Add your name as the first account and click **Save**.
6. In the navigation bar, click your username. Click **Change Organization**.
7. Select the new enterprise organization.
8. Optionally, configure the organization. For detailed instructions, see "Create and configure an organization" in the *BlackBerry AtHoc System Administrator User Guide*.
9. To create an additional enterprise organization, you can duplicate a peer-level organization. To duplicate the organization, go to the Organizations Manager, highlight the enterprise organization you created, and click **Duplicate**.

Create a suborganization

Prerequisite

Verify that you are logged in to the enterprise organization.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click **New**.
4. Enter the name of the new organization and click **Save**.
5. In the navigation bar, click your username. Click **Change Organization**.
6. Select the new organization.
7. (Optional or save for later) Configure the organization. For detailed instructions, see "Create and configure an organization" in the *BlackBerry AtHoc System Administrator User Guide*.
8. After you configure the new organization, you can duplicate a peer-level organization. To duplicate the organization, open the Organizations Manager, highlight an organization, and click **Duplicate**.

Migrate existing organizations to an enterprise

After you upgrade to the latest release of BlackBerry AtHoc, you can migrate to an enterprise configuration.

Best practices for migrating to an enterprise organization

Consider the following recommendations when you plan your migration:

- Rename any existing user attribute with the name “Organization” to avoid conflicts. BlackBerry AtHoc provides an enterprise user attribute with this name for targeting users by organization.
- Plan the number of suborganizations and how they are organized.
 - Create a new enterprise organization rather than reuse a headquarters organization if there are existing users. Move the headquarters organization under the enterprise level.
 - Do not make the suborganizations too granular. For example, in a large corporation, create organizations by a site, a region, or a division. Do not create an organization for each department or team.
- Plan the promotion of attributes and alert folders. Content that is common among the existing organizations should be promoted:
 - Using enterprise attributes and alert folders is a good way to enforce consistency.
 - If more than one organization uses the same user attribute, the attribute should be promoted to the enterprise level.
 - If organizations use different values for the same user attribute being promoted, all values are promoted to the enterprise level.
 - Think about situations in which you need to alert the entire enterprise. What attributes do you need to target all users in an alert? These attributes should be promoted to the enterprise level.
 - Attributes that are for only one suborganization should stay at the suborganization level.
 - The “Emergency Community” and “Organization Hierarchy” attributes are not available for targeting in the enterprise organization.
- Create all user accounts at the suborganization level, not at the enterprise level.
- Authorized administrators can manage suborganization accounts from the enterprise organization.

Prepare to migrate

Important: For Cloud configurations, BlackBerry AtHoc operations must perform the following steps.

Use the Enterprise Migrator tool to move your existing organizations to an enterprise configuration.

Important: Plan your hierarchy before you use the tool. After you save your changes, you cannot change the hierarchy.

Prerequisite: Before you run the tool, create an organization that will be the enterprise organization. Existing organizations likely have users and have been used for local alerting. Instead of re-purposing an organization for the enterprise, create an empty organization. This method allows current organizations to continue operations without interruption and enables you to start with a clean enterprise organization.

Using the migration tool, you will specify the new organization to be the enterprise organization. You then move other organizations under the enterprise. These organizations become subordinate to the enterprise.

- The Enterprise Migrator tool migrates existing operators that have an enterprise administrator role in a suborganization to organization administrator. Other operator permissions remain unchanged.

- When you move an organization into the enterprise organization, the AtHoc Connect relationships and user accounts remain unchanged for the organization.

Run the Enterprise Migrator tool

Run the Enterprise Migrator tool to move standalone organizations under an enterprise organization. You can also promote attributes and alert folders from suborganizations to the enterprise or system level.

