BlackBerry AtHoc

System Settings and Configuration

7.20

Contents

BlackBerry® AtHoc® set up and administration overview

Administrators create, configure, and manage the organization settings that operators use to communicate with their recipients as well as with other organizations. Setup includes configuring the features used by operators to communicate during situations. This guide covers the following administration tasks:

- The Configure BlackBerry AtHoc settings section describes how to configure the features provided by BlackBerry AtHoc to communicate and coordinate with teams and recipients during a crisis. The following topics are covered in this section:
  - Basic settings: Personalize your organization with a name, welcome or disclaimer text, and an icon. Enable and configure enterprise features, including user move and organization subscription. Map enterprise organizations to a super enterprise organization. Customize the time zone and time formats, create a security policy message, and control default page layouts. Configure settings for maps and external events.
  - Manage system settings: Configure the name, URL, time zone, database archive directory, system help desk information, support page content, redirection settings, client certificates, and disclaimers for your system.
  - Security policy settings: Define password rules and complexity, enforce system-wide password updates, set session timeout, limit active sessions, configure smart card authentication settings, and enable CAPTCHA validation.
  - Monitor system health: Create, view, edit, enable, disable, delete, and refresh system health monitors.
  - View the diagnostic log: Run basic and advanced searches of the diagnostic log.
  - View geolocation transactions and logs: View geocoding transactions and access their detailed logs.
  - Organizations Manager: Create organizations, enable and disable features, manage integrated device agents, provision applications for the web API, view the operator audit trail report and the alerts usage summary report. To create or migrate an existing set of organizations to an enterprise or to create a super enterprise organization, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.
  - Manage system jobs: View details about system jobs, create and export a system diagnostics report.
  - Configure device gateways: Configure the mobile app and AtHoc Cloud Delivery Service gateways.
  - Configure devices: Enable and disable devices, manage mass communication devices, configure giant voice devices, configure the AtHoc Connect organization network, manage the Cloud Services gateway, configure RSS and XML feed information and failover delivery gateways.
  - Configure desktop app settings: Select general desktop software options, customize the desktop client system tray, configure client server communications and failover settings, and set the desktop software authentication type.
- The Manage SMS Opt-In section describes how to configure and activate SMS Opt-In and how to create event codes.
- The Configure device gateways section describes how to configure settings for the BlackBerry AtHoc mobile app, and how to configure mobile phone notification.
- The Configure devices overview section describes how to enable and duplicate devices in BlackBerry AtHoc.
- The Configure devices section describes how to enable and disable devices, set device delivery priority, manage mass communication devices, and view and edit device details.

For information about creating and managing alert templates, specifying alert folders, managing delivery templates, and managing audio settings, see the *BlackBerry AtHoc Alert Templates* guide.

For information about managing settings for incoming alerts, see the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

For information about granting permissions for working with AtHoc Connect and updating sector visibility in the Connect profile, see the *BlackBerry AtHoc Connect* guide.

For information about settings related to users and user attributes, including creating, deleting, and editing user attributes and automatically disabling or deleting users based on attributes, see the *BlackBerry AtHoc Manage Users* guide.

Configure BlackBerry AtHoc settings

Important: To access the screens, features, and functions mentioned in this section, you must be a System Administrator, Enterprise Administrator, or Organization Administrator in the BlackBerry AtHoc organization. If you do not have these roles, many of the options on the Settings screen will be grayed out.

Users who have been granted administrator permissions in BlackBerry AtHoc can set up organizations and manage settings and users within an organization.

Basic settings

To configure basic settings, log in to the BlackBerry AtHoc management system as a System Administrator. In the navigation bar, click ⚙.

Section	Description	For more information
General Settings	Configure the settings for your organization, such as the name, logo, user layouts, and supported delivery languages.	General settings
Alert Placeholders	Insert custom text into predefined alerts.	"Placeholders for alert templates" in the *BlackBerry AtHoc Alert Templates* guide.
Accountability Templates	Manage predefined accountability events.	"Access the Accountability Templates screen" in the *BlackBerry AtHoc Account* guide.
Alert Templates	Manage predefined alerts.	"Alert template settings" in the *BlackBerry AtHoc Alert Templates* guide.
Alert Folders	Create and edit alert folders used to categorize alert templates.	"Configure alert folders" in the *BlackBerry AtHoc Alert Templates* guide.
Delivery Templates	Customize the look and feel of alert content for different device types.	"Access delivery templates" in the *BlackBerry AtHoc Alert Templates* guide.
Audio Files	Manage the audio files used in alerts.	"Manage audio files" in the *BlackBerry AtHoc Alert Templates* guide.
Mobile Alert Settings	Edit incoming mobile alert types, manage report categories, and associate alert templates with incoming mobile alerts.	"Configure mobile alert settings" in the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

Section	Description	For more information
Alert Rules	Create rules that associate a condition and an alert template, or action, with incoming alerts from other organizations.	"Manage alert rules" in the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.
Map Settings	Set map defaults and configure various map layers.	Map settings
External Events	Choose event types to gain situational awareness.	External events

General settings

You can use General Settings to customize settings for your organization, customize the time zone and time formats, enable enterprise features, and control default page layouts.

1. In the navigation bar, click ⚙.
2. On the **Settings** screen, in the **Basic** section, click **General Settings**.
3. On the **General Settings** screen, configure any of the following sections:
   - Organization Details
   - Enterprise Features
   - Customization
   - Dependents
   - Attachments
   - Layouts
4. Click **Save**.

Organization Details

The Organization Details section in General Settings contains the following prepopulated fields:

- The **Name** field displays the name of your organization.
- The **Organization Code** field serves as a short name used to register for Self Service and for the mobile app. The organization code must also be used in the URLs used to access Self Service and Single Sign-On (SSO). If not provided by a system administrator, the organization code is automatically generated from the organization name with spaces replaced with hyphens. You must have system administrator permissions to edit this field. The Organization Code field is mandatory.
- The **User Login** field displays the server address that users access to log in to Self Service.
- If Self Registration is enabled for the organization, the **Registration URL** field displays the server address that users access to register.

1. Optionally, enter a **Support Email** address.
2. Optionally, in the **Logo** field, click **Browse** to upload a graphic file you want to display in the top corner of each screen. The file type must be .gif, .jpg, or .png.
3. Optionally, in the **Logo Text** field, enter a text string of up to 100 characters that appears when users hover their cursors over the logo.
4. Click **Save**.

Enterprise Features

The Enterprise Features section in General Settings is available only for super enterprise organizations with sub enterprise organizations, and enterprise organizations with suborganizations.

1. On the **General Settings** page, scroll down to the **Enterprise Features** section.
2. Complete the steps described in the following sections to require user uniqueness, enable user initiated move, and select organizations for subscription as needed:
   - Enable enterprise features
   - Enable user move
   - Select organizations for subscription
3. Optionally, for super enterprise organizations only, Map enterprise organizations to a super enterprise.
4. Click **Save**.

Enable enterprise features

Enabling enterprise features in your enterprise or super enterprise organization enables the following items:

- **A single enterprise desktop app**: Set up the desktop client to connect to the enterprise or super enterprise. The desktop client then searches for users across the enterprise or super enterprise and connects to the correct suborganization. In an enterprise organization, if the user is not found, a new user is created in the enterprise. In a super enterprise organization, if the user is not found, a new user is created in the super enterprise.
- **A single enterprise Self Service URL**: In an enterprise organization, users in any suborganization can log in using the same Self Service URL for the enterprise organization or suborganization. In a super enterprise organization, users in any sub enterprise or suborganization across the super enterprise can log in using the same Self Service URL for the super enterprise, sub enterprises, and suborganizations.
- **Mobile registration from an enterprise organization code**: Users can register from their mobile device using the organization code for the super enterprise, enterprise, or any suborganization.
- **Enforcement of unique usernames and Mapping ID values for all users**: The system checks for uniqueness of usernames and mapping IDs in the super enterprise organization, enterprise organization or suborganizations when a new user is created through the desktop app, Self Service, CSV import, or the BlackBerry AtHoc management system.

1. Click **Check Readiness**. The system checks for user uniqueness (no users have the same username or mappingID). If the system finds duplicate users, the Duplicate Users Found window opens and provides a list of duplicate users, their usernames, mappingIDs, and organizations.
2. Modify any duplicate usernames or mappingIDs to proceed with enabling user uniqueness.
3. Run the duplicate user check again. If no duplicate users are found, a Check Passed message displays.
4. Click **Close** to return to the General Settings page. The Check Readiness button is replaced by an Enable check box.
5. Select the Enterprise Features **Enable** check box. The User Initiated Move check box appears.
6. Click **Save**.

Enable user move

If you have a large enterprise organization where users in your system need to move between organizations, you can enable the User Move feature. This reduces the burden on your administrators by enabling users to move themselves between the suborganizations of your enterprise organization in Self Service.

Enterprise Administrators can move users between suborganizations from the enterprise organization. Operators who are End Users Managers, Organization Administrators, Alert Managers, or Advanced Alert Managers in a suborganization can move and subscribe users from their suborganization to other suborganizations.

In a super enterprise organization, Enterprise Administrators can move users between sub enterprise organizations, between the suborganizations of those sub enterprises, from suborganizations to sub enterprises, and from the sub enterprises to suborganizations across the super enterprise.

When a user is moved to a different organization, their view of Self Service may change, depending on the settings of the organization they are moving to. If the user is an operator, any operator permissions they had in their original organization are revoked. If the user was an Enterprise Administrator in the super enterprise or enterprise organization, they retain this role in the suborganization they are moved to. If the user had roles and permissions in other organizations within the super enterprise, enterprise, or organizations outside of the enterprise organization, they are retained. If a user has dependents, those dependents are also moved.

When a user is moved, their position in the organizational hierarchy is removed. If the user is later moved back to their original organization, their place in the hierarchy is reinstated if the node still exists. However, if the node the user was associated with no longer exists in the original organization, the user is associated with the root node.

Prerequisites

- Require user uniqueness must be enabled.
- The User Move for End Users option must be enabled on each suborganization. In a super enterprise organization, the User Move for End Users option must be enabled on each sub enterprise and suborganization. This option can be set in the Customization > Self Service section in General Settings on the sub enterprise or suborganization. This option is enabled by default.

1. Select the User Move **Enable** check box. The Available Organizations list appears. The super enterprise, enterprise organizations and all suborganizations appear in the Available Organizations list.
2. Select the organizations that you want to be available for user move, or choose **Select All**. You can narrow the list of organizations by typing the name of an organization in the text box.
3. Click **Save**.

The list of selected organizations is shown to all users in the enterprise. End users will see the selected organizations in the Move to Organization screen in Self Service.

Select organizations for subscription

If you have a super enterprise or enterprise organization where users in your system may be assigned to different locations on a temporary basis, and they need to be able to receive alerts and events from their temporary location as well as their home location, you can configure organizations for subscriptions.

Before you select an organization for subscription, the Organization Subscriptions feature must be enabled. For more information, see "Manage organization subscriptions" in the *BlackBerry AtHoc Enterprise Features* guide.

Before an organization can be configured for subscription, user uniqueness must be enabled.

1. In the **Organization Available for Subscription** section, select individual organizations or choose **Select All**. You can narrow the list of organizations by typing the name of an organization in the text box.
2. Click **Save**.

The selected organizations are available for user subscription. End users will see the selected organizations when they click Add Subscription in the Organization Subscriptions section on the My Profile screen in Self Service. The Organization Subscription for End Users option must be selected in the Customization > Self Service section in General Settings on the sub enterprise or suborganization for it to be available for users to subscribe to from Self Service. This option is enabled by default.

Map enterprise organizations to a super enterprise

If you are an Enterprise Administrator, you can map enterprise organizations to your super enterprise organization. The **Set Up Enterprises** section in General Settings > Enterprise Features is visible only when logged in to a super enterprise organization.

When you map an enterprise organization to a super enterprise organization, the following actions occur:

- The BlackBerry AtHoc system checks for duplicate users. The enterprise organization cannot be mapped to the super enterprise organization if duplicate users are found. Duplicate users must be resolved by modifying user details or deleting duplicates.
- Any suborganizations of the mapped enterprise organization are added to the super enterprise.
- The mapped enterprise organization inherits entities including user attributes, alert folders, audio files, and delivery templates from the super enterprise organization. When an organization inherits entities that have the same name, when an operator hovers over the entity name, a tooltip appears that indicates that the entity is inherited and includes the name of the organization from which the entity was inherited.
- The mapped enterprise organization does not inherit alert templates and alert placeholders from the super enterprise.
- Users in the mapped enterprise organization are added to the super enterprise organization.

1. In the **Set Up Enterprises** section, click **Map Enterprises**. The **Organization Structure** window opens and displays enterprise organizations that are not mapped to any super enterprise in the **Enterprises** column. Mapped enterprise organizations are displayed in the **Selected Enterprises** column.
2. Click an enterprise organization in the **Enterprises** column.
3. Optionally, click **View Hierarchy** to view the organization hierarchy of the selected enterprise organization.
4. Click **Add** to add the selected enterprise organization to the **Selected Enterprises** column.
5. Click **Preview Hierarchy** to preview the organization hierarchy of the super enterprise with the added enterprise organizations. If the hierarchy is not correct, click **Cancel** and then repeat Steps 1 to 4.
6. Click **Save**.
7. Optionally, if there are duplicates entities such as attributes, placeholders, alert templates, accountability templates, folders, delivery templates, or audio files found in the enterprise organizations being mapped, the **Duplicated Entities Found** window appears. Do any of the following:
   a) Click **Export to Excel** to export the list of duplicate entities.
   b) Click **Cancel** to return to the General Settings page.
   c) Click **Next** to continue mapping.
8. On the **Confirm - Enterprise(s) Mapping to Super Enterprise** confirmation window, click **Confirm**.

CAUTION: This action cannot be undone.

Customization

The Customization section in General Settings enables you to update your home page with welcome text, adjust the locale settings for your organization, specify phone call settings, add a logo for your desktop app, customize the name on Self Service pages, add disclaimer messages for Self Service or the mobile app, and specify the layout of user profile and dependent pages.

Text

1. In the **Homepage Welcome Message** field, enter text that will appear at the top of the Welcome screen.
2. In the **Footer Text** field, enter text that will appear on the bottom left of every screen.

   Note: This text can be a disclaimer, if one is required, or any information that all users need to see.
3. Click **Save**.

Phone Call Setting

1. In the **Caller ID** field, enter the number you want to display on the mobile devices of alert recipients when an alert is published to them. You can enter up to 15 digits and special characters such as +.
2. In the **Default Country Code** field, select the country code that will be displayed by default whenever users enter a phone number into a field.
3. Optionally, in the **GETS** field, enter the Government Emergency Telecommunications Service (GETS) PIN number.
4. Click **Save**.

Desktop App

1. In the **Desktop App Logo** field, click **Browse** to upload the graphic file you want to display in the desktop app. The file must be a .gif, .jpg, or .png file type. The recommended size is 140 pixels wide by 70 pixels high.
2. Click **Save**.

Self Service

1. In the **Name on User Pages** field, enter your organization name.
2. Optionally, include an organization-specific disclaimer message to display to users when they log in to Self Service. The maximum size of the message is 4000 characters.
3. (For suborganizations only.) Optionally, select the **Organization Subscription for End Users** option to enable users to subscribe themselves to this organization in Self Service. This option is enabled by default.
4. (For suborganizations only.) Optionally, select the **User Move for End Users** option to enable users to move themselves to this organization in Self Service. This option is enabled by default.
5. Click **Save**.

Mobile App

1. In the **Disclaimer Message** text box, enter text that informs end users that when they register for the mobile app, their data is being shared with your organization. You can enter a maximum of 1000 characters. When text is entered in this field, a pop-up message is displayed to end users when they complete registering on the mobile app. End users must acknowledge the disclaimer message before using the mobile app for the first time.
2. Click **Save**.

Dependents

Note: To enable dependents, see Enable and disable features.

Note: The layout for dependent user pages is different than the layout for sponsors. This enables you to keep the layout page for dependents simple, providing only the needed information.

1. In the **Dependent Profile Layout** section, click **View/Edit**.
2. On the **Dependent Profile Layout** dialog, edit the XML to add, modify, or remove profile page sections.
3. Click **Save**.
4. On the **General Settings** page, click **Save**.

Attachments

Note: To enable attachments, see Enable and disable features.

1. In the **Attachments** section, select the **Enable** check box to enable adding attachments to alerts and events.

2. Click **Save**.

Layouts

In the **Layouts** section, you can add or update the default view for various user screens such as the user profile in Self Service, the My Profile or Users page in the management system, and user information when accessed from an alert or accountability event. You can also adjust the display of columns on the Users page and in reports and set group targeting definitions.

1. Click **View/Edit** to open a window to modify the layout settings for any of these screens:
   - **User Details - My Profile**: (Do not modify this setting without first consulting BlackBerry AtHoc customer support.) Determines the layout of standard user attributes when viewed through the My Profile page in the management system or Self Service.
   - **User Details - Full Page**: (Do not modify this setting without first consulting BlackBerry AtHoc customer support.) Determines the layout of standard user attributes when viewed anywhere outside of the main Users list. For example, when seen through the Inbox or from alert or event publishing screens.
   - **User Details - Popup View**: Determines the layout of standard user attributes when viewed anywhere outside of the main Users list. For example, when seen through alert publishing screens or in maps. Information about a user's devices and distribution list membership can also be added to a user's pop-up view.
   - **Default Columns - User Page**: Determines the columns that appear by default from the Users page in the management system.
   - **Default Columns - User Reports**: Determines the columns that appear by default when viewing alert reports or when the user list is shown in a pop-up window.
   - **Targeting Settings**: Determines the attributes that are available for targeting in the By Groups tab on the New Alert and New Event pages. The selected attributes are also available when searching for users by group. Only attributes that have predefined values are available.
2. Click **Save**.

Map settings

As an administrator user, you can use the Map Settings screen to set up and configure map defaults, shape layers, and distribution list layers. For more information about the, BlackBerry AtHoc live map, see the *BlackBerry AtHoc Live Map* guide. For more information about the publisher map, see "Manage the publisher map" in the *BlackBerry AtHoc Create and Publish Alerts* guide.

External events

BlackBerry AtHoc improves emergency managers' situational awareness by providing alerts for external events that impact their organization and employees. External event categories include: Earthquake, Fire, Hurricane, and Flood.

When external events are enabled, Organization Administrators can define the locations and external events they want to monitor. When an external event occurs that impacts a selected location, it appears in the Inbox in the BlackBerry AtHoc management system and on the live map. Operators can also receive notifications on their chosen devices (email, SMS, and mobile app) when events that impact their selected locations appear in the Inbox.

Before you begin:

IsExternalEventSupported must be enabled by a System Administrator in **Settings** > **Feature Enablement**.

1. In the navigation bar, click .

2. In the **Basic** section, click **External Events**.
3. On the **External Events** screen, in the **Your Organizational Area** section, click .
4. On the map, do any of the following:
   - Click **Create Custom Locations**, and then select a shape. Click and drag on the map to draw a shape.
   - Click **Select Predefined Locations**, and then select a location from the pull-down menu.

   You can create multiple custom locations and select multiple predefined locations. You can select a combination of custom and predefined locations.
5. Click **Apply**.
6. In the **External Event Types** section, select the types of external events to receive in the Inbox.

   If the external event type you need is not listed, you can submit a request to add it. Go to the BlackBerry AtHoc support portal at: https://www.blackberry.com/us/en/support/enterpriseapps/athoc/support-request. Include the Event Type keyword and region in the support request form. If available, provide the external event feed source. For example: COVID-19, United States, https://tools.cdc.gov/api/v2/resources/media/404952.rss.

   RSS, Geo-JSON, CAP, and ATOM formats are supported. Each requested feed type must have consistent location data and event type information. Requested feed types should be applicable to a regional (for example U.S. West Coast), national, or international area. For more information, see "Request a new external event type" in the *BlackBerry AtHoc External Events* guide.
7. Optionally, in the **Setup Admin Notifications** section, click **Select Targets**.
8. On the **Users** dialog, select the operators to notify when an external event occurs in the selected organizational areas. All external events that impact the organizational area appear in the Inbox in the BlackBerry AtHoc management system and on the live map. The operators you select will receive an alert about the event on the selected devices.
9. Click **Apply**.
10. From the **Devices** pull-down menu, select the devices (email, SMS, and mobile app) that the targeted operators will receive notifications on. You can select more than one device.
11. From the **Frequency** pull-down menu, select the interval to send the event notifications at. Choose **24 Hrs** or **48 Hrs**. One notification is sent for each event category. For example, Earthquake.
12. Click **Save**.

Manage system settings

The following sections describe how to configure and maintain your BlackBerry AtHoc organizations at the system level.

Specify system settings options

Use the System Settings options tab to configure the name, URL, time zone, database archive directory, system help desk information, and support page content link that are displayed throughout the BlackBerry AtHoc system. You can also configure the client certificate and BlackBerry AtHoc Cloud Services (PSS) settings.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **System Settings**.
5. Click **Edit** to configure the global settings described in the following sections.
6. Click **Save**.

System Setup Parameters

In this section, determine the following values:

- **Name**: Unique name for each BlackBerry AtHoc installation
- **Identifier**: Unique identifier for the organization determined when the organization is created
- **System Setup URL**: Web address for BlackBerry AtHoc
- **Desktop Traffic URL**: Web address for the BlackBerry AtHoc desktop app
- **Time Zone**: The time zone for the application server
- **Database Archive Directory**: Location where the database is archived. Provide the full path name relative to the computer that BlackBerry AtHoc is installed on.

Custom Content

Customize messages for the operator in every organization in the system. In this section, you can configure the following:

- **Management System Help**: Display support information text that displays on the log on screen. Typical information includes directions or a link for when the user forgets their password. HTML formatting is supported.
- **System Disclaimer Message**: Display a required disclaimer, such as limitations on liability or use of copyrighted materials. The limit is 4,000 characters. The disclaimer can display as a splash screen before operators log in or as a banner in the BlackBerry AtHoc desktop window. The banner displays regardless of the module selected from the navigation bar. For example, use a banner to notify operators that the information they are currently viewing is classified and protected from unauthorized use.

Redirection Settings

Select the check box to enable client redirection. Client redirection allows you to set up redirection rules for the desktop app. To configure redirection rules for the desktop app, click **Redirection Rules**.

For more information, see "Redirection" in the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Advanced Settings

Client Certificates

Specify client certificates for the client computer. Use the Microsoft Management Console (MMC) snap-in tool to view certificates on a Windows computer. To access, type **MMC** in the **Start** menu field. Within this section, you can configure the following:

- **Client Certificate**: Select this check box to append a client certificate.
- **Subject**: Enter the value of the Subject parameter found on the Details tab of the certificate settings.
- **Store Name**: Certificates are found in stores. Specify **Personal** or select one of the options in the drop-down list.
- **Store Location**: The stores are located either in the current user store or the local machine store.

BlackBerry AtHoc Cloud Services

BlackBerry AtHoc Cloud Services checks for messages sent between BlackBerry AtHoc and the mobile application. In this section, you can configure the following:

- **Enable Cloud Services**: Select this check box to use the mobile app or AtHoc Connect.

- **Server Address**: Enter the name of the server URL for BlackBerry AtHoc Cloud Services. The server address is provided by BlackBerry AtHoc customer support.
- **Username**: Enter the username that the Polling Agent for BlackBerry AtHoc Cloud Services uses when it polls requests from the service. The username is provided by BlackBerry AtHoc customer support.
- **Password**: Enter the password that the Polling Agent uses when polling requests from the service. The password is provided by BlackBerry AtHoc customer support.

SMS Opt-In Service

Enter the URL for the SMS Opt-In service.

System Data Maintenance

Specify the frequency of records maintenance for the system.

- **Event Viewer**: Enter the number of days after which event records are deleted.
- **Desktop Sessions**: Enter the number of days after which data is deleted for sessions of the desktop app.
- **Geo History**: Enter the number of days after which historical data for geolocation data is deleted.

URL Referrer Whitelisting

Add URLs for external domains or websites to the **Whitelisted Domain Addresses** field to allow users to access the BlackBerry AtHoc management system and Self Service from them. URLs must be in the HTTPS format. Separate URLs by commas, not spaces. The maximum number of characters allowed is 2000.

Add or remove a disclaimer for the BlackBerry AtHoc management system

If your organization requires posting a disclaimer, such as limitations on liability or use of copyrighted materials, you can create a disclaimer that displays in the form of a splash screen before operators log in to BlackBerry AtHoc. You can also customize a banner that displays in the BlackBerry AtHoc desktop window. The banner displays regardless of the module selected from the navigation bar.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **System Settings**.
5. In the text-entry box under the **Custom Content** section, type the text of the disclaimer. The limit is 4,000 characters.
6. Click **Save**.

These changes are applied at the next login to BlackBerry AtHoc management system.

To remove a disclaimer, delete the text in the text-entry box, then click **Save**.

Security policy settings

The security policy manages password rules, sessions settings, and Captcha settings. Additionally, it allows you to force users to change their passwords the next time that they log in.

Note: Security policy settings configured on an enterprise organization are inherited by each suborganization.

Note: Security policy settings configured on a super enterprise organization are inherited by each sub enterprise organization and their suborganizations.

Define password rules

Threats of security breaches have motivated organizations to develop stringent rules governing password creation and mandatory password change cycles. BlackBerry AtHoc enables customizing the rules for password creation and password complexity to conform to your organization's policies, including compliance with the United States Department of Defense password requirements.

System Administrators and Enterprise Administrators can access the Security Policy screen, change the rules for password creation, control the visibility of the Password Never Expires setting on user profile pages, and enforce a system-wide password update for all operators the next time the operators log in.

Important: In addition to the rules covered on the Security Policy screen, consider communicating the following guidelines to your organization when defining passwords:

- Avoid words found in a dictionary, or a proper name, spelled forwards or backwards.
- Avoid simple keyboard sequences with repeated keystrokes.
- Avoid previously used passwords.
- Avoid strings that reference personal information.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. In the **Password Update Rules** section, on the **Security Policy** screen, specify values based on the following information:

   Note: If a password rule is unnecessary in your organization, type 0 (zero) as its value.

   - **Renew Password After**: Force operators to change their passwords every n number of days. Type the number of days that a password is valid. Type **0** to never force operators to change their passwords.
   - **Show "Password Never Expires"**: Select this option to display the Password Never Expires option on user profile pages. This option is selected by default. You must have system administrator or enterprise administrator permissions to set this option.
   - **Reuse Password After**: Prevent operators from recycling recent passwords. For example, if you type **5** the system does not accept any of the last 5 passwords created by an operator. Type **0** to allow operators to use any previous password.
   - **Minimum Password Age**: Set the minimum time interval for changing passwords. For example, type **15** to force users to wait at least 15 days before changing their passwords.
   - **Minimum Changes in Password**: Specify the minimum number of characters in a password to prevent users from using very similar passwords. For example, type **5** to force users to change at least 5 characters each time they change their passwords.
   - **Lock Account After**: Prevent unauthorized attempts to guess an operator's password. Type the maximum number of login attempts allowed. Operators cannot log in using the same username after a lockout. Type **0** to allow an unlimited number of login attempts.
   - **Reset Lockout After**: If a lockout occurs, reset it after a specified number of minutes. Set to **0** (zero) to prevent the lockout from being automatically reset. For this last case, to reactivate the account, the administrator must go to **Users** > **Users**. Click the user's name, then click **Edit Operator Permissions** on the user details screen. Click **Unlock** to change the status.
4. Click **Save**.

The updated password requirements go into effect for all new operators and for existing operators when their passwords expire. Operators whose passwords never expire do not have to change their passwords to conform to updated password requirements.

Configure password complexity

In addition to creating password rules, if you have the required permissions, you can configure the level of complexity required for user passwords.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Password Update Rules** section, select values for each of the following components:
   - **Minimum Length**: Specify the minimum number of characters that a password must contain. Select a value between 7 and 20.
   - **Minimum Lowercase Characters (a-z)**: Specify the minimum number of lowercase characters that a password must contain. Select a value between 1 and 6. If no lowercase characters are required, select 0.
   - **Minimum Uppercase Characters (A-Z)**: Specify the minimum number of uppercase characters that a password must contain. Select a value between 1 and 6. If no uppercase characters are required, select 0.
   - **Minimum Numeric Characters (0-6)**: Specify the minimum number of numeric characters (0-9) that a password must contain. Select a value between 1 and 6. If no numeric characters are required, select 0.
   - **Minimum Special Characters**: Specify the minimum number of special characters (!@#$%^&*()_+) that a password must contain. Select a value between 1 and 6. If no special characters are required, select 0.
4. Click **Save**.

The updated rules go into effect for all new operators and for existing operators when their passwords expire. Operators whose passwords never expire do not have to change their passwords to conform to updated password complexity rules.

Enforce a system-wide password update

If you have the necessary permissions, you can enforce a system-wide password change with the current password rules and complexity. Selecting this option forces all operators to change their password the next time they log in. The operators whose passwords are set to never expire are exempt from this enforcement.

Important: After this action is taken, it cannot be undone.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, click **Enforce password update**.

Revoke operator permissions automatically

If you are an Organization Administrator, Enterprise Administrator, or System Administrator, you can configure your BlackBerry AtHoc system to automatically revoke operator permissions. When configured, operators who have not logged into the system for the specified time have their permissions revoked.

The operator's inactivity period is calculated using the Last Login Date attribute. If the operator has not logged in to the system, the inactivity period is calculated based on the date the operator was granted permissions on. When automatic revocation of operator permissions is enabled, a system job runs every 24 hours to revoke operator permissions based on the operator's last successful login.

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

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

The Accountability Officer and SDK User roles cannot be automatically revoked.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** screen, in the **Revoke Operator Permissions** section, click **Add Condition**.
4. Select one or more roles from the **Operator Roles** list.
5. Select the number of days of inactivity from the **Auto Revoke Permissions after** list.
6. Optionally, click **Add Condition** to add an additional revocation rule. You can add up to three rules.
7. Optionally, click to remove a revocation rule.
8. Click **Save**.

Set session timeout and continue session values

You can set the maximum amount of time a user session can be inactive before auto-logout occurs and when a timeout warning appears.

Note: Enterprise Administrators can set the session timeout and warning settings for an enterprise organization or for any suborganization. If the session timeout setting is changed for an enterprise organization, the suborganizations' settings are also changed.

Note: Enterprise Administrators can set the session timeout and warning settings for a super enterprise organization or for any sub enterprise organization. If the session timeout setting is changed for a super enterprise organization, the sub enterprises and their suborganizations' settings are also changed.

1. In the navigation bar, click .
2. On the **Settings**screen, in the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** page, in the **Login Session** section, enter a value (in minutes) in the **Session Timeout** field. The maximum session timeout value is 1440 (24 hours.)
4. In the **Warning Before Session Timeout** field, enter the number of minutes prior to auto-logout that the warning message appears on the user's screen. If the user does not click to continue the session before the timer runs out, they will be logged out of the system automatically.
5. Click **Save**.

The session timeout value is applied the next time a user logs in to the BlackBerry AtHoc management system.

Limit active sessions

You can configure your BlackBerry AtHoc system to limit the number of active sessions a user can have open at the same time with the same user account. Session information is maintained by a user's browser. Multiple tabs on the same browser use the same session. When the active session limit is reached, the user is prompted to close an existing session. The session that has been inactive for the longest time is terminated and the user is redirected to the login page.

Note: When the limit active sessions setting is configured on a super enterprise or enterprise organization, it is inherited by each sub enterprise and suborganization that does not have this setting defined.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. On the **Security Policy** page, in the **Login Session** section, select **Limit Active Sessions**.
4. Select the number of allowed active sessions from the **Active Sessions per User Account** list. You can select up to ten active sessions.
5. Click **Save**.

Enable operator login using smart cards

When Smart Card authentication is enabled in addition to regular username/password authentication, users have the option of logging in to BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. This is commonly used for Department of Defense systems.

Note: In order to use this option, you must set up Mapping IDs for each user through the Users manager.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **Smart Card Authentication** section, select **Smart Card Login**.
4. Click **Save**.

Require operator login using smart cards

When smart card authentication is required, users can *only* access BlackBerry AtHoc by inserting their smart card into a card reader and then entering a PIN. This is commonly used for Department of Defense systems.

Note: In order to use this option, you must set up Mapping IDs for each user through the Users manager.

If you choose to require operators to log in using smart cards, the following changes occur in the administrative side of the BlackBerry AtHoc system:

- All suborganizations of the main organization inherit the Smart Card-Only authentication method.
- The log in screen continues to display Username and Password fields because until a user attempts to log in, the system has no way of knowing what organization the user belongs to and what restrictions, if any, the user's organization has imposed on authentication.
- After the user attempts to log in with a username or password combination, the system returns an error message informing them that they must use their smart card for system authentication.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **Smart Card Authentication** section, select **Smart Card Login**.
4. Select **Require Smart Card**.
5. Click **Save**.

Enable SSO certificate revocation list checking

When Single Sign-On (SSO) is enabled for your organization, a Certificate Revocation List (CRL) is maintained. A CRL is a list of digital certificates that have been revoked and should not be trusted. If CRL checking is enabled, BlackBerry AtHoc checks the CRL before initiating a Security Assurance Markup Language (SAML) authentication request to an identity provider (IDP) or after receiving an SAML response from the IDP.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Security Policy**.
3. In the **SSO CRL (Certificate Revocation List) Settings** section, select the **Enable CRL Checking** option.

   Note: If the **SSO CRL (Certificate Revocation List) Settings** section is not visible, SSO is not enabled. For information about enabling SSO, see "Enable single sign-on" in the *BlackBerry AtHoc Manage Users* guide.
4. In the **CRL Timeout Interval** field, enter the number of seconds to allow for certificate validation information to be retrieved from the Certificate Authority (CA). The minimum is 1 and the maximum is 60 seconds. The default is 20 seconds.
5. Optionally, select the **Ignore Verification Errors** option. This option is selected by default. When selected, any error that occurs during CRL verification is added to the diagnostic log. This option does not interrupt the SSO

authentication flow. If this option is not not selected, when CRL verification fails, the user is redirected to an error page.

6. Click **Save**.

Import a service provider certificate

Import a BlackBerry AtHoc signed service provider certificate for use in Single Sign-On (SSO). This enables administrators to select a BlackBerry AtHoc certificate instead of uploading and maintaining a custom SP certificate.

You must have system administrator permissions to import a service provider certificate.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click .
4. In the **System Setup** section, click **Security Policy**.
5. On the **Security Policy** page, in the **Service Provider Certificate** section, click **Import Certificate**.
6. On the **Import Certificate** window, enter a valid password for the service provider certificate.
7. Click **Browse** and navigate to and select a valid BlackBerry AtHoc certificate. Only .pfx and .p12 files can be imported.
8. Click **Import**.
9. On the **Security Policy** page, click **Save**.

Enable CAPTCHA validation

A CAPTCHA field is a security test that validates whether a human is entering content into a field rather than an automated program by requiring users to enter the specific numbers or text that they see in an image into a text-entry field.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. Under **Captcha Settings**, select **Enabled**.
4. Click **Save**.