1. Log in to the BlackBerry AtHoc server and change to the following directory:

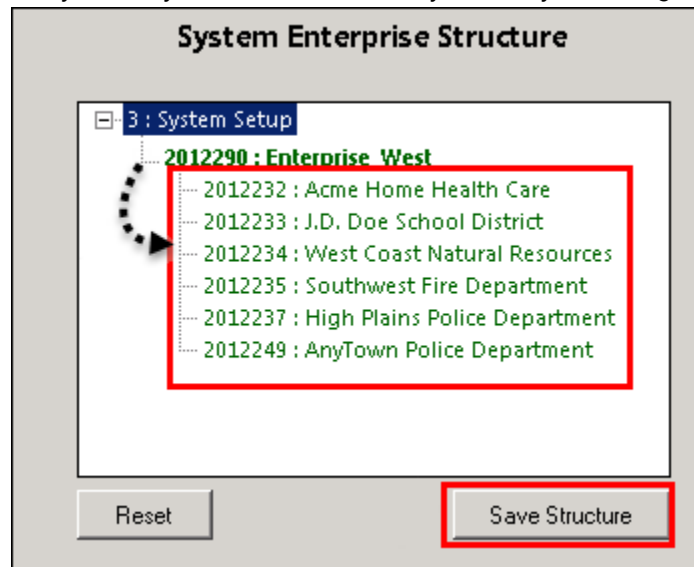
```
..\AtHocENS\ServerObjects\Tools
```

2. Locate the following file: `EAMigrator.exe`.
3. Right-click the file and select **Run as Administrator**.

Migrate organizations to the enterprise

The Enterprise Migrator tool displays the organizations currently in your BlackBerry AtHoc system. By default, new organizations that are created in the system are listed under the System Setup node. These are standalone organizations. You can move them under an enterprise organization to become a suborganization. If an organization is missing, it likely has an incorrect organization type, such as "draft."

Prerequisite: Plan your hierarchy before you use the tool. After you save your changes you cannot change them.

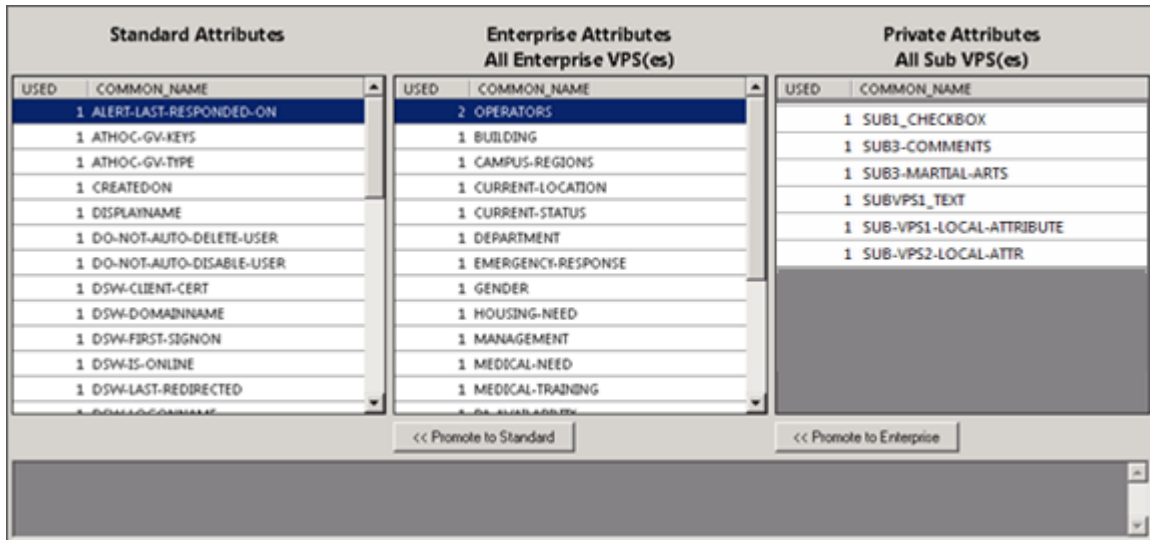


1. In the first column of the Enterprise Migrator, drag and drop any organization under another organization to specify the enterprise and suborganization levels. For example, the following image shows seven organizations. When the tool opens, all are considered standalone organizations. Six organizations have been dragged under Enterprise West, migrating them to suborganizations.
2. Verify your structure carefully. You cannot undo the next step.
3. Click **Save Structure**.

Promote user attributes and alert folders

During migration, you specify at which level the user attributes and alert folders are defined: system, enterprise, or suborganization level. If only a small group of users in a suborganization needs access to an attribute, it should be handled locally. However, for commonly used attributes or alert folders, the system or enterprise level is the typical location.