Monitor system health

The supervision and monitoring framework within BlackBerry AtHoc graphically illustrates the current status and any abnormal conditions or failures in the management system homepage, and provides access to its status and administration functions.

Overview of system health monitoring

BlackBerry AtHoc can monitor and supervise the operational status of the following:

- BlackBerry AtHoc internal modules and processes
- Integrated systems and devices

This monitoring and supervision framework operates at global and organization levels, allowing you to do the following:

- Define scheduled monitors of different types to check various system operational conditions.
- Designate normal and abnormal operating conditions.
- Define what actions to take when state transitions take place including proactive notification to system administration and operation teams.

- Access every monitor associated with the system through the System Visibility Console and view all monitors that are in an Error state from a tab on the BlackBerry AtHoc homepage.

View default health monitors

Your BlackBerry AtHoc system includes a set of default health monitors that are grouped into the sections described below. When you create a new monitor, you can add it to one of the groups or create a new group and give it any name.

Note: You must be a System Administrator, Enterprise Administrator or Organization Administrator to view health monitors. You must be an Enterprise Administrator or System Administrator to edit or create a new health monitor.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Global System Health** or **System Health**.

   Note: Global monitors can be viewed from the Global System Health and System Health links. Organization monitors can be viewed only from the organization view. Monitors can only be edited through the Global System or organization under which they were created.

The following table describes the available default health monitors.

Section	Monitor	Description
Database		
	Database Full Backup	Runs a database query to identify the time of the most recent full database backup.
	Database Space	Runs a database query to identify how much space is available in the database and displays an error if the TempDB size falls below the threshold that you specify.
	TempDB Size	Identifies the minimum Microsoft TempDB data sizes required by BlackBerry AtHoc. The following sizes are recommended: • 1 GB for Microsoft SQL Express edition • 2 GB for Microsoft SQL Standard edition • 4 GB for Microsoft SQL Enterprise edition
Web Applications		
	Bing GIS	Tests the Bing GIS URL for responsiveness. You can edit this setting through the Global System Health screen.

Section	Monitor	Description
	Desktop Client Server Interface	Tests the Desktop Client Server Interface URL for responsiveness.
	Management System Console	Tests the Management System URL for responsiveness.
	OEM	Tests the OEM URL for responsiveness.
Services		
	IIS Longevity	Tests how well the Web Application is operating by evaluating the BlackBerry AtHoc diagnostic logs.
	Scheduled Job Queue	Tests how well the Scheduled Job Queue is operating by running a query on the database.
	System Tasks	Tests how well the system tasks are functioning by running a query on the database.
	Tracking & Reporting	Tests how well the Tracking & Reporting system is operating by running a query on the database.
Delivery Gateways		
	AtHoc Cloud Delivery Service (East)	Tests the connectivity of the AtHoc cloud delivery service.
	AtHoc Cloud Delivery Service (West)	Tests the connectivity of the AtHoc cloud delivery service.
	AtHoc Mobile Service	Tests the connectivity between the current organization and the AtHoc Mobile Service.
	OEM Cloud Delivery Service (East)	Tests the connectivity of the OEM cloud delivery service.
	OEM Cloud Delivery Service (West)	Tests the connectivity of the OEM cloud delivery service.
General		

Section	Monitor	Description
	CAP Events Process	Checks the CAP events processor to see if it is correctly processing CAP events.
	CAP Polling Agent	Checks the CAP Polling agent to see if data is being correctly added to the database.
	Database Tables - Identity Seed Max Limit	This monitor checks the identity seed values across tables to determine if they are within the safe limit.
	Desktop Notifier Load Balancing	Monitors the Desktop App incoming traffic across two or more application servers. Warnings are provided when the load is not balanced evenly across all servers.
	Online Users	Identifies the number of Online Users using desktop pop-up alerts within the past 24 hours.
	IIM	Checks the status of connectivity between the BlackBerry AtHoc system and IIM.
Alert publishing		
	Delivery	Checks delivery batches for the alert publishing cycle and reports if there have been publishing errors within the last 24–48 hours.
	Publishing	Checks live publishing activity, and reports if alerts do not go live within a specified amount of time.

View system health monitors with errors

You can view the details of system health monitors that are in an Error state.

Note: You must be a System Administrator, Enterprise Administrator or Organization Administrator to view health monitors. You must be an Enterprise Administrator or System Administrator to edit or create a new health monitor.

1. In the navigation bar, click ⚙.
2. Do one of the following:
   - In the **System Setup** section, click **Global System Health** to view errors for the global system.

- In the **System Setup** section, click **System Health** to view errors for the organization.

3. On the **System Visibility Console** or **Organization Visibility Console** screen, in the **Errors & Warnings** section, click a monitor name.

The screen that appears has a red field at the top that explains why the monitor is in an Error state. The Testing history field displays the state of the monitor during each recent test is displayed. Expand additional sections to view more detailed information about each error.

Create a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to create a new system health monitor.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor that you want to edit. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Create new monitor** at the top of the screen.

   Note: You can also click any of the **Create new monitor** links within the groups on the System or Organization Visibility Console screen. The difference is that when you click a link within a group, the New Health Monitor screen that opens has the **Is it associated with other Health Monitors?** field preset to the name of the group the link appeared within.
4. On the **New Health Monitor** screen, complete the fields in the following sections:

   - **Basic details**

     a. Enter the name of the monitor, the location where you want it to appear on the Visibility Console screen, and the time and frequency of the monitoring checks.
     b. Designate whether or not the monitor will appear on the Organization Visibility Console and whether errors and warnings about the monitor will appear on the System area on the BlackBerry AtHoc homepage.
   - **How does this Monitor test the system?**: Select the kind of test the Monitor will run on the system. Note that the type of test cannot be edited after it is saved. The following options are available:

     - Web URL Test
     - Combined Health Monitors
     - BlackBerry AtHoc Event Logs
     - Database Procedure
     - UAP Health Test

     After you make a selection, sample configuration XML for that type of test appears below the Test Configuration field. Use that as the basis for the XML code you enter into the Test Configuration field.
   - **How is the state of this Health Monitor determined?**: Designate the way the state of the monitor will be determined by selecting one of the following options:

     - **Use the most recent test result**
     - **Calculate it over multiple test results**: If you select this option, use the drop-down lists in the section to specify how the calculation should be determined. Optionally, select **Match the state if** if you want to also use "X" number of identical test results as a trigger for a state change, where you set the value for X.
   - **What happens when this Health Monitor reaches a particular state?**: For each of the Health Monitor states, specify the following:

     a. The implications of the state:

        - **Error**: The test returned an error condition on the object being tested.

- **Warning**: The test returned a warning condition on the object being tested.
- **Good**: The test run returned the expected results.
- **Inoperative**: The test process failed. This does not reflect the health of the object being tested. This state indicates the operational status of the monitor itself. For example, if in a database query, the database referenced has a typo and the system cannot find the database to query.

b. Actions to take when the monitor is in the selected state:

Define the actions that should be taken any time a monitor transitions into each of the states. To make this process faster and less prone to errors, click **Show a list of possible actions** for each state and then add either or both of the actions **Trigger a URL** or **Send an Email** on the pop-up screen for the **Configure** field.

5. Click **Save**. The system evaluates the parameters you set. If the parameters are correct, the system creates a new monitor. If the syntax in any of the conditions is incomplete or incorrect, an error message is displayed.

Edit a health monitor

Note: You must be an Enterprise Administrator or System Administrator to edit a system health monitor.

1. In the navigation bar, click  .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to edit.
3. On the **Organization Visibility Console** or **System Visibility Console** screen, click the name of the monitor you want to edit. The monitor details screen opens, displaying the current state of the monitor and its recent testing history.
4. Click any or all of the sections on the screen to edit the fields within them:
   - **Testing history**:
     a. Change the granularity of the time frame displayed in the history table by clicking **Hourly**, **Daily**, **Weekly**, or **Monthly**.
     b. Click  and  to change the block of time you are looking at. For example, if the granularity is set to Monthly, click  to display the testing history for the previous month.
   - **Basic details**:
     - Change the name of the monitor, its location on the Visibility Console screen, and the time and frequency of the monitoring checks.
     - Change the setting that determines whether the monitor appears on the Organization Visibility Console and whether errors and warnings about the monitor appear on the System tab on the BlackBerry AtHoc homepage.
   - **Database Procedure**:
     - Update the test configuration script that is used in the monitor.
   - **How is the state of this Health Monitor determined?**:
     - Change the way the state of the monitor is determined by selecting the other option: *most recent result* or *combined results*.
   - **What happens when this Health Monitor reaches a particular state?**:
     - Change the implications of any or all states, and configure different transaction actions for any or all states.
   - **Special Case: Edit the IIS Longevity Health Monitor**: If you have more than one application server, you need to modify the default settings for the IIS Longevity health monitor using the following values:

- `WarningCountThreshold`: The default value is 2. This default assumes one application server. For a multiple application server installation, change the value of `WarningCountThreshold` to (application server count) x (default). For example, if there are two application servers, the value should be 4.
- `ErrorCountThreshold`: The default value is 5. The default setting assumes one application server. For a multiple application server installation, change the value of `ErrorCountThreshold` to (application server count) x (default). For example, if there are two application servers, the value should be 10.

5. Click **Save**.

Disable a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to disable a system health monitor.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to disable. The System Visibility Console screen opens, displaying the system monitors in the system.
3. Click **Disable** in the row for the monitor you want to disable.

The System Visibility Console screen refreshes and the monitor appears with no icon next to its name and two buttons, **Enable** and **Delete**, in the row.

Enable a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to enable a system health monitor.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to enable. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Enable** in the row for the monitor you want to enable.

The System or Organization Visibility Console screen refreshes and the monitor appears with either a green or a red beside its name and Refresh, Disable, and Delete buttons in the row.

Delete a system health monitor

Note: You must be an Enterprise Administrator or System Administrator to delete a system health monitor.

Note: Deleting the monitor permanently deletes all history and configuration for the monitor.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to delete. The System or Organization Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Delete** in the row for the monitor you want to delete.
4. On the **Delete Health Monitor** dialog, click **OK**.

The System or Organization Visibility Console screen refreshes and the monitor no longer appears on the screen.

Refresh a system health monitor

Although health monitors refresh automatically based on their internal monitor schedule, you can refresh a monitor manually at any time.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Global System Health** or **System Health**, depending on which system contains the monitor you want to refresh. The Organization or System Visibility Console screen opens, displaying all of the system monitors in the system.
3. Click **Refresh** in the row for the monitor you want to refresh.

The System Visibility Console screen refreshes and the "Last tested" information next to the monitor name updates to the current time and date.

The Testing history field on the monitor details screen also updates, displaying the time and date you manually refreshed the monitor with the words *Manually Run Test*.

View the diagnostic log

The diagnostic log allows you to view various logs and events and export that information to a .csv file, which can be then sent to BlackBerry AtHoc customer support for troubleshooting purposes. You can export a maximum of 30,000 events.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Diagnostic Log**. The diagnostic log appears.
3. Optionally, click **Refresh** to refresh the log manually and show the most recently received alerts.
4. Optionally, click **Clear Log** to remove all entries from the log.

   Note: You must be logged in to the System Setup (3) organization and have system administrator permissions to clear the diagnostic log
5. Optionally, click **Export** to export the contents of the log to a .csv file.
6. Click **Current Page** or the number of events that you want to export.

Run a basic search of the diagnostic log

To limit the number of events displayed in the diagnostic log, you can run a basic search.

1. On the **Diagnostic Log** page, in the **Search** field, enter a single search criteria such as an event ID, event type, or server name.
2. Click .

Run an advanced search of the diagnostic log

To limit the number of events displayed in the diagnostic log, you can run an advanced search.

1. On the **Diagnostic Log** page, click **Advanced**.
2. In the **Advanced search** section, enter search criteria in any combination of the following fields:
   - Event Id
   - Type
   - Server
   - Assembly
   - Module
   - Member
   - Short Message
   - Time
   - Thread Id
3. Click **Search**.

View geolocation transactions and logs

Administrators can bulk update users' physical addresses using the BlackBerry AtHoc User Sync client.

When a bulk update transaction is submitted, the Geocoding Summary and Logs settings page displays the following information:

- Date and time the transaction was submitted.
- User name of the person who initiated the transaction.
- Organization name of the users whose geolocation attributes were updated.
- The total number of records included in the transaction.
- The number of records that were successfully processed.
- The number of records that were not processed.
- The current status of each transaction.
- A link to download the log of each transaction.

The status of each transaction can be any of the following:

- **Pending**: The transaction has not yet been submitted to the API for processing.
- **In Progress**: The transaction has been submitted to the API, but the API response is not complete.
- **Partially Processed**: The API has processed some of the transaction, but is not complete. This status is usually only seen for larger transactions of over 200,000 records.
- **Completed**: The transaction is complete and all job records were successfully processed.
- **Partially Complete**: The transaction is complete but some records failed.

Note: For more information about bulk updates of users' physical addresses using the BlackBerry AtHoc User Sync client, see "How to bulk update users' physical locations" in the *BlackBerry AtHoc User Sync Client* guide.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **Geocoding Summary and Logs**.
3. Optionally, change the **From** and **To** fields to view transactions from a different date range and then click **Search**. The default is 1 day.
4. Optionally, click **Clear All** to remove all transactions.
5. Optionally, click **Download to Excel** to export all displayed transactions to a .csv file.
6. Optionally, click **Download Log** in the row for a transaction to download the details of that transaction to a .csv file.

Database archiving

Database archiving is an important system task. If the database becomes full, the system will fail. From the Database Archiving Job system task, users with enterprise administrator or system administrator permissions can see the current size of databases and execute the archiving job as needed. A warning displays on the BlackBerry AtHoc homepage when the database size reaches 90% of capacity.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.
4. In the **System Setup** section, click **Archive**.

   Note: If archiving needs to be performed, a status message appears at the top of the Database Archiving screen.
5. Review the details on the **Database Archiving** screen to determine which database or databases will be archived. You can do this by comparing the current size of each database against the maximum size allowed. If previous archiving jobs have been run, details of those jobs appear in the History table below the Database Status table.

6. Click **Archive**.
7. On the **Database Archiving Activation** screen, read the entire screen of explanations and cautions about archiving.
8. In the **Data Deletion Settings** field, specify the minimum number of days old data must be in order to be archived.
9. Select the check box at the bottom of the screen to indicate you have read the explanations and understand the conditions.
10. Click **Start Archiving Job**.

    Note: If an archiving job seems to be running for a long time, check the BlackBerry AtHoc process status to make sure that the service is running.

Organizations Manager

This section describes how to create and duplicate organizations using the Organizations Manager. To learn how to work with enterprise and super enterprise organization hierarchies, see the *BlackBerry AtHoc Plan and Manage Enterprise Organizations* guide.

Note: Administrators who manage multiple organizations must be assigned the System Administrator role. Having only the administrator role is not sufficient and does not allow assigning operator roles in other organizations.

To assign roles, see "Grant operator permissions to a user" in the *BlackBerry AtHoc Operators Roles and Permissions* guide.

For detailed configuration steps for AtHoc Connect, see "Configure the BlackBerry AtHoc management system for AtHoc Connect" in the *BlackBerry AtHoc Connect* guide.

Create an organization

To create a new organization in the system, you must be a System Administrator with permissions to switch between organizations from within the BlackBerry AtHoc management system.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. To access the Organizations Manager, do one of the following:

    a. In the navigation bar, click .
    b. In the **System Setup** section, click **Organizations Manager**.

    Or:

    a. In the navigation bar, click the name of your organization and then click the link with your organization name.
    b. On the **Organization Hierarchy** window, click **Manage Organization Hierarchy**.
3. On the **Organizations Manager** screen, click **New**.
4. Enter a name for the new organization.
5. Select one of the following organization types:

    - **Super Enterprise**: Choose this type if you are logged into the **System Setup (3)** organization and are creating a super enterprise organization.
    - **Enterprise**: Choose this type if you are logged into the **System Setup (3)** organization and are creating an enterprise organization.
    - **Sub Organization**: Choose this type if you are logged in to an enterprise organization and are creating a member organization.
    - **Basic**: Choose this type if you are creating a basic organization.
6. Select a locale for the organization.

7. Click **Save**. Information about the new organization appears on the Organizations Manager screen.
8. To change the BlackBerry AtHoc interface to display the organization you just created, click your username and then click **Change Organization**.
   a. 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.
   b. Click **Switch** on the row for the organization you just created.
   c. On the **Change Organization** confirmation window, click **OK**.
   d. The system refreshes and displays the new organization.
9. Configure the new organization using the tasks outlined in Configure a new organization.

Configure a new organization

After you have created the organization and have switched to the new organization, you can define the URLs, name, logo images, default alert templates, and Self Service defaults for that organization.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. Configure basic settings: In the **Basic** section, click **General Settings** and then complete the steps in General settings.
4. Configure devices: Complete the tasks described in Configure devices.
5. Configure gateways: Complete the tasks described in Configure device gateways.
6. Enable devices: Complete the tasks described in Enable devices on the BlackBerry AtHoc server and the "Enable a Device" task described in Enable and disable devices.
7. Create user attributes: Complete the tasks described in the "Create a user attribute" and "Configure an Organizational Hierarchy attribute" sections of the *BlackBerry AtHoc Manage Users* guide.
8. Add users: Complete the steps described in the "Create a user" section of the *BlackBerry AtHoc Manage Users* guide.

Duplicate an organization on the same server

You can copy an existing organization and rename it. Be aware that most settings are copied from the original organization, including alert templates, except as specified.

Important:

- You must be a system administrator.
- Duplication includes device and protocol duplication.
- After duplicating an organization, review all alert templates and make adjustments if necessary.
- Creating organizations using the New button in the Organizations Manager should be performed only with assistance from BlackBerry AtHoc technical support to ensure the new system has all the appropriate settings.
- By default, a duplicated organization will not have a common name. If you plan to access the duplicated organization with the BlackBerry AtHoc SDK, you must assign it a common name.
- You can duplicate a peer organization, but not a child (member) organization.

1. In the navigation bar, click .

2. In the **System Setup** section, click **Organizations Manager**.
3. On the **Organizations Manager** screen, click to select the organization you want to copy.

   Note: If the list is extensive, use the search field at the top of the screen. You can also click a column heading sort the list.
4. Click **Duplicate**.
5. On the **Duplicate Organization** dialog, enter the name of the new organization.
6. Click **Save**.

The duplicate organization appears in the list on the main screen.

Duplicate organizations across systems

Duplicating organizations from one server to another is an advanced configuration task. For more information, see "Advanced server configuration" in the *Install and Configure BlackBerry AtHoc* guide. For access to this guide, contact BlackBerry AtHoc customer support.

Enable and disable features

Note: The Feature Enablement section is for internal use only.

You can enable and disable features at a system, super enterprise, enterprise, or individual organization level. You must be a System Administrator to enable or disable features.

Feature enablement is inherited from parent organizations by default. Feature enablement on a system level is inherited by all organizations in the system. Feature enablement on a super enterprise organization is inherited by its sub enterprise organizations and their suborganizations. Feature enablement on an enterprise organization is inherited by its suborganizations. You can override these inheritance rules by explicitly enabling or disabling a feature on a super enterprise, enterprise, or individual organization.

1. Log in to the management system as a System Administrator.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **Feature Enablement**. The Feature Enablement screen opens and displays the features currently available in the system.

   The Organization column displays the organization where the feature is explicitly enabled. The Enabled column displays the current status of the feature, and whether this value is due to inheritance. For example, True in the Enabled column indicates that the feature is enabled in the current organization, while Inherit (True) indicates that the feature is enabled due to inheritance rules.

   Note: If a feature has been explicitly enabled or disabled in the organization you are currently logged in to, the feature row appears in bold.
4. Click the row for the feature you want to enable or disable.
5. On the **Edit Feature Enablement** window, from the **Enabled** list, select **True** to enable the feature, **False** to disable the feature, or **Inherit**. If you select Inherit, the feature status is inherited from the parent organization.

   Note: The Inherit option is not displayed for a system level organization.
6. Optionally, select the **Force all children to inherit** option if you want the feature status you are setting to be inherited by all child organizations, regardless of the feature status set on those child organizations.

   Note: This option is not available for suborganizations.
7. Click **Save**.

Note: Some features require additional steps before they are fully disabled. For more information, see Additional steps to disable features.

Additional steps to disable features

After you disable the following features on the **Feature Enablement** screen, they require additional steps to be performed before they are completely disabled. In the following table, the Default disable action column describes the state of the feature when it is disabled on the Feature Enablement screen. The Additional steps column describes the steps you need to perform after disabling the feature on the Feature Enablement screen.

Feature	Default disable action	Additional steps
IsAdvancedQuerySupported	• The Advanced Query section is hidden in alert templates. • Users targeted by advanced query in alert templates are removed. • Users targeted by advanced query are still targeted in existing alert templates.	Open and save the template.
IsCallBridgeSupported	• Existing alert templates do not display call bridge information. • Alerts published from the alert publishing page using an existing alert template display call bridge information.	Open and save the template.
IsDependentSupported	• Dependents are not displayed on alert templates. • Targeted user counts on alert templates are correct. • Alerts published from existing alert templates still target dependents. The number of targeted dependents is included in the targeting summary on the Alert Summary page and in reports.	Open and save the template.
IsIndividualUserTargetingSupported	• The targeted user count in existing alert templates is 0. • Alerts sent using existing alert templates can still target individual users.	Open and save the template.

Feature	Default disable action	Additional steps
IsMassDeviceTargetSupported	• The Mass Device section is not visible in existing alert templates. • The Mass Device section is not displayed on the Review and Publish window. • Alerts sent from existing alert templates are targeted to mass devices. • Targeted mass devices are displayed on the alert summary and in advanced reports.	Open and save the template.
IsPlaceholderSupported	• Placeholders are displayed during alert publishing. • Placeholder default values are displayed. • Placeholders are resolved after an alert is published.	Delete all instances of placeholders and save the template.
IsTargetByAreaSupported	• The Target By Location section is not displayed in alert templates. • The Targeted Users count in alert templates is not updated. • Alerts published from existing alert templates target users by location.	Open and save the template.
IsAccountabilitySupported	All existing live events continue.	End all live events.
IsWAMSupported	Background jobs do not support weather modules.	Disable all weather alert rules.
IsFillCountSupported	Users are still targeted with fill count when sending an alert from an existing alert template.	Remove fill count criteria and save the template.
IsDeviceDeliveryOrderSupported	Device delivery order is still supported on existing alert templates.	Open and save the template.
IsAlertTemplateSettingSupported	• The Content section still appears in template settings for existing alert templates. • The Content section does not appear when creating a new alert template.	Clear any custom settings and save the template.

Feature	Default disable action	Additional steps
IsChannelSupported	• The folder drop-down menu does not appear when creating a new alert template. • Folders can be created and folder restrictions can be added to existing alert templates.	Open and save the template.
IsDeviceOptionSupported	• Device options can still be set from an alert email. • Device options are disabled in the BlackBerry AtHoc management system.	Clear any custom device option settings and save the alert template.
IsDropboxSupported	• Existing alert templates continue to retrieve files from DropBox. • New alert templates do not display the DropBox option.	Remove links to DropBox and save the alert template.
IsGroupBlockingSupported	Alerts are not sent to blocked users.	Clear user restrictions (blocked distribution lists or users) and save the alert template.
IsPrintAlertSupported	The **Print** button is still visible in the Report page.	This feature cannot be disabled.
IsSchedulingSupported	Alerts sent from existing alert templates still end after the scheduled duration.	End or cancel all existing scheduled alerts in the organization.
IsScheduledLocationAccessSupported	Scheduled location access continues to function for existing alert templates.	Clear all existing scheduled location access criteria in the organization.
IsRecordedAudioSupported	Alerts published from existing alert templates still include audio files.	Remove all references to audio files and save the template.

Manage the agents for integrated devices

If you have the necessary permissions, the Integration Manager screen allows you to view and edit agents for communicating with external devices, such as fire panels.

Note: The full Configuration XML for public agents is visible on the System Setup (3) organization. For enabled organizations, only the relevant Configuration XML is displayed.

Provision applications that can call the web API

You can provision a new API integration with the BlackBerry AtHoc management system. You must have be an Organization Administrator, Enterprise Administrator, or System Administrator to provision applications. You must be a System Administrator to enable a provisioned application.

Note: The Client ID and Client Secret can only be used in the organization in which they are created. If the Client ID and Client Secret are created in the System Setup (3) organization, they can be used in any organization. If the Client ID and Client Secret are created in an enterprise organization, they can be used in any of that enterprise's suborganizations. If the Client ID and Client Secret are created in a super enterprise organization, they can be used in any of that super enterprise's sub enterprises and their suborganizations. If the Client ID provided does not follow these inheritance rules, a 400 (Bad request) error code is returned.

1. Log in to the BlackBerry AtHoc management system as an Organization Administrator, Enterprise Administrator, or System Administrator.
2. In the navigation bar, click ⚙.
3. On the **Settings** screen, in the **System Setup** section, click **API Applications**.
4. On the **API Applications** window, click **New**.
5. On the **New API Application** window, enter a name for the API integration.
6. (System Administrators only) Select **Enabled** beside **Status**.
7. In the **Authentication** section, select a Grant Type. The default is Password. If you select Implicit, enter a redirect URI in the text box that appears.
8. Click **Save**. A Success message appears that includes the Client ID and Client Secret.
9. Take note of the displayed Client Secret. It is displayed only once and will need to be regenerated if lost.

Note: After you provision your application in the BlackBerry AtHoc management system, contact BlackBerry AtHoc customer support to have the application reviewed and enabled.

Reset the client secret

If you need to reset the client secret for your API integration, complete the following steps:

1. Log in to the BlackBerry AtHoc management system.
2. In the navigation bar, click ⚙.
3. In the **System Setup** section, click **API Applications**. The API Applications window opens.
4. Optionally, enter a name in the search box to filter the list of applications.
5. Optionally, select **Enabled Applications** or **Disabled Applications** from the **All Applications list** to filter the list of applications.
6. Click the application you want to modify.
7. Click **Reset Client Secret**. A confirmation window opens.

   Note: Any existing calls to the selected API with the existing client secret will be blocked when you reset the client secret.
8. Click **Continue**. You are returned to the API application window. The new client secret is displayed.
9. Take note of the displayed client secret.
10. Click **Save**.
11. Add the new client secret to your authentication payload.

Configure API throttling settings

Note: The API Throttling section is for internal BlackBerry AtHoc use only.

Throttling of API usage is required to protect BlackBerry AtHoc server resources from being over-used, or used in ways that are not intended by BlackBerry AtHoc that can result in slow responsiveness. Throttling limits are applied to overall API usage by any single caller, client, organization, or endpoint. If an API call has reached its throttle limit, the server returns a 429 (Too Many Requests) error.

1. Log in to the BlackBerry AtHoc management system as a System Administrator.
2. Change to the **System Setup (3)** organization.
3. In the navigation bar, click ⚙.

4. In the **System Setup** section, click **API Throttling**.
5. On the **API Throttling** page, complete the steps in the following topics to configure client and endpoint whitelists, general rules, and client rules.
6. Click **Save**.

Whitelist

In the Whitelist section, System Administrators can specify endpoints and clients to be whitelisted. Whitelisted clients and endpoints are exempt from API throttling.

1. Select one or more clients from **Client Whitelist** pull-down menu to add them to the whitelist.
2. Click **Add Endpoint** to add an endpoint to the whitelist. A new row appears in the list.
   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. In the **URL** field, enter a URL.
   c. Click **Save**.

   The endpoint is added to the endpoint whitelist.
3. Optionally, click to edit an endpoint.
4. Optionally, click to remove an endpoint.

General rules

In the General Rules section, system administrators can add general rules that apply to all endpoints.

1. Click **Add General Rule**. A new row appears in the list.
   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. Optionally, in the **URL** field, append a URL to **api/v2/**. Use ***** as a wildcard in a URL. Enter only ***** to specify all endpoints.
   c. Specify a time (in minutes) and a limit for the number of requests.
   d. Click **Save**.
2. Optionally, click to edit a general rule.
3. Optionally, click to remove a general rule.

Client rules

In the Client Rules section, system administrators can add rules that apply to specific clients. Rules applied to a specific client override rules specified in the General Rules section.

1. Click **Add Client Rule**.
2. In the **Add Client Rule** window, select a client from the pull-down list.
3. Click **Add Client Rule**. A new row appears.
   a. Select a **Verb** from the list to specify a request type. For example, GET.
   b. Optionally, in the **URL** field, enter the client URL.
   c. Specify a time (in minutes) and a limit for the number of requests.
   d. Click **Save**.
4. Optionally, repeat Step 3 to add additional client rules. You can add multiple rules for a single client.
5. Click **Add**.
6. Optionally, click to edit a client rule.
7. Optionally, click to remove a client rule.

View the operator audit trail

The operator audit trail enables authorized users to audit the system based on a specific operator or action performed in the BlackBerry AtHoc system, such as login attempts, logouts, or password changes. The operator audit trail retains data for 12 months.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Operator Audit Trail**.
3. From the **Operator Audit Trail** screen, you can perform any of the following actions:
   - Change the report time frame by selecting different **From** and **To** dates. Enter the dates manually or click and select each date on the pop-up calendar. The report that is generated will then include activities between and including the To and From dates you select.
   - Enter an operator name or ID in the **User** field to view their activity in the system. If no value is entered in this field, all operators are included in the report.

     Note: The User field is not case-sensitive. You can use the **?** wildcard as a substitute for a single letter or the ***** wildcard as a substitute for a string of letters.
   - View all activities by leaving the **Entity** field set to the default value of **All Entities** or view activities for a specific entity by selecting one from the list.

     To further filter activities, select an entity and then select **Search by Specific Action(s)**. In the **Action(s)** field, click the list and select each of the actions that you want to use as filter criteria.

     Note: If you apply filtering criteria, you must click **Search** to refresh the screen and view the updated results list.
   - Export or print the System Log Report by completing either of the following steps:
     - If Microsoft Excel is installed on your computer, click **Download excel file**, then either save the report to a location on your machine or open the report directly.
     - Click **Printer friendly report** to view the formatted report in a new browser window, then use the browser's **Print** command to print the report.

View an alerts usage summary report

Alerts Usage Summary reports are used to determine how many reports or messages have been sent out within a designated amount of time. To create one of these reports, see "Create and view an alerts usage summary report" in the the *BlackBerry AtHoc Alert Tracking and Reporting* guide.

Manage system jobs

You can manage common system jobs such as database archiving and purging log data in BlackBerry AtHoc. If you have administrator permissions, for each system job you can do any of the following:

- View the status of historical runs (start time, end time, duration, result.)
- Determine the next scheduled run date and time.
- Manually run the system task.

View details about system jobs

The System Tasks screen displays a list of all automated jobs in the system.

1. Log in to the BlackBerry AtHoc management system.
2. Click the down arrow beside your log in name and select **Change Organization**.
3. On the **Change Organization** screen, click **Switch** on the **System Setup** row.
4. On the **Change Organization** confirmation window, click **OK**.

5. In the navigation bar, click .
6. In the **System Setup** section, click **System Jobs**.
7. On the **System Jobs** screen, click the name of any task to view additional details.
8. On the task details screen, you can perform any of the following tasks:
    - View a description of the task.
    - View the run interval, the last run time, and last run result for the task.
    - View a history of the most recent runs of the task, including the start time, end time, duration and result of each run.
    - Click **Click to Disable** or **Click to Enable** to change the status of the task.
    - Click **Run now** to manually initiate the task.
    - Click **OK** in the **Result** column in the **History** section to view the job log for any recent run.

Descriptions of System Jobs

The following jobs are displayed on the System Jobs screen:

- **AtHoc Connect Update Alert Responses**: This job updates AtHoc Connect with organization alert responses.
- **AtHoc Connect User-Base Sync**: This job synchronizes the IAC user base with the agreement state in AtHoc Connect.
- **Auto Delete Users**: This job deletes end users based on the settings configured on the Disable and Delete End Users screen.
- **Auto Disable Users**: This job disables end users based on the settings configured on the Disable and Delete End Users screen.
- **Batch Geocoding: Postprocessor**: This job verifies job statuses, downloads, processes submitted requests, updates the database, and sends an email for the completed uploads.
- **Batch Geocoding: Preprocessor**: This job creates Bing batch geocoding requests if the addresses are not found in the local geocoding lookup table.
- **Cap Event Processor**: This job processes captured inbound CAP events and publishes an alert for each inbound alert based upon the rules configured for the agent.
- **Cap Feed Poller**: This job fetches the index feed and creates a queue entry in the BlackBerry AtHoc database queue.
- **Cisco DMS Synchronization**: This job polls NDS for the Digital Media Player groups to import.
- **Delivery Batch Recovery**: This job recovers batches with incomplete delivery due to gateway related failures.
- **Delivery Batch Retry**: This job resets delivery batches that have either timed out or completed with error.
- **Desktop Sessions Maintenance**: This job cleans up stale sessions and updates the online users graph that is visible on the homepage.
- **Desktop SignOn Processing Job**: This job updates user attributes and live alert sessions for all desktop sessions created since the last run time.
- **Email Publisher**: This job processes alert publishing requests that are sent by email.
- **External Events - Orgs Sync**: This job provisions organizations for external events.
- **Feed Poller**: This job polls feeds from various sources.
- **Feed Processor**: This job processes feeds from various sources.
- **IEM IPAWS Plugin Agent - For All VPS**: This job communicates with IPAWS for all organizations on the server.
- **Mobile Devices Purge Service**: This job removes any temporary or transient mobile device data that is no longer required by the system. This system job does not remove any business data.
- **MTR: Database Tables – Identity Seed Max Limit**: This task checks if the identity seed value has exceeded the threshold where it should be reset.
- **Process Accountability Event Job for Recipient Re-Compute**: This job manages accountability event recipient re-computation.

- **Process Accountability Event Job for Reminder**: This job manages accountability events related to sending reminder alerts.
- **Process Accountability Events for End**: This job manages accountability event lifecycle and status management.
- **Process Accountability Events for Status Update**: This job manages the status attribute value changes for affected uses during the accountability event lifecycle.
- **Process Accountability Events Tracking Summary**: This job manages the accountability events tracking summary.
- **Process BBME Tracking – UAP – BBM-E**: This job retrieves tracking from NDMS systems and updates alert reports in BlackBerry AtHoc.
- **Process Geo Fencing**: This job checks if users have entered a geofenced area and, if so, publishes the alert to them.
- **Process Inbound Event for Report Category**: This job manages the triggering alert for Report Inbound Event.
- **Process NDMS Tracking - ATHOC-NDMS-EAST**: This job retrieves tracking data from AtHoc Cloud Delivery Service (East) and updates Alert reports within the system.
- **Process NDS Tracking- ATHOC-NDMS-WEST**: This job retrieves tracking data from AtHoc Cloud Delivery Service (West) and updates alert reports within the system.
- **Process NDS Tracking <device>**: These jobs retrieve tracking information from NDS systems for various devices and updates alert reports in BlackBerry AtHoc.
- **Process OEM Tracking - UAP-OEM-EAST**: This job retrieves tracking from the OEM Cloud Delivery Service (East) and updates alert reports within the system.
- **Process OEM Tracking - UAP-OEM-WEST**: This job retrieves tracking from the OEM Cloud Delivery Service (West) and updates alert reports within the system.
- **Process Situational Response Incident Steps for End**: This job manages ending incident steps for ended alerts and events.
- **Purge Older Logging Data**: This job removes any temporary or transient data from the database tables that is no longer required. This job runs daily at 11:00 PM.
- **Rebuild Database Indexes**: This job performs weekly index maintenance on the databases.
- **System Diagnostics Report**: This job runs diagnostic stored procedures and collects the output in a diagnostic log.