1. Open the Enterprise Migrator tool and click **User Attributes**.
2. Determine how many instances there are of an attribute at the suborganization and enterprise organization level and promote if it seems efficient. If you promote an attribute to the enterprise level, it is promoted from the suborganizations within the enterprise.



3. Select the attribute name.
4. Verify that you want to promote the attribute. You cannot undo the next step.
5. Click **Promote to Enterprise** to move the attribute up to a higher level.

Promote an attribute from suborganization to enterprise if the entire enterprise needs to use the attribute. Keep the attribute at suborganization if you want to restrict access to a single organization. For example, promote a general attribute like `DepartmentName` to enterprise because each employee needs to be grouped in a department. Alternatively, keep an attribute like `SoftballTeam` at the suborganization because its members have joined a lunch-time league.

6. Click **Alert Folders** button.
7. Select an alert folder type to promote, and click **Promote to Enterprise** based on what types of alerts certain personnel should see.

For example, promote an alert folder such as `FireDrills` from suborganization to enterprise if the entire enterprise needs to receive alerts from that alert folder. Keep an alert folder such as `ExecutiveSafety` at suborganization if you want to restrict access to operators and users that have a need to know.

8. Save your changes.
9. Restart IIS after you have made structure or content changes.

You have completed the migration to the enterprise.

Postrequisite

Grant permissions to the enterprise for the enterprise administrator for access to the suborganizations. Next, grant enterprise access to operators that need to publish alerts across the enterprise.

Manage users in the enterprise

The enterprise configuration provides centralized user management for all suborganizations under the enterprise organization. The enterprise organization shows a virtual view of users in all suborganizations. Using the virtual view, you can perform most of the operations as if the user accounts were actually created in the enterprise.

Enable enterprise features


You can manage user accounts from the enterprise organization or from a suborganization if user uniqueness is enforced in your enterprise. When uniqueness is enforced, the system checks for uniqueness of usernames and mapping IDs in the enterprise organization and suborganizations when a new user is created from the BlackBerry AtHocDesktop App, Self Service, SDK, or through the BlackBerry AtHoc management console. When user uniqueness is enforced the following items are enabled:

- A single enterprise Desktop App: Set up the Desktop App to connect to the enterprise. The Desktop App will then search for users across the enterprise and connect to the correct suborganization. If the user is not found, a new user is created in the enterprise.
- A single enterprise Self Service URL: Users in any suborganization can log in using the same Self Service URL for the enterprise organization or suborganization.
- Mobile registration from an enterprise organization code: Users can register from their mobile device using the organization code for the enterprise or for any suborganization.
- Enterprise user import and export: Users can be imported into any suborganization directly from the enterprise organization. Users from suborganizations can be exported from the enterprise.
- User move: Users can be moved from one suborganization to another. You can move users between suborganizations through the Users page in the management console, or through the import process.
- Subscribed organizations: Users can subscribe to multiple suborganizations in an enterprise organization. Once subscribed, users can receive alerts and events targeted to them in both their home and in their subscribed organizations.

For more information, see the *BlackBerry AtHoc Enterprise Features User Guide*.

Note: Unique email addresses are not enforced in the BlackBerry AtHoc system when user uniqueness is enabled. However, it is a best practice to have a unique email address for each user in your enterprise and suborganizations.

Enable user uniqueness

1. In the navigation bar, click .
2. In the **Basic** section, click **General Settings**.
3. In the **Enterprise Features** section, click **Check Readiness** beside Enterprise Features. The system checks for user uniqueness (no users have the same username or mapping ID).

If the system finds duplicate users, the Duplicate Users Found window opens and provides a list of duplicate users, their usernames, mapping IDs, and organizations. You must modify any duplicate usernames or mapping IDs to proceed with enabling user uniqueness.

Click **Export to Excel** to download and save the list of duplicate users. After you update the duplicate users, run the duplicate user check again. If no duplicate users are found, a Check Passed message displays. Click **Close** to return to the General Settings page. The Check Readiness button is replaced by an Enable check box.

4. Select **Enable**.
5. Click **Save**.

Move users in an enterprise organization

The Enterprise User Move feature enables operators in an enterprise organization to easily move users between the different organizations in their enterprise. An enterprise operator with Enterprise User Manager permissions can move users from the enterprise organization to any suborganization, from one suborganization to another, or from a suborganization to the enterprise organization. Enterprise operators can import users at the enterprise level, and then move them into the appropriate suborganization.