Create and export a system diagnostics report

During a service call, BlackBerry AtHoc customer support might ask you to export the System Diagnostics Report and then send the results to them. The System Diagnostics Report job runs every day at 12:00 PM and the report appears in the Diagnostic Log as an event. If asked, you might also need to run the report job before exporting the report.

1. In the navigation bar, click ⚙.
2. In the **System Setup** section, click **System Jobs**. The System Tasks screen opens, displaying a list of all automated jobs in the system.
3. If requested by BlackBerry AtHoccustomer support, run the diagnostics job by completing the following steps:
   a. Click **System Diagnostics Report** at the bottom of the tasks list.
   b. On the **System Diagnostics Report** screen, click **Run now**.
4. After the report runs, click ⚙.
5. In the **System Setup** section, click **Diagnostic Log**.
6. Use the search field at the top of the screen to find all of the System Diagnostics Reports in the system.
7. In the results list, click the most recent report to open it.
8. Click **Export** at the top of the screen.
9. When prompted, save the diagnostic log to the default file, `AtHocEventViewer.xml`.

10. Send the report to your contact in BlackBerry AtHoc customer support.

Purge ended alerts

System Administrators, Enterprise Administrators, and Organization Administrators can enable alert purging by selecting purge criteria for an organization. The purge criteria is the number of days after an alert or event has ended.

Important: Purged alerts and events cannot be recovered.

The purge deletes all ended alerts, events, and their related attachments from the system. Purging ended alerts and events is disabled by default and can be enabled per organization. Suborganizations do not inherit purge criteria from the enterprise organization. Sub enterprise organizations and their suborganizations do not inherit purge criteria from a super enterprise organization.

Any changes made to the purge criteria take effect at the next scheduled purge.

Only ended alerts and events are purged. Drafts alerts and events, templates, manual logs, the operator audit trail, and scheduled and recurring alerts are not purged.

For events, purge criteria are applied after the last alert for the event is published. For example, if an event is for 30 days with one recurring alert per day, and the purge criteria is set to 120 days, then all 30 alerts are purged on the 121st day after the last alert for the event is ended.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Purge Ended Alerts**.
3. Optionally, in the **Status** section, click the link in the in the **Result** field to view information about the last purge job, including the date of the last purge and the number of alerts that were purged.
4. In the **Schedule** section, select the purge criteria from the **Purge Ended Alerts** list. You can select to purge ended alerts and events after 90, 120, or 180 days.
5. Click **Save**.

Manage SMS Opt-In

SMS Opt-In enables operators to allow community members, visitors, event participants, or other users outside of their organization to subscribe to receive alerts by SMS. These outside users can subscribe to receive alerts by sending a text event code via SMS.

Organization Administrators create event codes, and then share the event code and the short code with users. When a user opts-in by sending an SMS with the event code, they are added to the BlackBerry AtHoc management system. Operators can then target them in alerts.

Entries are added to the operator audit log when SMS Opt-In is enabled or disabled.

Configure the SMS Opt-In service URL

The SMS Opt-In service URL is pre-populated with the following URL: `https://optin.athoc.com`. Configuring a different SMS Opt-In service URL is optional.

1. Log in to the BlackBerry AtHoc management system as a system administrator.
2. Change to the **System Setup (3)** organization.
3. Click .
4. On the **Settings** page, in the **System Setup** section, click **System Settings**.
5. On the **System Settings** page, click **Edit**.
6. Scroll down to the **Advanced Settings** section.
7. In the **SMS Opt-In Service** section, enter a URL in the **Service URL** field.
8. Click **Save**.

Activate SMS Opt-In

Entries are added to the operator audit log when SMS Opt-in is enabled or disabled.

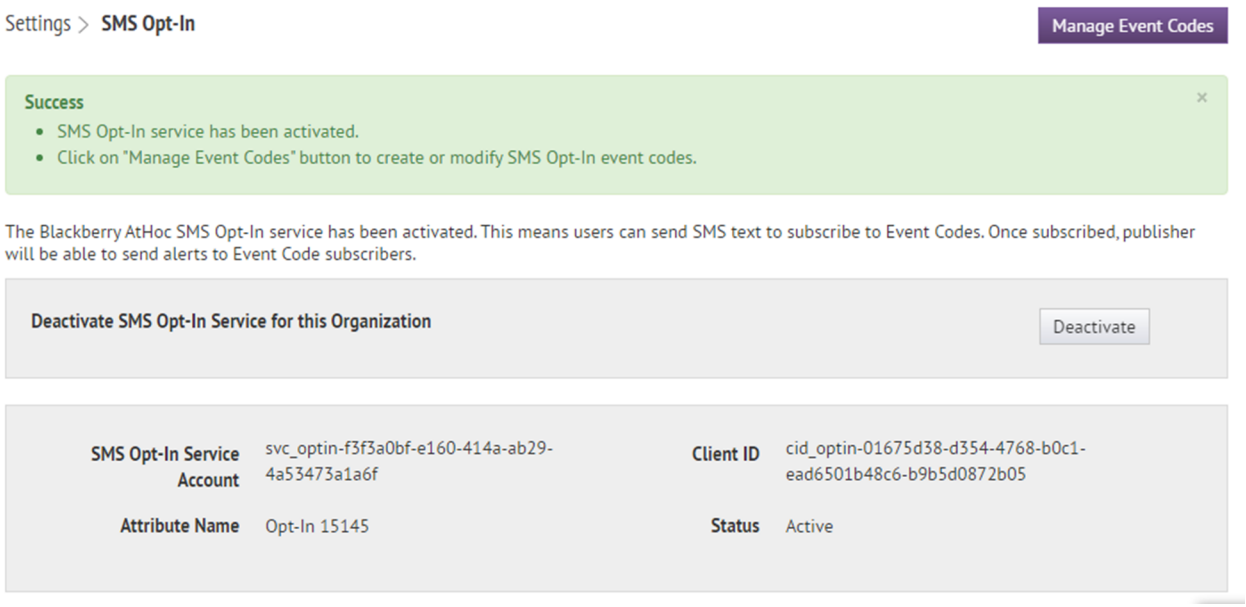
Before you begin:

- You must be an Organization Administrator, Enterprise Administrator, or System Administrator to enable and activate SMS Opt-In.
- SMS Opt-In is disabled by default. To enable it, log in as a System Administrator and go to **Settings** > **System Setup** > **Feature Enablement** and set the IsSMSOptInEnabled feature to True.
- To activate SMS Opt-In, the text messaging device must have the Common Name "sms". Verify the device's Common Name in **Settings** > **Devices** > **Device**. If a second text messaging device is required, select that device when targeting SMS Opt-In users in alerts or accountability events.
- A text messaging device with the Common Name "sms" must be enabled for SMS Opt-In to work. To enable a text messaging device, or to verify that your enabled device has the Common name "sms" go to **Settings** > **Devices** > **Device**. If you need to add a second text messaging device in order to have one with the Common Name "sms" you must select that device when targeting SMS Opt-In users in alerts or accountability events.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click .
3. In the **Users** section, click **SMS Opt-In**.
4. On the **SMS Opt-In** page, click **Activate**.

- A success message and details about the SMS Opt-In service are displayed on the **SMS Opt-In** page.

- A multi-select picklist attribute is automatically created that can be used to target users in alerts.



Make the Opt-In user attribute available for targeting and user management

When you enable SMS Opt-In, an Opt-In user attribute is automatically created. In order to target users in alerts and events using this SMS opt-in user attribute, you must make it available for targeting.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. Click ⚙.
3. In the **Basic** section, click **General Settings**.
4. On the **General Settings** screen, in the **Layouts** section, click **View/Edit** beside **Targeting Settings** .
5. On the **Group Targeting Definition** window, in the **Available Fields** column, click the **Opt-In** *<opt-in-number>* attribute.
6. Click **Add**.
7. Optionally, use the control buttons on the right to move the Opt-In attribute higher or lower in the **Selected Fields** list.
8. Click **Save**.
9. On the **General Settings** screen, click **Save**.
10. In the navigation bar, click **Users** > **User Attributes**.
11. On the **User Attributes** screen, click the **Opt-In** *<opt-in-number>* attribute.
12. On the user attribute details page, in the **Page Layout** section, select a value from the **User Details - Full Page** pull-down menu. Do not leave this option set to **Do Not show**.
13. Click **Save**.

Create an event code

Create an event code so that you can target users outside your organization with SMS alerts.

1. Click .
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event Codes**.
4. On the **Manage Event Codes** page that opens in a new tab on your browser, click **New**.
5. On the **Create New Event code** window, enter an event code name. Spaces and the following characters are not allowed: `!$%&^()={},;\:?"<>|\
6. In the **Event Code** field, enter an event code. This is the code that you will provide to your end users. They send this event code in an SMS to subscribe to alerts.
7. Optionally, in the **Expiration** field, select a date for the event code to expire. When an event code expires, users can no longer use the event code.
8. Click **Save**.

After you finish: When you promote your event code, include the following text: `Text [event-code] to [sms-number]`. If you do not know the SMS number, see SMS numbers for U.S. hosted systems and SMS numbers for European hosted systems.

SMS numbers for U.S. hosted systems

Country	Primary SMS number	Backup SMS number
Canada	73101	73102
Japan	81502	80447
New Zealand	2316	2575
United Arab Emirates	3775	6991
United States	28462	73101

SMS numbers for European hosted systems

Country	Primary SMS number	Backup SMS number
Canada	555666	333666
Croatia	815517	815518
Japan	85136	80447
New Zealand	4840	8434
United Arab Emirates	1727	2496
United Kingdom	65165	65465

Country	Primary SMS number	Backup SMS number
United States	333666	444666

Edit an event code

Event codes can be edited until they expire. Event codes cannot be deleted.

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. On the **SMS Opt-In** screen, click **Manage Event codes**.
4. Optionally, on the **Manage Event Codes** window, enter an event code in the **Search** field and click 🔍 to narrow the list of event codes.
5. On the **Manage Event Codes** window, click ✎ on the row for the event code you want to edit.
6. Optionally, update the **Event Description**, **Event Code**, and **Expiration** fields.
7. Click **Save**.

Deactivate SMS Opt-In

1. Click ⚙.
2. In the **Users** section, click **SMS Opt-In**.
3. Click **Deactivate**.

Configure device gateways

To set up alert delivery devices, you must configure the gateway for each device. The gateway is an API that translates alert text to XML format and delivers it to the provider for a device. The provider can be a BlackBerry AtHoc service such as AtHoc cloud telephony or a third-party provider.

Note: When a device delivery gateway is added, deleted, reordered, or configured, it is captured in the operator audit trail. To view these entries in the operator audit trail, click > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select specific actions from the **Action(s)** list.

1. In the navigation bar, click .
2. In the **Devices** section, click the name of the device gateway that you want to configure.

   The gateway configuration settings screen opens. The values that you need to provide depend on the device you want to configure. The following table describes how you can find configuration values for a particular device.

Gateway	Documentation
AtHoc Cloud Delivery Service (East Coast)	Configure the hosted gateway for cloud services
AtHoc Cloud Delivery Service (West Coast)	Configure the hosted gateway for cloud services
BlackBerry AtHoc Mobile App	Configure the BlackBerry AtHoc mobile app
AtHoc Connect	*BlackBerry AtHoc Connect*
BlackBerry Messenger	*BBM Enterprise Alerts Installation and Administration Guide*
CAP Feed	Manage a CAP feed device
Desktop App	• Configure desktop app settings • *BlackBerry AtHoc Desktop App Installation and Configuration Guide*
OEM Cloud Delivery Service (East)	Configure the hosted gateway for cloud services
OEM Cloud Delivery Service (West)	Configure the hosted gateway for cloud services
RSS Feed	Configure RSS feed information for RSS and Atom content feeds
Text Messaging	Configure the text messaging device for hosted SMS
TTY/TDD Phone	Manage a TTY/TDD phone device
Xml Feed	Configure XML feed information for mass communication devices

The following custom device gateways should only be configured with the help of BlackBerry AtHoc customer support:

- ADT Giant Voice
- AM Radio Broadcast
- AM Radio Transmitter
- American Signal Giant Voice
- American Signal Giant Voice - V2
- ATI Giant Voice
- Benbria Classroom Emergency Notification
- Cable TV + Radio
- Cable TV Scroller
- Cisco IP Phone Display
- Cisco UCM (Blast)
- Cisco UCM (TAS)
- Cisco Unified Communication Manager
- Eaton WAVES
- Emergency Digital Information Service (EDIS)
- Federal Signal Giant Voice
- IPAWS CAP Exchange, EAS, NWEM, and WEA
- Land Mobile Radio
- Land Mobile Radio - Eastman
- LRAD Giant Voice
- Monaco Warning System
- Motorola ACE 3600
- On-Premise Email
- RGM Digital Signage
- SiRcom
- Talk-A-Phone Giant Voice
- TechRadium
- X (Twitter)
- Whelen Giant Voice, v1
- Whelen Giant Voice, v2
- Xml Feed Reset
- Zetron Pager
- Zetron Pager Group

3. Configure the values based on the device and information provided by BlackBerry AtHoc customer support or the configuration information provided in the referenced documents.
4. Click **Save**.

Configure the BlackBerry AtHoc mobile app

Use the Devices screen to verify available devices, check settings, and if necessary, disable or restore specific devices such as mobile devices for the Personal Safety Service. You can also control and edit permissions to make certain device addresses only available to operators, or to end users, or to both roles.

Configure the Mobile app gateway to deliver alerts to and receive alerts from the mobile device.

For more information about Mobile App settings, see "Configure mobile alert settings" in the *BlackBerry AtHoc Incoming Alerts in the Inbox* guide.

Configure the mobile app gateway settings

Configure the Mobile App gateway settings to deliver alerts to and receive alerts from the mobile device.

Note: Contact BlackBerry AtHoc customer support for assistance in setting up the BlackBerry AtHoc mobile app. Before you begin this process, you should also contact your system administrator to get the NDS address used for the notification delivery server.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mobile App**.

   The Mobile App gateway configuration screen opens with the default settings that are listed in the following table.

   Note: You should use the default values to set up and configure the BlackBerry AtHoc mobile app.

Option	Description
Notification Delivery Server Settings	

Option	Description
Notification Delivery Server Address	`https://mobile.athoc.com`
Username	Must be between 3 and 100 characters long.
Password	Must be between 3 and 100 characters long.
Debug Trace	Avoid performance degradation by enabling debug tracing for the mobile delivery gateway only while actively debugging the mobile notifications for the mobile app. Options: Yes | No **Default:** No
Features	
Alerts	Selected. Available for all users.
Collaboration	Selected. Available for all users and operators.
Map	Not selected. Available for all users.
Alert Publishing	Selected. Available for operators only.
Advanced Features	Selected. When selected, advanced features display. Select a distribution list to give access to advanced features to a group of users. Options include: • Emergencies • Check In/Check Out • Reports • Tracking: When this option is selected, the Tracking Interval option displays. Select a tracking interval. • My Profile Page: When this option is selected, the "Show Preferred language selection to support bilingual alerts" option displays. For more information about advanced features, see Role-based permissions for the mobile app.
Settings	
Photo Quality	Options: Low | High **Default:** Low
Video Quality	Options: Low | High **Default:** Low

Option	Description
Emergency Contact Number	Designate the emergency contact telephone number. If no phone number is entered in the field, the mobile app will not have an emergency contact number button.
Support Email Address	Enter an email address that administration log and feedback from the mobile app can be sent to.
Enable Mobile Analytics	Collects mobile app usage analytics. No personal, private, or sensitive information is collected. Options: Yes | No **Default:** No
Enable Personal Alert Button	Enables sending an emergency using a paired personal alert button. Emergencies must be enabled in Advanced Features. Options: Yes | No **Default:** Yes
Enable Jail-Break/Root Detection	Enables the mobile app to check if the device OS security has been compromised. Options: Yes | No **Default:** No
Send Location with Response	Sends user location information with alert or event responses. Options: Yes | No **Default:** Yes
User Choice	Enables each mobile user to choose whether to send location information with alert or event responses. Options: Yes | No **Default:** Yes This option is visible only when "Yes" is selected for Send Location with Response.
Enable Debug Log	Enables debug tracing on the mobile app. Enable this option to allow a detailed log to be written on the mobile app. Options: Yes | No **Default:** No

3. Click **Copy Default Settings**.

4. In the **Notification Delivery Server Address** field, enter the NDS address you received from your system administrator. By default, the URL points to `mobile.athoc.com`.
5. Add the user name and password provided by BlackBerry AtHoc.
6. In the **Features** section, select the options that will be available to users when they are using their mobile device:
   - **Alerts**: Users can receive alerts.
   - **Collaboration**: Enables the Collaboration feature for all users and operators.
   - **Alert Publishing**: Operators can publish alerts.
   - **Advanced Features**: Advanced features are available to a selected group of users. When you select this option, advanced features are displayed. Each mobile feature in the Advanced Features section includes its own menu to select a distribution list. To learn about the advanced features, see Role-based permissions for the mobile app.
7. In the **Settings** section, select the photo and video quality.
8. In the **Emergency Contact Number** field, enter the phone number of the operations center to which emergencies are sent from mobile devices.
9. In the **Support Email Address** field, enter an email address where logs are sent for error debugging.
10. In the **Enable Mobile Analytics** section, select whether to enable the mobile app to collect usage analytics.
11. In the **Enable Personal Alert Button** section, select whether to enable users to send an emergency duress message using a paired personal alert button.
12. In the **Enable Jail-Break/Root Detection** section, select whether to enable the mobile app to check if the device OS security has been compromised.
13. In the **Send Location with Response** section, select whether to send location information with alert or event responses. When **No** is selected, location information is prevented from being returned with alert or event responses even if mobile location services are active on the mobile device.
14. In the **User Choice** section, select whether to enable mobile users to choose to send location information with alert or event responses. This option is only available when **Yes** is selected in the **Send Location with Response** section.
15. In the **Enable Debug Log** section, select whether to enable debug tracing on the mobile app.
16. Click **Save**.

Assign an AtHoc mobile gateway to a phone

To assign an AtHoc mobile gateway to a phone and set up mobile phone notification, see Configure mobile phone notification.

Configure mobile phone notification

After BlackBerry AtHoc customer support has set up the correct Notification Delivery Server (NDS) address, you can assign an AtHoc mobile gateway to the phone and enable mobile phone notification.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, click **Mobile App**.
4. On the **Mobile App** page, click **Edit**.
5. In the **Name** field, enter `Mobile App`.
6. In the **Common Name** field, enter the following text with no space between the words: `mobileNotification`.
7. In the **Delivery Gateways** section, click **Add a Delivery Gateway** > **Mobile App**.
8. Click **Save** in the top menu bar.
9. Click **More Actions** > **Enable** in the top menu bar if the device is not yet enabled.

Role-based permissions for the mobile app

As a System Administrator, you can specify what controls a user can see on the mobile device, depending on their roles and responsibilities (also known as role-based permissions). For example, you might want an emergency team to be able to see the map, send field reports, start tracking, and send emergency duress alerts. However, you might want a student on a campus or non-emergency personnel to only be able to receive notifications and to send duress (emergency) alerts to security without having access to the map or to tracking or field reports.

1. For users who need advanced features, create a distribution list.

   Note: Only one distribution list can be used for the organization.
2. In the navigation bar, click ⚙.
3. In the **Devices** section, click **Mobile App**.
4. On the **Mobile app** screen, in the **Features** section, select **Alerts** to grant permission to receive alerts on mobile devices.
5. Select **Alert Publishing** to provide publishing permission to operators.
6. Select **Advanced Features** to provide advanced features to a group of users. When selected, the **Select advanced features** section appears.
7. In the **Select advanced features** section, select one or more features and distribution lists that the user can access from the mobile app:

   - **Emergencies**: Send duress messages.
   - **Check In/Check Out**: Perform user check-ins and check-outs on the map.
   - **Reports**: Send field reports.
   - **Tracking**: Track mobile device location for a specified amount of time.
   - **My Profile Page**: Enable users to edit their My Profile page and manage their organization subscriptions.

     When selected, the **Show Preferred language selection to support bilingual alerts** option appears. Select this option to display the Preferred Language field on the My Profile screen on the mobile app. This option enables users to choose to receive alerts in their preferred language.
8. After selecting an advanced feature, choose a distribution list that can use the selected feature.
9. Make any other needed changes for the mobile app settings.
10. Click **Save**.

Configure devices overview

You must specify the devices that users receive alerts on. For example, a user can receive an alert on multiple devices, including smart phones, SMS, tablets, desktop pop-ups, work or home phones, through loudspeakers, or email.

Perform the following high-level tasks to configure devices that end users receive alerts on:

1. Enable devices on the BlackBerry AtHoc server.
2. Configure the device delivery gateway.
3. Configure and enable the device from the Devices screen.
4. Verify that the device appears in the End User details display settings.

For additional configuration steps that must be completed for mass communication devices, see Manage mass communication devices.

Enable devices on the BlackBerry AtHoc server

The first step in configuring devices for BlackBerry AtHoc is to enable the device on the BlackBerry AtHoc server. When you enable the device, it appears in the list of gateways on the Settings screen and in the list of devices in Devices.

1. Log in as an administrator to the server that BlackBerry AtHoc runs on.
2. Navigate to the following folder: `../Program Files (x86)/AtHocENS/ServerObjects/Tools`.
3. Open the following application: `AtHoc.Applications.Tools.InstallPackage`.
4. On the **Configure Device Support** screen, select the check boxes next to each device needed for the organization.
5. Click **Enable**.
6. Click **Close**.

Duplicate a device on the BlackBerry AtHoc server

When you enable a device on the BlackBerry AtHoc server, you have the option to create a duplicate of that device. Only Giant Voice devices can be duplicated. If you attempt to duplicate a non-Giant Voice device from the Configure Device Support screen, an error is displayed.

When you duplicate a device, it appears in the list of gateways on the Settings screen and in the list of devices in the Devices screen with a "-DUP1" extension. You can create additional duplicates of the same device, as needed. Each duplicate is appended with a new "-DUP#" extension. For example, ATI-DUP1, ATI-DUP2, and ATI-DUP3.

You can duplicate a Giant Voice device up to six times. There is a 30 character limit to the ID of the duplicated device.

1. Log in as an administrator to the BlackBerry AtHoc server.
2. Navigate to the following folder: `../Program Files (x86)/AtHocENS/ServerObjects/Tools`.
3. Open the following application: `AtHoc.Applications.Tools.InstallPackage`.
4. On the **Configure Device Support** screen, select the check box next to the device you want to duplicate.
5. Click **Duplicate**.
6. Optionally, click **Enable**.
7. Click **Close**.

Configure devices

If you are an administrator, you can use the Devices screen to verify available devices, check settings, set the device delivery priority for enabled personal devices, and enable and disable devices. You can also control and edit permissions to make certain device addresses available only to operators, or to end users, or to both roles.

Availability of delivery devices other than the AtHoc desktop software depends on the BlackBerry AtHoc edition and licensed delivery devices. Contact your BlackBerry AtHoc account manager for details.

Note: When a device's common name, display name, group order, or contact information is updated, it is captured in the operator audit trail. To view these entries in the operator audit trail, click > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select specific actions from the **Action(s)** list.

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.

   On the **Devices**screen, the **Personal Devices** tab opens by default. Click the **Mass Devices** tab to configure a mass device. Each tab displays the available devices and their details in a table with the following columns:

   - **Device Name**: Displays a description of the device type.
   - **Delivery Gateway**: Displays the designated delivery gateways, if applicable.
   - **Group**: Displays the type of alert that gets delivered, such as email or phone.
   - **# Users**: (Personal Devices tab only.) Displays the number of users that have the personal device enabled in their profile.

   Disabled devices are grayed out in the display. Disabled devices are not available for delivering alerts. Each device has a default delivery template that defines the appearance and formatting used to deliver alerts.
3. Optionally, set device delivery priority.
4. Optionally, use the **Search For Device** field to search for a device. Click **Advanced**, and select from the **Delivery Gateway**, **Group**, and **Status** drop-down menus to refine the search results.
5. Optionally, click the **Mass Devices** tab to view and edit mass devices.
6. Click the device name to configure the related template.

For more information on device configuration, see View and edit device details.

Enable and disable devices

If you have administrator permissions, you can use the Devices screen to disable and enable specific devices to control which devices appear in the user profile and to add them to the list of devices for alert targeting.

Enable a device

Only devices that have at least one associated gateway can be enabled. Although some devices have a gateway already assigned to them, for other devices such as Xml Feed, Twitter, or Zetron Pager, you must first open the device's details screen and add the gateway manually before you can enable the device.

1. In the navigation bar, click .
2. In the **Devices** section, select the check box in the row for the device you want to enable.
3. Click **More Actions** > **Enable**.
4. Click **OK**.

Disable a device

1. From the list, select the check box in the row for the device you want to disable.

2. Click **More Actions** > **Disable**.
3. Click **OK**.

Set device delivery priority

Operators can set the priority of alert delivery by device type. When enabled, the device delivery preference feature prevents end uses from receiving the same alert on multiple devices. When configured, end users receive alerts on their enabled devices in the order specified at the organization level or at the alert level selected by the operator. End users can also set a device priority for the devices they have enabled and provided an address for in their user profile. By default, the device delivery preference is in this order:

- Mobile App
- Email
- Text Message
- Pager
- Fax
- Phone TTT/TDD Phone
- User Callback

Additional enabled devices are added to the bottom of the list.

Note: The BlackBerry AtHoc desktop app does not support device delivery preference.

When a device's delivery priority is changed, it is captured in the operator audit trail. To view this entry in the operator audit trail, click > **System Setup** > **Operator Audit Trail**. Select **Delivery Device** from the **Entity** list. Select the **Search by Specific Actions(s)** option and then select **Device Delivery Preference Updated** from the **Action(s)** list.

Before you begin: Device delivery preference must be enabled for your organization.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Devices** section, click **Devices**.
4. On the **Devices** page, on the **Personal Devices** tab, click **Edit**.
5. Optionally, to change the delay interval, select the number of minutes from the **Delay Interval** pull-down menu. The delay interval is the time in minutes that the system waits before sending an alert to the next device. The default delay interval is 2 minutes. The delay interval is consistent between each priority level.
6. Optionally, to change the delivery priority for any device in the list, click and drag the device to the desired priority position. When organization-defined or system-defined is selected in an alert or event template, the alert or event is targeted to devices in the order they appear in the list.
7. Click **Save**.

Add a device to the user details contact information

After you enable the gateway and configure the device on the Devices page, you might need to add the device to the list of available devices for end users. BlackBerry AtHoc provides a draft list that you might need to modify so that a user can add contact information in their profile.

Prerequisite

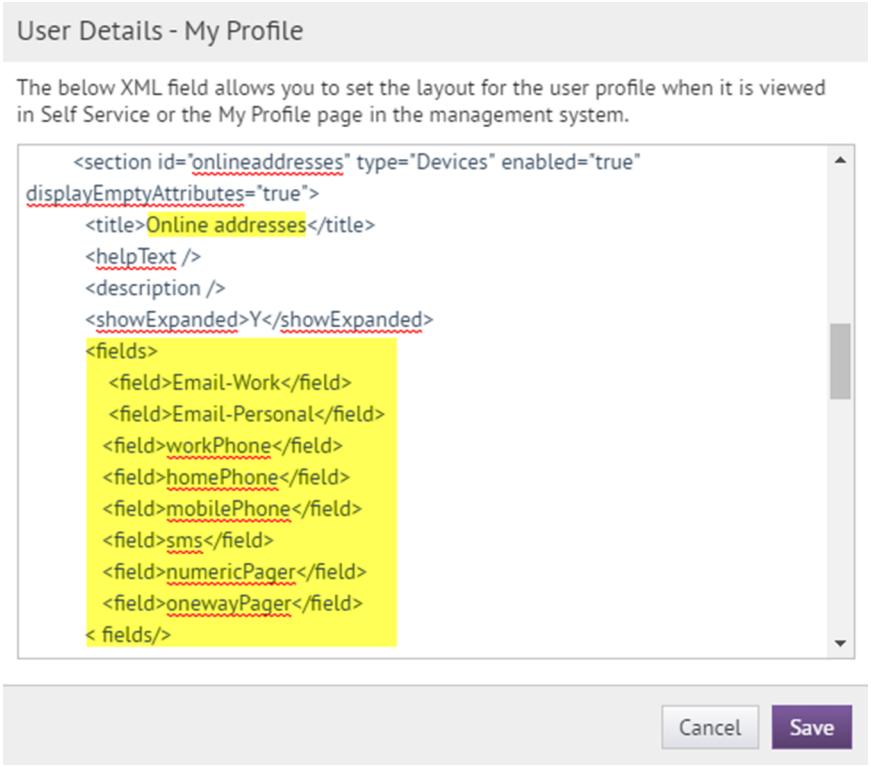
To add a device to the end user device display list, you must know its common device name. To determine a common device name, complete the following steps:

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. Click to open each device you need the common name for.

   The **Common Name** field appears in the **Details** section.
4. Write down the common name so that you can insert it when adding a device to the end user device list.

To add a device to the end user device display, complete the following steps:

1. Log in to BlackBerry AtHoc as an administrator.
2. In the navigation bar, click ⚙.
3. In the **Basic** section, click **General Settings**.
4. Scroll down to the **Layouts** section.
5. In the **User Details - My Profile** row, click **View/Edit**.
6. In the **User Details - My Profile** window, scroll down to the **<Online addresses>** section.
7. Check to see if the needed devices are in the list. If not, manually add them in the XML file.



8. If the devices are not in the list, add `<field></field>` values for each device using the common device names that you wrote down in the prerequisite section above.
9. Click **Save**.
10. On the **General Settings** page, click **Save**.

Manage mass communication devices

To manage support for a mass communication device such as a digital sign, a loudspeaker, or an XML feed, complete the following tasks:

- Enable devices on the BlackBerry AtHoc server
- Configure device gateways

- Configure devices
- Create a mass device endpoint

Mass device types and categories

Mass devices in BlackBerry AtHoc are divided into these categories: Giant Voice, Feed, CAP Feed, Social, and Common.

The following table lists the supported mass devices and their categories.

Mass device	Mass device category
ALERTUS-BEACON	Giant Voice
AM-RADIO	Common
BENBRIA	Common
CAP Feed	CAP Feed
CATV	Common
EAS	Common
EMERGE-ENOTIFY	Common
FIRE-PANEL - 8 Channels	Common
FIRE-PANEL - 16 Channels	Common
GIANT-VOICE-ACE3600	Giant Voice
GIANT-VOICE-ATI	Giant Voice
GIANT-VOICE-FEDSIG	Giant Voice
GIANT-VOICE-WHELEN-V2	Giant Voice
IIM-LRAD	Giant Voice
IIM-SERIAL-GIANT-VOICE	Giant Voice
IIM-ZETRON-PAGER	Pager
IIM-ZETRON-PAGER-GROUP	Pager
INDUSTRIALSTROBE-BEACON	Common
LAND-MOBILE-RADIO-EASTMAN	Common
LAND-MOBILE-RADIO-V2	Common
MINITOR_V_TWO_TONE	Common

Mass device	Mass device category
MONACO-WARNING-SYSTEM	Giant Voice
MOTOTRBO_TWO-WAY_RADIOS	Common
PUBLIC-ADDRESS-SYSTEM	Common
PUBLIC-FEED (CWS)	Common
PUBLIC-FEED-V2 (CWS v2)	Common
SN-FEED (XML)	Feed
SN-FEED-SECONDARY (RSS)	Feed
SN-TWITTER	Social
UAP-DS (RMG Digital Signage)	Common
UAP-IAC	Common
UAP-IPAWS	Common
UAP-IPAWS-NWEM-EAS	Common
UAP-IPAWS-WEA2	Common
UAP-LED	Common
VOICE-DTMF	Giant Voice
Zetron Pager	Common

Create a mass device endpoint

To distribute messages through mass communication devices like a digital sign, you must create a BlackBerry AtHoc mass device endpoint. Creating a mass device endpoint makes the mass device available for targeting in alerts.

Mass devices are divided into these categories: Giant Voice, Feed, CAP Feed, Social, and Common. Complete any of the following tasks to create mass device endpoints.

You must have Operator or End Users Manager privileges to create a mass device endpoint.

Note: You can export the information about mass device endpoints to a CSV file by selecting the endpoints on the Mass Device Endpoints screen, and then selecting **More Actions** > **Export**.

Giant Voice

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.

4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **Configuration** section, select a Giant Voice Type: **Pole**, **Zone**, **Key**, or **Other**.
6. Enter the address for the Giant Voice device.
7. (For Giant Voice Key type only) Enter the **Giant Voice Key XML**.
8. Click **Save**.

Feed

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **General** section, enter a common name. Enter a value between 4 and 80 characters long. The following special characters are not allowed: (` ! $ % ^ ( ) = { } , ; : ? " < > | [space])
6. In the **Configuration** section, enter a title for the feed. Enter a value between 1 and 100 characters.
7. Optionally, enter a description for the feed.
8. Select whether to require authentication. The default is **No**. If you select **Yes**, enter an authentication username and password.
9. Optionally, enter a URL to use to access alerts through the content feed.
10. Click **Save**.

Social

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **Configuration** section, if no Twitter account already exists, click **Provide Twitter Credentials**.
6. On the **Twitter / Authorize an application** page, enter the account name and password for your Twitter account.
7. Click **Authorize app** to give permission to BlackBerry AtHoc to tweet to this Twitter account.
8. On the **New Mass Device Endpoint** screen, click **Save**.

Common

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** and then select the mass device you want to target.
4. On the **New Mass Device Endpoints** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.

5. In the **Configuration** section, enter the address for the mass device. The following special characters are not allowed: (`!^=<>)

CAP Feed

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Mass Device Endpoints**.
3. Click **New** > **CAP Feed**.
4. On the **New Mass Device Endpoint** screen, in the **General** section, enter an endpoint name. Enter a value between 4 and 80 characters. The following special characters are not allowed: ` ! $ % ^ ( ) = { } , ; : ? " < >

   Note: The Display Name is automatically populated with the name entered in the Endpoint Name field.
5. In the **Configuration** section, enter an address for the feed. Enter a value between 1 and 100 characters.
6. Select whether to require authentication. The default is **No**. If you select **Yes**, enter an authentication username and password.
7. In the **URL** field, enter the following URL to use to access alerts through the content feed: /Syndication/{*ENDPOINT_DISPLAY_NAME*}/CapFeed
8. Click **Save**.