Users must be unique across the enterprise and all suborganizations to use the enterprise user move feature. See [Enable enterprise features](#) for more information.

When a user is moved from an organization, any roles they had in their original organization are revoked. If a user is later moved back to their original organization, the user's roles are not reinstated. The one exception is for users in the enterprise organization with the enterprise administrator role.

The history of moved users is preserved. Sent alert reports still display all targeted users that were in the organization at the time the alert was sent.

The status of a user in their original organization (enabled or disabled) is preserved after being moved.

The attribute values for users (for example, personal device addresses) are preserved after being moved, even if those devices or attributes are not enabled in the new organization.

Once a user is moved out of an organization, they can no longer be targeted in any alerts, including draft or scheduled alerts, from that organization.

If you want to prevent users from being moved between organizations after you have manually moved them either through the management console or by using the CSV import process, set the Prevent User Move attribute for those users. This is useful if you want to prevent users from being moved by an external synchronization source such as LDAP or ADSync.

Move users from the management console

Enterprise operators with enterprise administrator permissions can move users between their enterprise and suborganizations using the BlackBerry AtHoc management console. You can move up to 1000 users at a time.

User uniqueness must be enabled before you can move users between organizations. For more information, see [Enable enterprise features](#).

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check box next to the users that you want to move.
4. Click **More Actions > Move**. The Move Users window opens.
5. Select an organization from the **Organization** list.

If any users you are moving have the Prevent User Move attribute enabled, the **Move locked users** check box appears and is selected by default. When selected, the Move locked users check box allows users to be moved regardless of whether the Prevent User Move attribute has been set.

The **Lock all users after move** check box is selected by default. When selected, the Lock all users after move check box adds the Prevent User Move attribute to all moved users. This is useful to prevent any external synchronization sources from moving the users.

6. Click **Move**.

The selected users are moved to the selected organization. Any roles that the users had in their original organization are revoked. Users in an enterprise organization with the enterprise administrator role retain this role.

Move users with a .csv file

Operators with enterprise administrator permissions can use the import and export process to move large groups of users between their enterprise and suborganizations.

User uniqueness must be enabled before you can move users between organizations. For more information, see [Enable enterprise features](#).

1. In the navigation bar, click **Users**.
2. Click **Users**.
3. Select the check boxes next to the users that you want to move.
4. Click **More Actions > Export**.
5. On the **Export Users** window, use the **Add >** button to select the Organization and Prevent User Move columns.
6. Use the **Add >** button to select any additional columns that you want to include in the export file.
7. Click **Export CSV**.
8. Save the .csv file to your local system.
9. Open the .csv file on your local system.
10. Update the Organization column for any users you want to move. You can also add rows to include new users and specify the organization you want to add them to.
11. Update the Prevent User Move column. Enter **Yes** for all users to block them from being moved to another organization. Enter **No** to unblock users if they already have the Prevent User Move attribute set.
Note: When creating users, the Prevent User Move check box is set and the user is created. If a user is already in an organization, the Prevent User Move attribute is respected upon import. You cannot move and then prevent a future move in the same import action when moving users with the .csv import process.
12. Save the updated .csv file.
13. In the BlackBerry AtHoc management console, click **Back** to return to the user management screen.
14. Click **More Actions > Import**.
15. Click **Browse** button and navigate to the updated .csv file on your local system.
16. Verify that the Organization and Prevent User Moves columns are selected in the **Select the columns to import** window.
17. Click **Import**.

When the import process completes, you can select the **Download Log** link to view the results.

View and manage user accounts

You can manage user accounts from the enterprise organization or from a suborganization.

From the enterprise organization users list

An enterprise administrator can perform many of the user management tasks that you can from a stand-alone or suborganization:

- View and update user accounts from any suborganization
- Use search and filter to find user accounts from any suborganization
- Add or change roles to any user, such as adding enterprise operator roles
- Restrict the user base of an operator at the enterprise or suborganization
- Create static and dynamic distribution lists across multiple organizations
- Delete or disable user accounts in the enterprise

From the sub organization users list

The following user management tasks that need to be performed in the suborganization:

- Create user accounts
- Add an operator role for a specific suborganization
- Import users when you create a new organization

Create enterprise distribution lists

When you plan your alerting strategies, you need to identify groups of users to alert across the enterprise and create distribution lists that target the right constituencies. Distribution lists help the operator send an alert quickly under stressful conditions, reducing the risk of targeting the wrong recipients.