View and edit device details

Note: You should consult BlackBerry AtHoc customer support before editing the values for a device to ensure that your changes will not have a negative impact on the way the device operates.

Note: You must be an Enterprise Administrator to edit the details of a device.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, click to select a device.

   The screen refreshes to display the settings for the device, divided into the following three sections: Details, Help Text, and Delivery Gateways.

   The Details section varies by device. Use the Help Text section to change the help text in the targeting, contact, or contact information tool tip. The Delivery Gateways section provides information about device-specific gateways. A device must have at least one associated gateway before it can be enabled. For more information on enabling devices, Enable and disable devices.
4. Click **Edit** to modify the details, help text, or delivery gateway details.
5. Click **Save**.

Configure Giant Voice devices

The following integration gateways are related to Giant Voice loudspeaker systems:

- ADT Giant Voice
- American Signal Giant Voice
- American Signal Giant Voice - v2
- ATI Giant Voice
- Eaton WAVES
- Federal Signal Giant Voice
- LRAD Giant Voice
- Monaco Warning System
- SiRcom
- Talk-a-Phone Giant Voice

- Whelan Giant Voice - v1
- Whelan Giant Voice - v2

To learn how to configure Giant Voice gateways, see the BlackBerry AtHoc integrations documentation at the following URL: https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/integrations/

Configure the AtHoc Connect organization network

The Organization feature provides inter-agency communications between organizations that have joined AtHoc Connect. Organizations are members of AtHoc Connect that you can add as a connection. You can then publish alerts to that connection or subscribe to alerts that they publish.

To learn how to set up the gateway and device for AtHoc Connect, see the *BlackBerry AtHoc Connect* guide.

Manage the Cloud Services Gateway

BlackBerry AtHoc provides hosted SMS, email, and telephony notification services. If your organization uses any of these services, you need to configure and enable the gateway.

The following sections describe these configuration tasks:

1. Enable the Cloud Services Gateway on the BlackBerry AtHoc server.
2. Enable the Cloud Services Gateway on the Settings screen.
3. Configure and enable the Cloud Services devices. Complete only the sections that correspond with the services your organization uses:
   - Hosted SMS Text Messaging
   - Hosted Email
   - Hosted Telephony

Configure the hosted gateway for cloud services

Use this gateway to set up devices using the AtHoc or OEM Cloud Delivery Service. After configuring this gateway, you can set up telephony (TAS), email (OPM), and SMS.

1. In the navigation bar, click .
2. In the **Devices** section, click to open one of the following gateways, based on information supplied by your BlackBerry AtHoc services representative:
   - AtHoc Cloud Delivery Service (East)
   - AtHoc Cloud Delivery Service (West)
   - OEM Cloud Delivery Service (East)
   - OEM Cloud Delivery Service (West)
3. Click **Copy default settings** at the top of the screen.

   The default templates for the services appear in the SMS and Email template fields.
4. Enter the user name and password values provided to you by BlackBerry AtHoc customer support.
5. Optionally, for TAS, you can enter a Caller ID (ANI) value to override the default value for the account.

   The value should be a valid phone number or extension that is 4-16 numeric characters.
6. For the SMS (texting) template, replace the existing template, with the following template:

7. Optionally, modify the SMS XML template fields for your organization by adding placeholders.

   The following table describes the parameters that you can add to either the SMS or the Email template. The placeholders values are preset:

Placeholder	Required	Purpose and Values
[MessageBody]	Yes	The contents of the SMS message (the alert text.)
[MessageTitle]	Yes	The title of the SMS message.
[PublishedAt]	No	The time when the alert is published.
[PublishedBy]	No	The operator account name that sends the alert.
[RecipientName]	No	The name of recipients the alert is sent to.
[ResponseOptions]	No	The response options provided for the recipient of the text message. If empty, the Response Option instruction line does not appear in the alert. The default is `Reply:`, but can be customized text like “Select a response.”
[SelfServiceUrl]	No	Link to the user’s Self Service screen.
[Severity]	No	The value of the Severity field for the alert.
[SystemName]	No	The name of the current organization.
[TargetUrl]	No	The URL in the optional "More Info Link" field, provided for more information.
[Type]	No	The category of the alert, such as Safety.
[OrganizationName]	No	The organization name that is displayed in the BlackBerry AtHoc title pane.

8. Optionally, if you use the hosted email service, you can configure a custom "From" address in the **From Display Name** field. The From Display Name must include a valid email address in angle brackets. For example, XYZ Alerts<Alerts@xyz.com>.

   Note: The From Display Name email domain must be registered with the AtHoc Cloud Delivery system before use. Using an invalid email address will prevent emails from being delivered.

After setting up the Cloud Delivery Services Gateway, you can configure the related devices from the Devices screen.

- Hosted SMS text messaging
- Hosted email
- Hosted Telephony

Configure the text messaging device for hosted SMS

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, on the **Personal Devices** tab, click **Text Messaging**.
4. On the **Text Messaging** screen, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization.
6. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
7. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option users are still able to provide the information, but it is not required.
8. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to edit the Help Text fields.

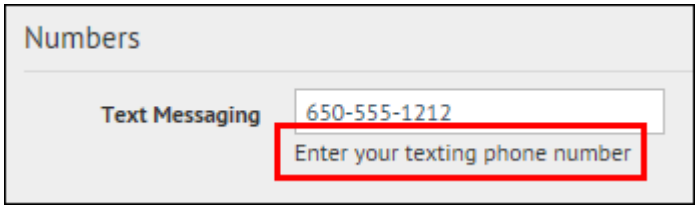
   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if you want to remind operators that text messages have a character limit, you can enter the following text:

     "SMS: Alert will be split into multiple messages if it exceeds 140 characters or 70 unicode characters."

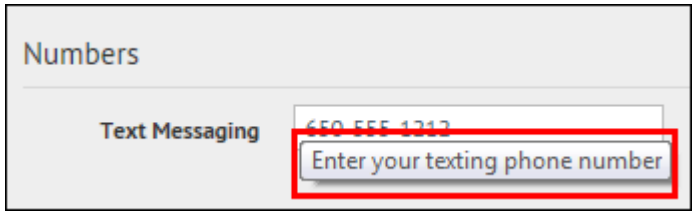
     The text then appears at the top of the Review and Publish screen.

   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.

   - **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



9. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select AtHoc **Cloud Delivery Service**. You can specify up to three gateways for the Hosted SMS device.
10. Click **Save**.
11. If you are ready to make the device available for alert publishing, click **More Actions** > **Enable**. The Hosted SMS Text Messaging device is then fully configured.

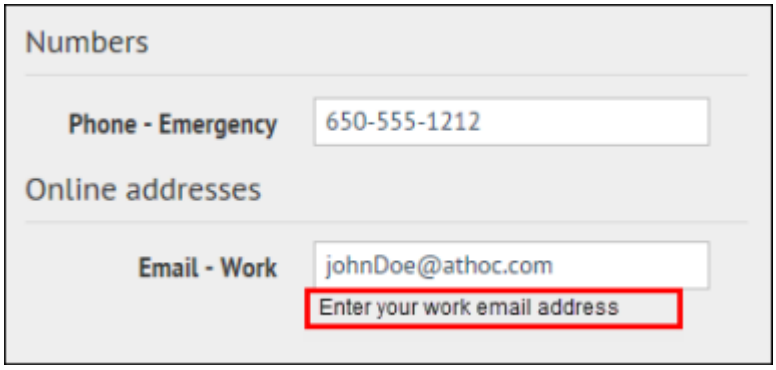
Manage the hosted email service

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** page, on the **Personal Devices** tab, click an email device.
4. On the device details page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization.
6. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
7. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option, providing the information will be optional.
8. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

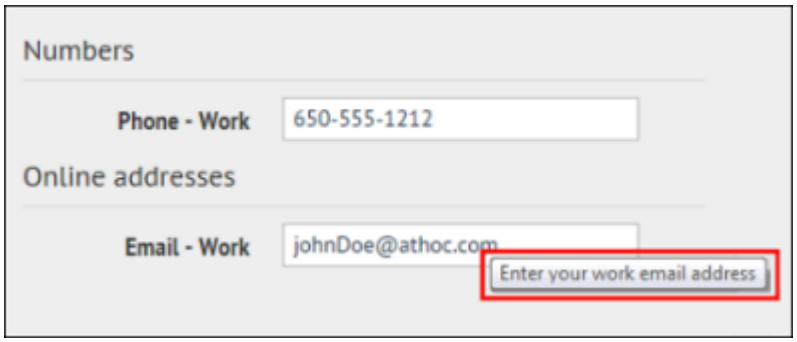
   Note: You must be an Enterprise Administrator to edit the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if the device is a work email account, you can enter, "Email - Work: Do not use for off-shift alerts" so that users know not to select the device if they are trying to contact people who are not at work.

   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.



- **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers the cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



9. In the **Delivery Gateway** section, click **Add a Delivery Gateway** and then select **AtHoc Cloud Delivery Service Gateway** or **OEM Cloud Delivery Service**, either East or West, based on the information BlackBerry AtHoc customer support has provided.
10. Click **Save**.
11. If you are ready to make the device available for alert publishing, click **More Actions** > **Enable**.

The device is available for alert publishing.

Manage the hosted telephony service

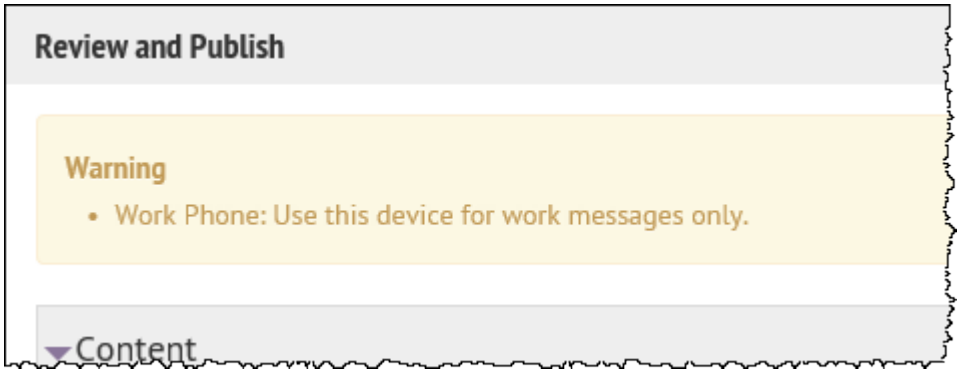
1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Devices** screen, in the **Personal Devices** tab, click a phone device such as **Phone-Work** or **Phone-Mobile**.
4. On the device details page, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must be an Enterprise Administrator to update the Name, Common Name, and Device Group Order.
6. In the **Contact Info Editing** field, select either **All** or **End Users** depending on whether you want everyone or just end users to have the ability to edit their contact info.
7. Optionally, select the **Enable GETS** option to enable Government Emergency Telecommunications Service (GETS) calls. GETS calls can be made only from land lines and not from mobile phones.
8. Optionally, select **Users must provide contact info for this Device in Self Service** if you want to require users to provide that information. If you do not select this option, users will still be able to provide the information but it will not be required.
9. In the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to modify the help text fields.

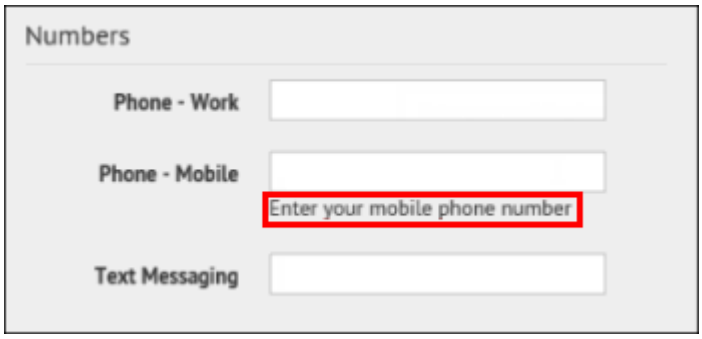
- **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if the phone is a work phone, you can enter the following text:

  "Work Phone: Use this device for work messages only."

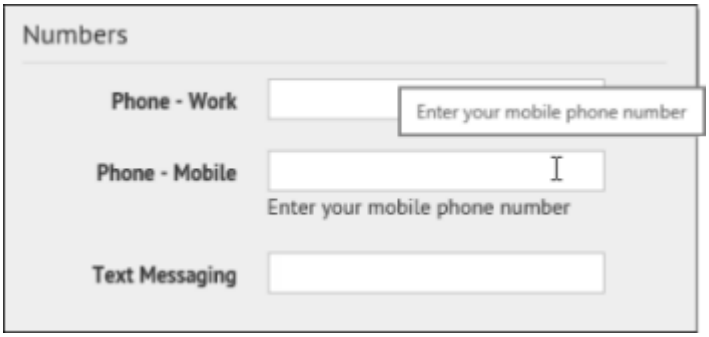
  The text then appears at the top of the Review and Publish screen.



- **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.



- **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.



10. In the **Delivery Gateways** section, select one of the **AtHoc Cloud Delivery Service Gateway** options, either East or West.
11. Click **Save**.
12. Click **More Actions** > **Enable**.

The device is available for alert publishing.

Configure RSS feed information for RSS and Atom content feeds

Mass communication devices include the IP Integration Module for RSS and Atom feeds. These devices use the templates for the RSS feed.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **RSS Feed**.
3. Click **Copy default settings** at the top of the screen to use the correct settings for the content feed.

   RSS or Atom feeds should have the following settings:

   - In the **Supported Formats** field, **Syndication: Atom** and **Syndication: RSS 2.0** are selected.
   - In the **Identity Source** field, the **End User** option is selected.
4. Click **Save**.

Configure XML feed information for mass communication devices

Mass communication devices include the IP Integration Module for loud speakers, as well as RSS and Atom feeds. These devices use the templates for the XML Feed.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Xml Feed**.
3. On the **Xml Feed** screen, specify the mass communication device you want to configure.
   - If you use Atom or RSS feeds, complete the following steps:
     a. In the **Feed Formats** section, select **Syndication: Atom** and **Syndication: RSS 2.0**.
     b. In the **Feed Source** section, select **End User**.
   - If you use an IIM CapCon feed for outdoor loud speakers, complete the following steps:
     a. In the **Feed Formats** section, select **Syndication: CapIndex** and **Syndication: CapIim**.
     b. In the **Feed Source** section, select **Delivery Gateway ID**.
4. Click **Save**.

Configure failover delivery gateways

The Delivery Gateway Failover feature adds redundancy to various devices such as phones that can be connected to multiple gateways. If one gateway fails, the other gateway takes over.

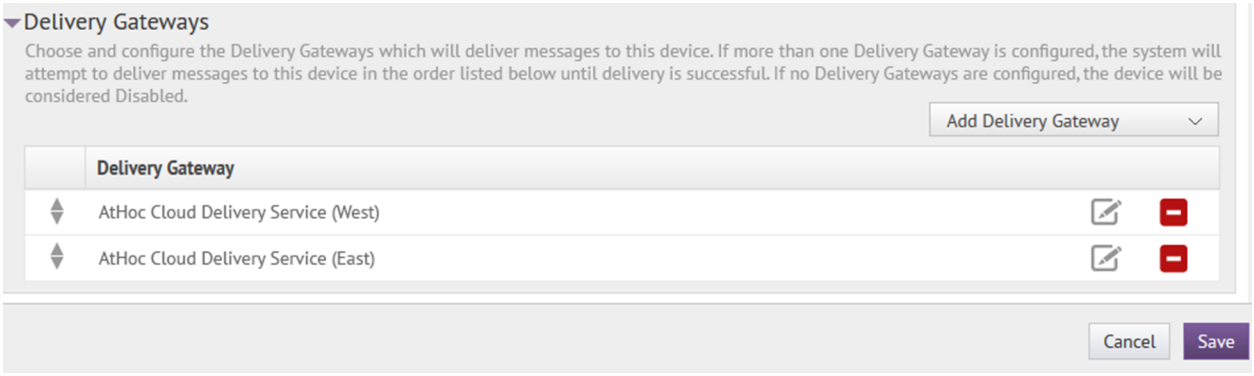
Most gateways have only one type of supported gateway and you enable a second gateway of the same type on a failover server. However, certain device groups have multiple gateways that manage alerts for the device. You can use a different gateway if the device is in the same group, where a group includes related devices such as phones, email, or text messaging.

Configuration of delivery gateway failover is handled from the Devices screen. The following list shows groups with multiple devices or gateways and specifies which gateways can be used with a device group.

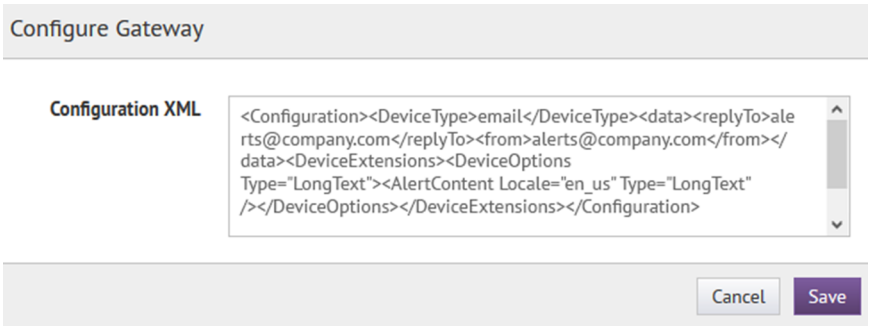
- **Email**: AtHoc Cloud Delivery Service (East and West), OEM Cloud Delivery Service (East and West)
- **Pager**: AtHoc Cloud Delivery Service (East and West)
- **Phone**: AtHoc Cloud Delivery Service (East and West)
- **Texting**: AtHoc Cloud Delivery Service (East and West)
- **Fax**: AtHoc Cloud Delivery Service (East and West)
- **TTY**: AtHoc Cloud Delivery Service (East and West)

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click a device name.