You can populate the distribution list with a static list of users or create a dynamic list based on attributes or queries that are flexible enough to handle changes within the enterprise.

Distribution Lists are not inherited by suborganizations.

- Use static distribution lists when the group is small or very stable, or when certain people (instead of roles) must receive alerts.
- Use dynamic distribution lists when there are large groups that need to be targeted, or when personnel frequently change roles.

Tip: Use the `Organization` attribute to search for users across multiple organizations when creating static distribution lists. You can also use this attribute in an advanced query when creating dynamic lists.

Create enterprise static distribution lists

Create a static distribution list by completing the following steps:

1. Log in as an Enterprise operator on the Enterprise organization.
2. Create a static distribution and provide a name that signals that it is Enterprise-wide, such as `Ent-SeniorStaff`.
3. Build the list of users in the **Distribution List Members** section of the screen.
 - a. Click the **Modify** link to add users to the list.

Note: If your user base has been restricted, the user list shows only those users in your user base.
 - b. Select users from the list. Use the Organizations column to determine which organizations users belong to.
 - c. Click **Add Selected** to save the users you selected to the distribution list.
4. Click **Save** to create the list.

Create enterprise dynamic distribution lists

Create a dynamic distribution list to target users in multiple organizations. Personnel changes can impact a list, so use a condition to target users that meet the criteria, instead of selecting individual users that might move out of the organization.

You can use the enterprise `Organization`, to select users based on the organization that they belong to.

1. Create a dynamic distribution list from the enterprise organization and provide a name that signals that the list is enterprise-wide, such as `Ent-SeniorStaff`.
2. In the **Distribution List Members** section, click **Edit**.
3. In the **Select Attribute** list, select an enterprise attribute to use as targeting criteria for the distribution list.

An enterprise attribute is defined at the enterprise organization level and inherited by suborganizations.

4. In the **Select Operator** list, select the query operator needed for the condition, such as `equals`.

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

5. In the third field, enter a value, or select one or more of the available values for the attribute.
6. When you have finished adding conditions, click **Add** to add the criteria to the dynamic list.

7. Click **Save**.

Manage roles and permissions

BlackBerry AtHoc roles are the same in the enterprise, with a few exceptions.

Define user accounts in suborganizations, and then grant them access from the enterprise organization.

The **enterprise administrator** is an operator role that creates and manages the member organizations and common content. Typically, there are 2–5 operators with this role in the enterprise, depending on the size of your organization. The enterprise administrator also grants operator access to the enterprise and specifies the user base for each enterprise operator.

Note: The operator account for the enterprise administrator exists in a suborganization, but the System administrator (or another enterprise administrator) grants the appropriate roles from the Users Manager in the enterprise organization.

The enterprise administrator role provides full permissions for the enterprise organization and for all suborganizations. The enterprise administrator role is granted to an operator account from one of the suborganizations.

An **enterprise operator** is an operator with any BlackBerry AtHoc role except the administrator roles. For example, when assigned the Advanced Alert Publisher role at the enterprise level, an operator can send alerts to users and distribution lists across the enterprise, based on their user base definition.

The enterprise operator can target users in multiple member organizations, based on a system or custom user attribute. They can also use a static distribution list with members from across multiple suborganizations. Or, the operator can use a dynamic distribution list (with a common attribute such as dept='IT') to target members in multiple organizations.

Some or all suborganizations might have enterprise operators, depending on which operators need to alert the enterprise.

Note: The operator account exists in a suborganization, but the enterprise administrator grants the appropriate roles from the Users Manager in the enterprise organization.

For detailed information about BlackBerry AtHoc roles, see [BlackBerry AtHoc roles](#).

Create the enterprise administrator

Best Practice: Do not create any user accounts in the enterprise organization.