4. On the device details screen, click **Edit**.
5. Assuming that the device has a primary gateway configured, in the **Delivery Gateways** section, click **Add a Delivery Gateway** to add a second gateway.



6. Click .
7. On the **Configure Gateway** window, modify the XML statements as needed for your organization.



8. Click **Save**.

Manage a TTY/TDD phone device

Note: Only the EN-US locale is supported on TTY/TDD phone devices.

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click **TTY/TDD Phone**.
4. On the **TTY/TDD Phone** screen, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must be an Enterprise Administrator to update the Name, Common Name, Group Name, and Device Group Order.
6. Optionally, select **Users Must Provide Contact Info For This Device in Self Service** if you want to require users to provide that information. If you do not select this option, users are still able to provide the information, but it is not required.
7. Optionally, select the **Enable GETS** option to enable Government Emergency Telecommunications Service (GETS) calls. GETS calls can be made only from land lines and not from mobile phones.
8. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
9. Optionally, in the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to edit the help text fields.

- **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if you want to remind operators that TTY/TDD phone messages have a character limit, you can enter the following text:

  "TTY/TDD Phone: Alert will be split into multiple messages if it exceeds 140 characters or 70 unicode characters."

  The text then appears at the top of the Review and Publish screen.
- **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.
- **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.

10. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select **AtHoc Cloud Delivery Service (West)** or **AtHoc Cloud Delivery Service (East)**.
11. Click .
12. On the **Configure Gateway** window, replace the content with the following:

```
<Configuration><DeviceType>TTY</DeviceType></Configuration>
```

13. Click **Submit**.
14. Click **Save**.
15. Click **More Actions** > **Enable** if you are ready to make the device available for alert publishing.

    The TTY/TDD Phone device is then fully configured.

Manage a CAP feed device

Before you begin

Complete the following tasks for a CAP feed device:

- Enable devices on the BlackBerry AtHoc server
- Configure device gateways
- Configure devices
- Create a mass device endpoint

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.
3. On the **Mass Devices** tab, click **CAP Feed**.
4. On the **CAP Feed** screen, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must be an Enterprise Administrator to update the Name, Common Name, Group Name, and Device Group Order.
6. From the **Contact Info Edit** pull-down menu, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
7. Optionally, in the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to edit the help text fields.

   - **Targeting Help Text**: When the operator selects the CAP Feed device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen. For example, if you want to remind operators

that they are publishing an alert to a CAP Feed, you can enter the following text: You are publishing to a CAP Feed.

The text then appears at the top of the Review and Publish screen.

- **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.
- **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.

8. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select **CAP Feed**.
9. Optionally, click to open the **Configure Gateway** dialog and review or edit the **Configuration XLM**. By default, the following Configuration XML is displayed:

```
<Configuration><CapFeedParams>
<GVSystemType>CAPFEED</GVSystemType>
<ContentSource>CAP-FEED</ContentSource>
</CapFeedParams></Configuration>
```

10. If you have made any changes to the configuration XML, click **Submit**.
11. On the **CAP Feed** screen, click **Save**.
12. Click **More Actions** > **Enable** if you are ready to make the device available for alert publishing.

The CAP Feed device is fully configured.

Manage a pager device

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.
3. On the **Personal Devices** tab, click one of the following pager devices:
   - **Pager**
   - **Pager (Numeric)**
   - **Pager (One Way)**
   - **Pager (Two Way)**
   - **Pager Group**
4. On the device details screen, click **Edit**.
5. Modify the values in the **Details** section with names and information that are valid for your organization. You must be an Enterprise Administrator to update the Name, Common Name, Group Name, and Device Group Order fields
6. Select a **Device Group Order** from the list.
7. In the **Contact Info Edit** field, select who can edit contact information. The options are **All**, **None**, **End Users**, and **Operators**.
8. Optionally, select **Users Must Provide Contact Info For This Device in Self Service** if you want to require users to provide that information. If you do not select this option, users can provide the information, but it is not required.
9. Optionally, in the **Help Text** section, enter text that will appear on the screen when operators are creating an alert.

   Note: You must be an Enterprise Administrator to edit the help text fields.

   - **Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the **Review and Publish** screen.

- **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.
- **Contact Info Tool Tip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.

10. In the **Delivery Gateways** section, click **Add a Delivery Gateway** and then select AtHoc **Cloud Delivery Service (West)**, or **Zetron Pager**.
11. Click **Save**.
12. Click **More Actions** > **Enable** if you are ready to make the pager device available for alert publishing.

The pager device is then fully configured.

Translate custom device attributes

Complete the following steps to provide custom translations of device attributes including the device name, alert targeting help text, contact information help text, and tooltips.

Before you begin:

- You must be a System Administrator to translate device attributes.
- You must be logged in to the System Setup organization.

1. Log in to the BlackBerry AtHoc management system and change to the **System Setup** organization.
2. In the navigation bar, click .
3. On the **Settings** screen, in the **Users** section, click **Custom Translation**.
4. On the **Custom Translation** screen, in the **Translation Type** section, select the **Devices** option.
5. Select a personal or mass device from the **Select Device** drop-down list. Only enabled personal and mass devices appear in the list.
6. Enter translated text for any of the following device attributes:
   - **Name**: This name appears in user profiles and when selecting devices for alert targeting. The Name field has a 128 character limit.
   - **Tooltip**: The text you enter in this field appears as a pop-up tool tip when the user hovers their cursor over the device name on the End User details screen. The text should explain what should be entered in the field.
   - **Alert Targeting Help Text**: When the operator selects this device as a target, the text you enter in this field appears at the top of the Review and Publish screen.
   - **Contact Info Help Text**: The text you enter in this field appears under the device name on the End User details screen. The text should explain what should be entered in the field.

   These fields have a 1024 character limit. These special characters are not allowed: `!$%&^()={}.,;\:?"'<>|[]
7. Click **Save**.

   BlackBerry AtHoc does not validate the accuracy of the translation. Verify the accuracy of all translated text before saving.

Configure desktop app settings

If you are an administrator, you can configure desktop app settings such as general display items, the system tray menu, client server communications, and failover.

Most settings for the BlackBerry AtHoc desktop app are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. However, the settings described in the

following sections might require editing over time and are of interest to most administrators because they affect things such as the time intervals for viewing new alerts and updating user configurations, as well as end user login expiration times.

For information about advanced features such as redirection, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Select general desktop software options

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

1. In the navigation bar, click .
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, in the **Basic Options** section, select or deselect the check boxes beside the following values:
   - **Show Welcome message for first-time sign-on**: Causes a web page with a welcome message to appear when the desktop app connects for the first time.
   - **Right-click to dismiss Desktop pop-up**: Allows end users to dismiss the desktop pop-up with a right mouse click.
   - **Show uninstall option in control panel and Start menu**: Shows the Uninstall button in the toolbar of the "Uninstall or change a program" dialog in Programs and Features when the AtHoc[edition] application is selected from the list of applications.
   - **Collect workstation information**: Allows the desktop app to send the IP address, computer name, username, and domain name to the BlackBerry AtHoc server. This reduces the amount of user information that is transferred over the network. When this option is deselected, IP targeting does not work.
   - **Stop checking for updates when Desktop is locked**: Prevents the desktop app from checking for updates when an end user's desktop is locked. This option is useful in environments where users do not turn off their computers.
4. In the **Email Address To Send Client Logs** field, enter an email address (`sendlog@athoc.com`) to send the desktop app log to. When the user selects the "Send <organization name> Log" in the Start menu for the desktop app, the email address entered in this field receives a copy of the log file.
5. In the **ActiveX Object Name** field, enter the ActiveX object name for the desktop app. This is used when creating the JavaScript code that is sent by the server to the desktop app in response to requests and in alerts. For example, when the user selects the “Access Self Service” menu option, selects a response option, or clicks a button on an alert.
6. In the **Audio** section, select how the desktop app works with built-in speakers. Select **Consider end user system settings** to prevent the desktop app from overriding the end user's local system speaker settings. Select **Always turn on speaker** to override local speaker settings. When this option is selected, the **Desktop Volume Threshold** slider control appears. This option specifies the volume level that the desktop app sets the audio to.

   Note: The operating system does not provide a way for the desktop app to distinguish between headphones and speakers. When end users are wearing headphones that are plugged into the computer's audio jack, an incoming alert may sound extremely loud.

Customize the desktop client system tray

The system tray icon ( ) appears in the system tray when the desktop app is running. You can change the order of the links that appear in the desktop app system tray using an XML-based menu control. You can also move the link separator up or down and add additional link separators as needed.

1. In the navigation bar, click .
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, in the **System Tray Menu** section, select **Display System Tray Icon**.

4. In the **Available Menu Items** section, click **Manage Menu Items**.
5. On the **Desktop App Menu Items** window, click **Add Menu Item**.
6. On the **Add Menu Item** window, enter a name and URL for the new menu item.
7. Click **Save**. Take note of the ID of the new menu item.
8. Click **Close**.
9. In the **Menu Configuration** field, add the new menu item to the menu configuration XML. Menu items have this format: <Item Id="8009" Type="Link"/>.
10. Optionally, add a separator to the Menu Configuration XML. Separators have this format: <Item Type="Separator" />
11. Optionally, cut and paste the code for each additional function to add or move menu items and separators.
12. Click **Save**.

The following menu items are available:

Option	Included by default	Code
About	Yes	8005
Access My Profile	Yes	520
Access Self Service	Yes	521
Always Minimize Deskbar to System Tray	No	8015
Auto Hide Deskbar	No	8012
BlackBerry AtHoc Management System	Yes	532
Check for New Alerts	Yes	8009
Clear Search Box History	No	8002
Connection Options...	No	8008
Deskbar always on top	No	8013
Dismiss All Audio Notifiers	No	8021
Dismiss All Desktop Popups	No	8020
Dismiss All Popups	Yes	8022
Enable Popup Auto Focus	No	8025
Exit	No	8006
Show Deskbar	No	9002
Uninstall	No	8004

Option	Included by default	Code
Update My Device Info	Yes	531
Update My Info	Yes	530

The following is a sample Menu Configuration XML:

```
<SystrayLayout>
   <Item Id="8009" Type="Link" />
   <Item Id="8022" Type="Link" />
   <Item Type="Separator" />
   <Item Id="521" Type="Link" />
   <Item Id="530" Type="Link" />
   <Item Id="531" Type="Link" />
   <Item Type="Separator" />
   <Item Id="8005" Type="Link" />
</SystrayLayout>
```

For more information, see "System tray menu" in the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure client server communications

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

You must have system administrator permissions to configure client server communications.

Most settings in the Desktop App settings page are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. The settings in the Client Server Communications section of the Desktop App settings page are used to configure the settings that govern communication between the BlackBerry AtHoc server and the desktop app, and the rate at which new alerts and user configuration updates are checked.

1. In the navigation bar, click .
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, scroll down to the **Client Server Communications** section.
4. Select a value from the **Check Update Interval** list.

   The Check Update Interval (CU) determines how frequently the desktop app polls the server for updates, including alerts. A lower value causes end users to receive desktop pop-up alerts sooner. A higher value causes users to receive desktop pop-up alerts later. The minimum value is 30 seconds. The maximum value is 15 minutes. The recommended value is 2 minutes.
5. Select a value from the **Reconnect Interval** list.

   The Reconnect Interval specifies the interval the desktop app waits before attempting to contact the server again when the connection is lost. The minimum value is 1. The maximum value is 10. The recommended value is 2.
6. Select a value from the **Recovery Interval** list.

   The Recovery Interval specifies the number of check update intervals the desktop app waits before attempting to contact the server again when the server responds to a Sign On (SO) or CU with an error. The minimum value is 1. The maximum value is 10. The recommended value is 2.
7. Enter a value in the **Start-up Delay** field.

   The Start-up Delay setting is a fractional value between 0 and 1 inclusive that is used to determine the amount of delay before the desktop app first attempts to sign on. A value of 0 specifies no delay and a value of 1

specifies to wait one full check update interval. A value of .5 specifies a delay of 50% of the check update interval.

8. Enter a value in the **Communication Session Expires After** field.

   This option determines when the desktop app session is reset on the server. The default value is 86400 seconds (24 hours). When the desktop app session expires, the desktop app performs a sign on at the next CU.

9. Enter a value in the **Override Default Communication Session Expiration Time After** field.

   This setting cleans up system sessions that were created by the SYSTEM user. Sessions that are created by the SYSTEM user when desktop apps are deployed with the installation script and RUNAFTERINSTALL is set to "Y". Sessions can be created by the SYSTEM user when the installation script is used to update computers after the desktop app is installed.

   This option also enables desktop apps to perform a sign on in environments where users do not turn off their computer. This option provides a way to configure desktop apps to redirect during SO.

10. Click **Save**.

For more information, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure failover settings

Note: Do not modify the following settings without first consulting BlackBerry AtHoc customer support.

Most settings in the Desktop App settings page are established during the initial installation and configuration with the assistance of BlackBerry AtHoc customer support. The settings in the Failover section of the Desktop App settings page are used to enable the primary BlackBerry AtHoc server to fail over to a secondary server when the primary server becomes unresponsive and CUs fail.

1. In the navigation bar, click ⚙.
2. In the **Devices** section, click **Desktop App**.
3. On the **Desktop App** window, scroll down to the **Failover** section.
4. Enter the URL for the failover server.
5. Select a value from the **Reconnect attempts before Failover** list.

   This setting specifies the number of attempts that the Desktop app makes to contact the primary server before switching to the failover server.

6. Click **Save**.

For more information, see the *BlackBerry AtHoc Desktop App Installation and Administration Guide*.

Configure user authentication

1. In the navigation bar, click ⚙.
2. In the **Users** section, click **User Authentication**.
3. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, select one of the following authentication methods from the **Desktop App** > **Authentication Method** list:

   - **LDAP Attribute**: This option enables the desktop app to authenticate with an Active Directory attribute.

     a. Enter an Active Directory attribute in the **Attribute** field. The desktop app queries this attribute directly from the signed-in user's directory profile and sends it to the server. This option allows the desktop app to operate while sending less user information to the server. When this option is selected, the desktop app does not send Windows user names or domain names in sign on or check update query strings.

     b. Optionally, enter a valid LDAP URL in the **Custom LDAP URL** field. When a custom LDAP URL is specified, it overwrites the USERDOMAIN value from the local LDAP directory. Format the

custom domain name using a regex to accept only URLs such as LDAP://<DOMAINNAME>.<TOP-LEVELDOMAIN>:<(Optional) PORT#>. Sample valid URLs:

- LDAP://DC=examplewebsite,DC=com
- LDAP://examplewebsite.com
- LDAP://DC=examplewebsite,DC=com,DC=org
- LDAP://examplewebsite.ca

c. Optionally, select **Fallback to Windows Authentication** to configure the desktop app to authenticate with Windows Authentication if authentication with LDAP fails. This option appears only if **Windows Authentication** is selected in the **Enable Authentication Methods** section.

- **Smart Card**: This option enables smart card authentication. Select the number of client certificates to collect. The recommended value is 3.

a. Select the number of client certificates to collect from the **Number of Certificates** pull-down list. The recommended value is 3.

b. Optionally, in the **Regular Expression** field, enter a regular expression in the following format: `UID=(?<edipi>\d{8,10})`. Contact BlackBerry AtHoc customer support to configure this field.

c. Optionally, in the **Custom Attributes** field, add custom attributes to the CAC certificate. Add multiple attributes separated by a comma. There is a 100 character limit. The special characters < and > are not supported.

d. Optionally, in the **Client Regular Expression** field, enter a client regular expression in the following format: `.*?(^)(?:(?!\s-[A||E||S]).)*`. This format extracts information from the client certificate subject name to find the identical certificates for authentication. The regular expression provided in the UI is a sample expression that may not be suitable for your environment. You can build you own regular expression or contact BlackBerry AtHoc customer support to configure this field.

- **Defer to Self Service**: This option configures the desktop app to use the user authentication method selected for Self Service. When this method is selected, end users will see a login window. When the user clicks Log In, they are redirected to Self Service to complete the sign in process. This process depends on the authentication method selected by the administrator.

  If the Self Service authentication method is set to Username and Password, the users sees a registration window and must provide their first name, last name, username, password, confirm their password, and fill in a captcha. The user has the option to register as a new user or to sign in with their existing user credentials.

  If the Self Service authentication method is set to Smart Card, the user sees a certificate selection screen and must pick a certificate. They may also be required to enter a PIN.

  If the Self Service authentication type is set to Windows Authentication, the user sees a Windows credentials screen and must provide their username and password.

  If the Self Service authentication method is set to Single Sign-On, the user is sent to the SSO URL.

- **Windows Authentication**: This option configures the desktop app to use only the Windows username and password or to use both the Windows username and the domain.

4. Optionally, if **LDAP Attribute**, **Smart Card**, or **Windows Authentication** is selected, select the **Create new user if an account is not found** option to configure the desktop app to create a user at sign on if the user does not already exist.
5. Click **Save**.

BlackBerry AtHoc 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

©2024 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.

Patents, as applicable, identified at: www.blackberry.com/patents.

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