1. Log in to the BlackBerry AtHoc management system as a system or enterprise administrator, and change to the suborganization.
2. Optionally, change to the appropriate suborganization and then create a new user, if needed.
3. Change to the enterprise organization and then open an existing user account from the Users list.
4. Grant the enterprise administration role for the user.
 - a. From the user details screen, click **Modify Operator Permissions**.
 - b. On the **Operator Permissions** screen, click **Operator Roles**.
 - c. Select the **Enterprise Administrator** role.

Note: Granting the enterprise administrator role gives the user full administrator permissions to all member organizations.

5. When needed, enter a password for the operator.
6. Click **Save**.

Assign operator permissions for the enterprise

Grant enterprise publishing roles for any operator that needs to send alerts to users in more than one organization. The role is granted to an operator account existing in one of the suborganizations.

1. Log in to the BlackBerry AtHoc management system as a system or enterprise administrator, and change to the suborganization.
2. Optionally, change to the appropriate suborganization and create a new user, if needed.
3. Change to the enterprise organization and open an existing user account from the Users list.
4. Grant roles for the user to specify their permissions within the enterprise.
 - a. From the user details screen, click **Modify Operator Permissions**.
 - b. On the **Operator Permissions** screen, click **Operator Roles**.
 - c. Click to select each of the roles you want to assign to the enterprise operator.

You can grant any available role, such as advanced alert manager or alert publisher. These roles provide the same access to the enterprise, as they do on a standalone or suborganization

- d. To remove an operator permission, click **X** next to the role name.

Tip: Specify a user base for the operator to limit their access to specific groups of users.

Restrict the operator user base

Your security policies might require that you limit enterprise operator access by the type of distribution lists, organization, or seniority of an end user. Use User Base definitions to define these restrictions for the operator.

1. From the operator profile, under **User Base**, select **Restricted** and click **Modify**.

The Create Conditions screen opens. You can create conditions (queries) that target users in more than one member organization of the enterprise. The conditions use enterprise attributes that are inherited at the member organization level.

- a. In the **Select Attribute** field, click the down arrow to select an attribute.
- b. Select an operator, such as `equals`, `not equals`, or `is empty`.
- c. Specify the values that either include or exclude users based on the chosen attribute.

Note: The `Organization` attribute targets users in specific member organizations.

For example, if the manager of the IT engineers across the enterprise should only be able to send alerts to their personnel, restrict their user base with the condition `Department equals IT`.

Or, if an enterprise operator should only be able to publish alerts to organizations in the United States, specify the `EastCoast`, `MidWest`, and `WestCoast` values for the `Organization` attribute.

2. When needed, enter a password for the operator.
3. Click **Save**.

BlackBerry AtHoc roles

The enterprise administrator, organization administrator, or system administrator must grant operator permissions to any user who needs access to the BlackBerry AtHoc management system. The act of 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 user manager and alert publisher.

The role to which a user is assigned determines what BlackBerry AtHoc features they can access.

For more information, see "BlackBerry AtHoc roles" in the BlackBerry AtHoc *Manage Operators and Administrators Guide* and the *BlackBerry AtHoc Roles and Permissions Matrix* available at: <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc>.

Manage alerts

Enterprise operators can publish alerts across the enterprise, either to the entire group or to subsets based on attributes or user base restrictions. To publish an enterprise alert, you must meet the following prerequisites:

- Must be logged into the enterprise
- Must have enterprise operator permission
- Must use an alert template created at the enterprise level
- Optional: Must have enterprise user attributes and alert folders that can be used to target users

You can create enterprise user attributes for each user segment that must be targeted. For example, if you need to publish alerts to the IT departments across the organization, create a Department attribute, with a pick list that includes the value `IT`.

Role Permissions: You must have enterprise administrator role or operator permissions on the enterprise organization to complete the tasks in the following sections.

Publish to the entire enterprise

Targeting the enterprise assumes that you want to contact all users in all suborganizations of the enterprise. This type of alert should be a rare event, especially if you have multiple organizations that are separated by geography or function.

Best Practice: Target the smallest group of users necessary. Done too frequently, publishing an alert to the full user base will be considered spamming and users will ignore the alerts that are urgent.

Prerequisites

- Verify that devices and gateways are enabled for all targeted devices and gateways in the enterprise organization.
 - Verify that you have alerting operator permissions on the enterprise with an unlimited user base.
1. Log in and switch to the enterprise organization.
 2. Create or open an enterprise alert template or blank alert.
 3. Enter the alert title and content.
 4. In the Targeting section, select the **By Groups** tab and select **All User Base**.
 5. Select the devices that you need for reaching as many users as possible. Include mass devices to extend coverage to users that are out of range of other targeted devices.

You can use the devices, gateways, and delivery templates that are enabled for the enterprise.

6. Review the alert:
 - Ensure that the content provides critical and relevant information to the majority of recipients.
 - Check the spelling and the accuracy of the content.
 - Verify that the device coverage reaches enough users.
7. Publish the alert.

Publish alerts to a subset of the enterprise

Typically, when you send an enterprise-level alert, you want to limit it to those sub groups for whom the alert is relevant. For example, if you have an enterprise with multiple locations in the United States, and you need to

send an alert only to users on the East Coast, you would not include those in the West Coast or the Mid West organizations

Tip: When users frequently receive irrelevant alerts, they begin viewing all alerts as spam and ignore or block them. Over-targeting on a regular basis becomes a serious issue when essential alerts are ignored.

You can target a subset of users by using user attributes that are defined in the enterprise organization, or by distributions lists.

For example, an enterprise operator sends out an alert to a subset of users in three member organizations. The operator can either use enterprise attributes, such as Office Building= "A, B, C" and Department = "IT", or a dynamic distribution list to target the IT staff in the three buildings on different campus locations in the region.

Target by advanced query

You can use user attributes in advanced queries to target users by department, location, skills, or status.

For example, enterprise operators in a federal agency can use the Department and OfficeBuilding enterprise attributes to target users by office building and department to alert IT personnel that there is an outage affecting three buildings.

1. Log in and switch to the enterprise organization.
2. Create or open an alert template, or create a blank alert.
3. Create the content.
4. To target by user attribute, click the **Advanced Query** tab.
5. Click **Add Condition**.
6. Create a condition (attribute, operator, and value) to target users that exist in the organizations that you must reach. The following image shows the conditions for our IT outage example.



The image shows a user interface for creating advanced queries. It consists of two rows of input fields. The first row has a dropdown menu with 'Office Building' selected, followed by a dropdown with 'equals', and a text input field containing 'A, B, C'. The second row has a dropdown menu with 'Department' selected, followed by a dropdown with 'equals', and a text input field containing 'IT'. Each row ends with a red minus sign icon, indicating that conditions can be added or removed.

7. Select the devices and any organizations that you need to include.
8. Review and publish the alert.

Target by distribution list

Enterprise distribution lists can include users in multiple organizations, as long as the creator has user base permission to access the user and the organization. Static and dynamic distribution lists provide a quick and efficient method for targeting multiple users across the enterprise.

For example, the enterprise operator can alert IT personnel in the federal agency suborganizations with an enterprise distribution list of just IT members.

Prerequisite: Distribution lists must exist in the enterprise organization and include members of the user base of the enterprise operator. These are users from organizations that the enterprise operator can access. For more information, see [Create enterprise distribution lists](#).

1. Log in and switch to the enterprise organization.
2. Create or open an alert template, or create a blank alert.
3. Specify the title and the content.
4. For targeting a subset of enterprise users, click the **By Groups** tab.
5. Click the **Distribution Lists** folder.
6. Select a distribution list that specifies the users in the organizations that you need to target.
7. Select the devices.

8. Ensure the devices are enabled in the organizations and that you are able to reach the users in the various organizations.
9. Review and publish the alert.

Inherited content and settings in the enterprise

The following objects can be defined at the enterprise organization, and inherited by each suborganization.

User attributes: You can find user attributes in the User Attributes section on the Settings screen.

- Attributes are inherited by lower-level organizations, except for Emergency Community and Organization Hierarchy, which exist at the suborganization level.
- Attributes defined at the system or enterprise can be viewed, but the only fields that can be modified are the Page Layout options. For the Page Layout options, you can decide whether the attribute appears on the Self Service My Profile page and the User Details page in the management system and if you opt to have it appear, you can decide how much information will be displayed: Basic Info, Physical Addresses, or Advanced Information.
- All aspects of attributes defined at your organization level can be modified with the exception of the attribute type and the organization the attribute is associated with.

Organization code: You can find the organization code in the Enterprise Features section on the General Settings screen.

Click **Check Readiness** beside Enterprise Features. The system checks for user uniqueness (no users have the same username or mapping ID). When the check passes, select the Enable check box next to the **Enterprise Features** field to enable enterprise aware mobile registration. When enabled, enterprise aware mobile registration enables users to sign on from a mobile device using the enterprise organization code, or the organization code for any suborganization.

Alert folders: You can configure alert folders in the Basic section on the Settings screen.

Security policies: You can configure security policies in the System Setup section on the Settings screen.

If you need to define unique security requirements for a suborganization, configure them in the Security Policy page for the suborganization, so that the change impacts only that suborganization.

Delivery templates for the BlackBerry AtHoc Desktop App: You can configure delivery templates for the desktop app in the Basic section on the Settings screen.

Audio files: You can configure audio files in the Basic section on the Settings screen.

Devices: You can configure devices in the Devices section of the Settings screen.

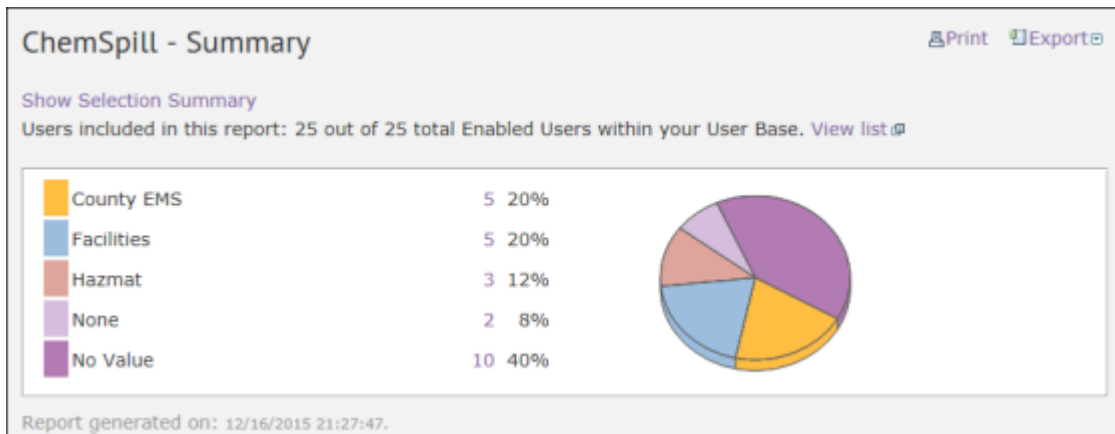
- Devices are defined at the system level using the Device Configuration Tool on the BlackBerry AtHoc server.
- Administrators can enable or disable a device for each suborganization.
- Administrators can specify whether the contact information for the device is required for each suborganization.

Available reports in the enterprise

You can create and review reports in the enterprise organization like you can in a standalone organization.

The following reports are available:

- **Personnel Reports:** This report is generated using enterprise user attributes; shows views of all enterprise personnel.



- **Alert Usage Summary:** This report shows the total number of alerts or messages, by organization, over time.

Alerts Usage Summary - Total Number of Alerts Over Time

Page 1 of 1

Organizations	Total	Dec 15	Nov 15	Oct 15
Acme Home Health Care (2012232)	0	0	0	0
AnyTown Police Department (2012249)	11	0	7	4
Enterprise_West (2012290)	2	0	2	0
High Plains Police Department (2012237)	6	0	4	2
J.D. Doe School District (2012233)	3	0	1	2
Southwest Fire Department (2012235)	4	0	4	0
West Coast Natural Resources (2012234)	5	0	3	2
Total	31	0	21	10

- **User Summary:** This report provides a count, by organization, of the number of enabled users.

User Summary

Page 1 of 1

Organizations	Enabled Users
Acme Home Health Care (2012232)	10
Enterprise_West (2012290)	7
High Plains Police Department (2012237)	8
J.D. Doe School District (2012233)	7
Southwest Fire Department (2012235)	3
West Coast Natural Resources (2012234)	2
Total	44

BlackBerry AtHoc 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